Acronis

acronis.com

Cyber Protection

24.03

Guía del usuario

REVISIÓN: 11/04/2024

Contenido

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. 19).

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. 19).

Requisitos de contraseña

La contraseña de las cuentas de usuario debe tener una longitud de al menos 9 caracteres. También se comprueba la complejidad de las contraseñas, que entran dentro de una de las siguientes categorías:

- Débil
- Medio
- Fuerte

No puede guardar una contraseña débil, incluso aunque contenga 9 caracteres o más. 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.

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 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. Instale una app de autenticación en su dispositivo móvil.
   Ejemplos de apps compatibles:
   - Twilio Authy
   - Microsoft Authenticator
   - Google Authenticator
2. 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**.
3. 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.
4. 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.

5. 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.

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 autenticación de doble factor (2FA) de su cuenta.

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

Si tiene acceso a la app de autenticación para entorno móvil instalada previamente

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:

a. 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.
b. Siga las instrucciones que aparecen en pantalla.

Si no tiene acceso a la app de autenticación para entorno móvil instalada previamente

1. Utilice un nuevo dispositivo móvil.
2. Utilice el archivo PDF almacenado para enlazar un nuevo dispositivo (el nombre predeterminado del archivo es `cyberprotect-2fa-backupcode.pdf`).
3. Restaurar el acceso a su cuenta desde la copia de seguridad. Asegúrese de que las copias de seguridad son compatibles con su app para entorno móvil.
4. Abra la app en la misma cuenta desde otro dispositivo móvil si es compatible con la app.

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**.
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.

Requerimientos de software

Navegadores web compatibles

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

- Google Chrome 29 o posterior
- Mozilla Firefox 23 o posterior
- Opera 16 o posterior
- Microsoft Edge 25 o posterior
- Safari 8 o una versión posterior que se ejecute en los sistemas operativos macOS y 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.

Sistemas operativos y entornos compatibles

Agente para Windows

Este agente incluye un componente para la protección antivirus y antimalware y el filtrado de las URL. Consulte "Funciones de protección compatibles con el sistema operativo" (p. 45) para obtener más información acerca de las funcionalidades compatibles por sistema operativo.

- Windows XP Professional SP1 (x64), SP2 (x64) y SP3 (x86)
- 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
- 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 (ediciones Home, Pro, Education, Enterprise y IoT Enterprise y LTSC, antes LTSB)
- 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

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 conocimientos para obtener más información sobre cuestiones relacionadas con la actualización del soporte de firma de código SHA2.

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)

Cada uno de estos agentes puede instalarse en un equipo que ejecute uno de los sistemas operativos indicados anteriormente y una versión compatible de la respectiva aplicación.

Agente para la prevención de la pérdida de datos

Control de dispositivos

- Microsoft Windows 7 Service Pack 1 y posterior
- Microsoft Windows Server 2008 R2 y posterior
- macOS 10.15 (Catalina)
- macOS 11.2.3 (Big Sur)
- macOS 12 (Monterey)
- macOS 13 (Ventura)

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 y posterior

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 de Advanced Data Loss Prevention

- Microsoft Windows 7 Service Pack 1 y posterior
- Microsoft Windows Server 2008 R2 y posterior

Agente para File Sync & Share

Para ver la lista de los sistemas operativos admitidos, consulte la Guía del usuario de Cyber Files Cloud.

Agente para Exchange (para la copia de seguridad de buzones de correo)

- 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

- 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)
- 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

- 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

- Linux: cualquier kernel y distribución compatibles con el Agente para Linux (se indican a continuación)

Agente para Linux

Este agente incluye un componente para la protección antivirus y antimalware y el filtrado de las URL. Consulte "Funciones de protección compatibles con el sistema operativo" (p. 45) para obtener más información acerca de las funcionalidades compatibles por sistema operativo.

Las siguientes distribuciones Linux y versiones de kernel se han probado específicamente. Sin embargo, aunque su distribución Linux o versión de kernel no aparezcan a continuación, puede que funcionen correctamente en todos los escenarios necesarios debido a las características específicas de los sistemas operativos Linux.

Si experimenta problemas al utilizar Cyber Protection con su combinación de distribución Linux y versión de kernel, póngase en contacto con el equipo de soporte técnico para que lo investigue.

Linux con kernel de 2.6.9 a 5.19 y glibc 2.3.4 o posterior, incluidas las siguientes distribuciones x86 y x86_64:

- Red Hat Enterprise Linux 4.x, 5.x, 6.x, 7.x, 8.x*, 9.0*, 9.1*, 9.2*, 9.3*
- 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
- Fedora 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 37, 38
- SUSE Linux Enterprise Server 10, 11, 12, 15

  Importante
  Las configuraciones con Btrfs no son compatibles con SUSE Linux Enterprise Server 12 y SUSE Linux Enterprise Server 15.

- Debian 4.x, 5.x, 6.x, 7.0, 7.2, 7.4, 7.5, 7.6, 7.7, 8.0, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 8.11, 9.0, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6, 9.7, 9.8, 10, 11
- CentOS 5.x, 6.x, 7.x, 8.x*

- CentOS Stream 8*, 9*
- Oracle Linux 5.x, 6.x, 7.x, 8.x*, 9.0*, 9.1*, 9.2* – tanto el Unbreakable Enterprise Kernel como el 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 conocimientos.

- CloudLinux 5.x, 6.x, 7.x, 8.x*
- ClearOS 5.x, 6.x, 7.x
- AlmaLinux 8.x*,9.0*, 9.1*, 9.2*
- Rocky Linux 8.x*, 9.0*, 9.1*, 9.2*, 9.3*
- ALT Linux 7.0

* A partir de la versión 8.4, solo se ofrece soporte con kernels de 4.18 a 5.19

Agente para Mac

Este agente incluye un componente para la protección antivirus y antimalware y el filtrado de las URL. Consulte "Funciones de protección compatibles con el sistema operativo" (p. 45) para obtener más información acerca de las funcionalidades compatibles por sistema operativo.

Se admiten las arquitecturas x64 y ARM (en procesadores de Apple Silicon, como Apple M1 y M2).

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

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.

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 para ejecutarse en un servidor ESXi.

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

Agente para VMware (Windows)

Este agente se suministra como aplicación de Windows ejecutable en cualquier sistema operativo de los enumerados anteriormente para el Agente para Windows, con las excepciones siguientes:

- 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.

Agente para Hyper-V

- 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
- 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 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

Agente para Virtuozzo

- 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

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

Agent para Scale Computing HC3

Scale Computing Hypercore 8.8, 8.9, 9.0, 9.1, 9.2, 9.3

Agente para oVirt

Red Hat Virtualization 4.2, 4.3, 4.4, 4.5

Agente para 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.

Cyber Protect Monitor

- Windows 7 y posterior
- Windows Server 2008 R2 y posterior
- Agente para Mac admite todas las versiones de macOS

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
- 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 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.

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.

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 la tabla siguiente se resume cómo las diferentes plataformas de virtualización son compatibles.

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. 68).

Nota
Si utiliza una plataforma de virtualización o una versión que no se encuentra en la lista a continuación, el método de **Copia de seguridad basada en agentes (Copia de seguridad desde dentro de un sistema operativo invitado)** aún puede 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

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** > **VMware ESXi** > **Agente para la instalación en Windows** o **Dispositivos** > **Añadir** > **Hosts de virtualización** > **VMware ESXi** > **Dispositivo virtual (OVF)**	Compatible **Dispositivos** > **Añadir** > **Estaciones de trabajo** o **Servidores** > **Windows** o **Linux**
VMware vSphere Hypervisor (Free ESXi)**	No compatible	Compatible **Dispositivos** > **Añadir** > **Estaciones de trabajo** o **Servidores** > **Windows** o **Linux**
VMware Server (VMware Virtual server) VMware Workstation VMware ACE VMware Player	No compatible	Compatible **Dispositivos** > **Añadir** > **Estaciones de trabajo** o **Servidores** > **Windows** o **Linux**

* 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.
- **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.
  - Equipos virtuales Hyper-V: En todos los equipos virtuales GEN2, Arranque seguro está deshabilitado cuando el equipo virtual se ha recuperado como un equipo virtual nuevo o como uno existente.
- La **Copia de seguridad de configuración de ESXi** no es compatible con VMware vSphere 7.0.
- **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. 58).

Microsoft

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 Windows 10 con Hyper-V Windows Server 2016 con Hyper-	Compatible **Dispositivos** > **Añadir** > **Hosts de virtualización** > **Hyper-V**	Compatible **Dispositivos** > **Añadir** > **Estaciones de trabajo** o **Servidores** > **Windows** o **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)
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		
Microsoft Virtual PC 2004, 2007 Windows Virtual PC	No compatible	Compatible **Dispositivos** > **Añadir** > **Estaciones de trabajo** o **Servidores** > **Windows** o **Linux**
Microsoft Virtual Server 2005	No compatible	Compatible **Dispositivos** > **Añadir** > **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 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.
- **Arranque seguro**
  En todos los equipos virtuales GEN2, Arranque seguro está deshabilitado cuando el equipo virtual se ha recuperado como un equipo virtual nuevo o como uno existente.
- **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. 58).
- **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.

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	Compatible **Dispositivos** > **Añadir** > **Hosts de virtualización** > **Scale Computing HC3**	Compatible **Dispositivos** > **Añadir** > **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. 58).

Citrix

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 XenServer/Citrix Hypervisor 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, 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** > **Añadir** > **Hosts de virtualización** > **Citrix XenServer** > **Windows** o **Linux**

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** > **Añadir** > **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** > **Añadir** > **Hosts de virtualización** > **Red Hat Virtualization (oVirt)**	Compatible **Dispositivos** > **Añadir** > **Estaciones de trabajo** o **Servidores** > **Windows** o **Linux**
Equipos virtuales basados en Kernel (KVM)	No compatible	Compatible **Dispositivos** > **Añadir** > **KVM** >

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 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** > **Añadir** > **Hosts de virtualización** > **Red Hat Virtualization (oVirt)**	Compatible **Dispositivos** > **Añadir** > **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** > **Añadir** > **Hosts de virtualización** > **Red Hat Virtualization (oVirt)**	Compatible **Dispositivos** > **Añadir** > **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** > **Añadir** > **Hosts de virtualización** > **Red Hat Virtualization (oVirt)**	Compatible **Dispositivos** > **Añadir** > **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. 58).

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** > **Añadir** > **Estaciones de trabajo** o **Servidores** > **Windows** o **Linux**
Parallels Server 4 Bare Metal	No compatible	Compatible **Dispositivos** > **Añadir** > **Estaciones de trabajo** o

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)
		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 Virtualization Manager (basado en oVirt)* 4.3	Compatible **Dispositivos** > **Añadir** > **Hosts de virtualización** > **Red Hat Virtualization (oVirt)**	Compatible **Dispositivos** > **Añadir** > **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** > **Añadir** > **Hosts de virtualización** > **Oracle** > **Windows** o **Linux**
Oracle VM VirtualBox 4.x	No compatible	Compatible **Dispositivos** > **Añadir** > **Hosts de virtualización** > **Oracle** > **Windows** o **Linux**

* Agente para oVirt admite Oracle Virtualization Manager.

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. 58).

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)
Nutanix Acropolis Hypervisor (AHV) 20160925.x mediante 20180425.x	No compatible	Compatible **Dispositivos** > **Añadir** > **Hosts de virtualización** > **Nutanix AHV** > **Windows** o **Linux**

Virtuozzo

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** > **Añadir** > **Hosts de virtualización** > **Virtuozzo**	Compatible solo con máquinas virtuales. No se admiten contenedores. **Dispositivos** > **Añadir** > **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** > **Añadir** > **Hosts de virtualización** > **Virtuozzo**	Compatible solo con máquinas virtuales. No se admiten contenedores. **Dispositivos** > **Añadir** > **Estaciones de trabajo** o **Servidores** > **Windows** o **Linux**
Virtuozzo Hybrid Server 7.5	Compatible **Dispositivos** > **Añadir** > **Hosts de virtualización** > **Virtuozzo**	Compatible solo con máquinas virtuales. No se admiten contenedores. **Dispositivos** > **Añadir** > **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. 58).

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	Compatible **Dispositivos** > **Añadir** > **Hosts de virtualización** > **Virtuozzo Hybrid infrastructure**	Compatible **Dispositivos** > **Añadir** > **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. 58).

Amazon

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)
Instancias de Amazon EC2	No compatible	Compatible **Dispositivos** > **Añadir** > **Estaciones de trabajo** o **Servidores** > **Windows** o **Linux**

Microsoft Azure

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)
Equipos virtuales de Azure	No compatible	Compatible **Dispositivos** > **Añadir** > **Estaciones de trabajo** o **Servidores** > **Windows** o **Linux**

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.
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 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. 435).

El bloqueo de retención (modo de administración) es compatible. Si el bloqueo de retención está habilitado, tiene que añadir la variable de entorno `AR_RETENTION_LOCK_SUPPORT` al equipo con el agente de protección que utiliza este almacenamiento como destino de copias de seguridad.

Nota
Agente para Mac no admite almacenamiento Dell EMC Data Domain con el bloqueo de retención habilitado.

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:
   - 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. Reinicie el equipo del dispositivo virtual.

Funciones de protección compatibles con el sistema operativo

Este tema contiene información acerca de las funciones de protección de Cyber Protect Cloud. En la lista no se muestran las funciones de copia de seguridad y recuperación.

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

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.

Conjunto de características	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

Conjunto de características	Windows	Linux	macOS
Planes de protección predeterminados			
Consulte las versiones de Windows compatibles en "Sistemas operativos y versiones compatibles" (p. 46).			

Conjunto de características	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 en "Sistemas operativos y versiones compatibles" (p. 46).			

Funciones	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 en "Sistemas operativos y versiones compatibles" (p. 46).			

Conjunto de características	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 en "Sistemas operativos y versiones compatibles" (p. 46).			

Conjunto de características	Windows	Linux	macOS
Active Protection			
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
Protección de carpetas de red	Sí	Sí	Sí
Protección del servidor	Sí	No	No
Protección de Zoom, Cisco Webex, Citrix Workspace y Microsoft Teams	Sí	No	No
Para obtener más información sobre los sistemas operativos y sus versiones, consulte "Plataformas compatibles" (p. 865).			

Conjunto de características	Windows	Linux	macOS
Protección antivirus y antimalware			
Funcionalidad Active Protection integrada por completo	Sí	No	No
Protección contra malware en tiempo real	Sí	Sí, con el pack de antimalware avanzado	Sí, con el pack de antimalware avanzado

Conjunto de características	Windows	Linux	macOS
Protección antivirus y antimalware			
Protección contra malware en tiempo real avanzada con detección basada en firmas locales	Sí	Sí	Sí
Análisis estadístico para archivos ejecutables portátiles	Sí	No	Sí*
Análisis antimalware bajo demanda	Sí	Sí**	Sí
Protección de carpetas de red	Sí	Sí	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	Sí***
Exclusiones de procesos	Sí	No	Sí
Motor de análisis de comportamiento	Sí	No	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 firewall****	Sí	No	No
Gestión del antivirus Microsoft Defender*****	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
Para obtener más información sobre los sistemas operativos y sus versiones, consulte "Plataformas compatibles" (p. 865).			

* En macOS, el análisis estadístico para archivos ejecutables portátiles solo se admite en los análisis programados.

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

*** En macOS, las exclusiones de archivos y carpetas solo se admiten cuando especifica los archivos y las carpetas que no se analizarán mediante la protección en tiempo real ni a través de análisis planificados.

**** La gestión del firewall es compatible con Windows 8 y versiones posteriores. Windows Server no es compatible.

***** La gestión del antivirus Windows Defender es compatible con Windows 8.1 y versiones posteriores.

Conjunto de características	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
Para obtener más información sobre los sistemas operativos y sus versiones compatibles, consulte "Productos de Microsoft y de terceros compatibles" (p. 1010), "Productos de Linux compatibles" (p. 1012) y "Productos de Apple y de terceros compatibles" (p. 1011).			

****** 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.

Conjunto de características	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	Sí	No	No

Conjunto de características	Windows	Linux	macOS
Gestión de parches			
ejecutando una copia de seguridad			
Consulte las versiones de Windows compatibles en "Sistemas operativos y versiones compatibles" (p. 46).			

Funciones	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
Consulte las versiones de Windows compatibles en "Sistemas operativos y versiones compatibles" (p. 46).			

Conjunto de características	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 en "Sistemas operativos y versiones compatibles" (p. 46).			

Funciones	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 en "Sistemas operativos y versiones compatibles" (p. 46).			

Conjunto de características	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	Sí	No	No

Conjunto de características	Windows	Linux	macOS
Análisis de copia de seguridad			
detectar si hay malware en la nube			
Análisis de malware de copias de seguridad cifradas	Sí	No	No
Consulte las versiones de Windows compatibles en "Sistemas operativos y versiones compatibles" (p. 46).			

Conjunto de características	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
Consulte las versiones de Windows compatibles en "Sistemas operativos y versiones compatibles" (p. 46).			

Conjunto de características	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 "Plataformas compatibles" (p. 1049).			

Conjunto de características	Windows	Linux	macOS
#CyberFit Score			
Estado de #CyberFit Score	Sí	No	No

Conjunto de características	Windows	Linux	macOS
#CyberFit Score			
Herramienta independiente de #CyberFit Score	Sí	No	No
Recomendaciones de #CyberFit Score	Sí	No	No
Consulte las versiones de Windows compatibles en "Sistemas operativos y versiones compatibles" (p. 46).			

Conjunto de características	Windows	Linux	macOS
Prevención de pérdida de datos			
Control de dispositivos	Sí	No	Compatible con equipos Mac con procesadores 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 en "Sistemas operativos y versiones compatibles" (p. 46).			

Conjunto de características	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.			

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

Conjunto de características	Windows	Linux	macOS
Cyber Protect Monitor			
App de Cyber Protect	Sí	No	Sí
Estado de la protección de Zoom	Sí	No	No
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 en "Sistemas operativos y versiones compatibles" (p. 46). En macOS, Cyber Protect Monitor es compatible con todas las versiones en las que pueda instalar Agente para Mac. Para obtener más información, consulte "Agente para Mac" (p. 28).			

Conjunto de características	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 en "Sistemas operativos y versiones compatibles" (p. 46). En macOS, el inventario del Software es compatible con las versiones 10.13.x − 13.x.			

Conjunto de características	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 en "Sistemas operativos y versiones compatibles" (p. 46). En macOS, el inventario del Hardware es compatible con las versiones 10.13.x − 13.x.			

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.

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	+	-	

Sistema de archivos	Compatibilidad con			Limitaciones
	Agentes	Dispositivos de arranque para Windows y Linux	Dispositivos de arranque para Mac	
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
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

Sistema de archivos	Compatibilidad con			Limitaciones
	Agentes	**Dispositivos de arranque para Windows y Linux**	**Dispositivos de arranque para Mac**	
				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 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

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.

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 Backup de Acronis.

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. 68).

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

Copia de seguridad basada en agente	Copia de seguridad sin agente
	de seguridad, ni mediante selección directa ni mediante el uso de reglas de directiva. Solo **Toda la máquina** está disponible en la sección **De qué realizar copias 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

	Desde la copia de seguridad basada en agentes	Desde la copia de seguridad sin agente
		◦ Microsoft Hyper-V ◦ Scale Computing HC3

Instalación e implementación de los agentes de Cyber Protection

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. 69).

Paso 3

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

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 "Implementación de agentes mediante la directiva de grupo" (p. 173).

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.

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 firewall 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.
- Puertos **44445** y **55556**

  Los agentes usan estos puertos para la transferencia de datos durante la realización de copias de seguridad y la recuperación.

Si hay un servidor proxy habilitado en la red, consulte "Ajuste de la configuración del servidor proxy" (p. 75) 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

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

- 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).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.

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 firewall.

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`

¿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, el Agente para MySQL/MariaDB y el Agente para Virtuozzo requieren que también esté instalado el Agente para Linux (de 64 bits). Estos agentes se incluyen en el archivo de instalación del Agente para Linux (de 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	
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 (de 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 (de 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 (de 64 bits)]	En el equipo que ejecuta Oracle Database.
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 "Uso del agente en la nube para Microsoft 365" (p. 640).
	Agente para Office 365	En un equipo Windows conectado

		a Internet. Para obtener más información, consulte "Usar el agente instalado localmente para Office 365." (p. 635).
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 "Uso del agente en la nube para Microsoft 365" (p. 640).
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. 676).
Active Directory		
Equipos que ejecutan Servicios de dominio de Active Directory	Agente para Active Directory	En el controlador de dominio.
Equipos virtuales		
Equipos virtuales VMware ESXi	Agente para VMware (Windows)	En un equipo Windows con acceso de red a vCenter Server y al almacenamiento del equipo virtual.**
	Agente para VMware (dispositivo virtual)	En el servidor ESXi.

Equipos virtuales Hyper-V	Agente para Hyper-V	En el servidor Hyper-V.
Equipos virtuales de Scale Computing HC3	Agente para Scale Computing HC3 (dispositivo virtual)	En el servidor de Scale Computing HC3.
Máquinas virtuales de Red Hat Virtualization (gestionadas por oVirt)	Agente para oVirt (dispositivo virtual)	En el servidor de Red Hat Virtualization.
Equipos virtuales y contenedores Virtuozzo***	Agente para Virtuozzo [Incluido en el archivo de instalación del Agente para Linux (de 64 bits)]	En el servidor Virtuozzo.
Equipos virtuales de la Virtuozzo Hybrid Infrastructure	Agente para Virtuozzo Hybrid Infrastructure (dispositivo virtual)	En el servidor de la Virtuozzo Hybrid Infrastructure.
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.		
Equipos virtuales de Citrix 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		
Equipos virtuales Nutanix AHV		
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		
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. 728).

***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 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.

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. La copia de seguridad basada en agentes 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. 64)

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. 32).

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:

- Funcionalidad de protección adicional, como antivirus y antimalware, gestión de parches o conexión de escritorio remoto. Para obtener más información sobre estas características, consulte "Funciones de protección compatibles con el sistema operativo" (p. 45).

- 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 característica 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 característica, consulte "Agente para VMware: copia de seguridad sin LAN" (p. 728).
- Menos sobrecarga de configuración. El agente dedicado respalda las máquinas virtuales en el nivel de hipervisor, independientemente del sistema operativo de los invitados.

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.

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
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

Paquetes de Linux

Para agregar los módulos necesarios al kernel de Linux, el programa de instalación 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` and `gcc version 4.5.1`
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 la `versión de GCC` del paso 1. Para **hacerlo**, 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: `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 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
  ```

- 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.

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. 80).

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 el monitor de Cyber Protection. Para obtener más información, consulte "Configuración del servidor proxy en el monitor de Cyber Protect" (p. 325).

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.
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. 85).

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.
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 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 de agentes de protección

Es posible instalar agentes en equipos en los que se ejecute cualquiera de los sistemas operativos enumerados en "Entornos y sistemas operativos compatibles". Los sistemas operativos compatibles con las funciones de Cyber Protect aparecen en "Funciones de Cyber Protect que son compatibles con el sistema operativo".

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 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**.
   - **Versión anterior**: descargue la versión anterior del agente.
   - **Actual**: descargue la versión más reciente disponible 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 procesadores Mac con Apple Silicon (como Apple M1)] Haga clic en **Cancelar**. En el panel **Añadir Mac** que se abre, haga clic en el enlace **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

1. Haga clic en el icono **Usuario** en la esquina superior derecha de la consola 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**.
   - **Versión anterior**: descargue la versión anterior del agente.
   - **Actual**: descargue la versión más reciente disponible 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**.

Instalación de agentes de protección en Windows

Requisitos previos

Descargue el agente que necesite en la carga de trabajo que desee proteger. Consulte "Descarga de agentes de protección" (p. 79).

Pasos para instalar Agente para Windows

1. Asegúrese de que el equipo está conectado a Internet.
2. Inicie sesión como administrador e inicie el programa de instalación.
3. [Opcional] Haga clic en **Personalizar configuración de la instalación** y realice los cambios necesarios para:
   - Para cambiar los componentes que se deben instalar (por ejemplo, para deshabilitar la instalación del Cyber Protection Monitor o la herramienta de línea de comandos, o para instalar el agente para la protección antimalware o el agente para el filtrado de URL).

     Nota
     En las máquinas Windows, la función de protección antimalware requiere la instalación del agente de protección antimalware y la función de filtrado de URL requiere la instalación del agente para el filtrado de URL. Estos agentes se instalan automáticamente en el caso de las cargas de trabajo protegidas si los módulos de **Protección antivirus y antimalware** o **Filtrado de URL** están habilitados en sus planes de protección.

   - Cambiar el método de registro de la carga de trabajo en el servicio de Cyber Protection. Puede cambiar de **Usar la consola de servicio** (opción predeterminada) a **Usar credenciales** o **Usar token de registro**.
   - Cambiar 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. 88).

- Verificar o modificar el nombre de host, la dirección IP, el puerto y las credenciales del servidor proxy. Si hay un servidor proxy habilitado en Windows, se detectará y usará automáticamente.

4. Haga clic en **Instalar**.
5. [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**.

   Le recomendamos utilizar una cuenta dedicada para acceder al host de vCenter Server o ESXi en lugar de utilizar una cuenta existente con el rol de Administrador. Para obtener más información acerca de los privilegios necesarios para la cuenta dedicada, consulte "Agente para VMware: privilegios necesarios" (p. 738).
6. [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.
7. Si ha seguido el método de registro predeterminado **Usar la consola de servicio** en el paso 3, espere a que aparezca la pantalla de registro y, a continuación, siga con el paso siguiente. De lo contrario, no se requieren más acciones.
8. Realice uno de los siguientes procedimientos:
   - Si inicia sesión con una cuenta de administrador de empresa, registre las cargas de trabajo para su empresa:
     a. Haga clic en **Registrar carga de trabajo**.
     b. En la ventana del navegador que se abrirá, inicie sesión en la consola de Cyber Protect y revise los detalles de registro.
     c. En la lista **Registrar para cuenta**, seleccione la cuenta de usuario en la que quiere registrar la carga de trabajo.
     d. Haga clic en **Comprobar código** y, a continuación haga clic en **Confirmar registro**.
   - Si inicia sesión con una cuenta de administración de partner, registre las cargas de trabajo para sus clientes:
     a. Haga clic en **Registrar carga de trabajo**.
     b. En la ventana del navegador que se abrirá, inicie sesión en la consola de Cyber Protect y revise los detalles de registro.

c. En la lista **Registrar para cuenta**, seleccione la cuenta de usuario de su cliente en la que quiere registrar la carga de trabajo.
d. Haga clic en **Comprobar código** y, a continuación haga clic en **Confirmar registro**.

- Haga clic en **Mostrar información de registro**. El programa de instalación mostrará el vínculo y el código de registro. Si no puede completar el registro de la carga de trabajo en el equipo actual, copie el código y el enlace de registro y, a continuación, siga los pasos de registro en un equipo diferente. En ese caso, deberá escribir el código de registro en el formulario de registro. El código de registro tiene una validez de una hora.
  También puede acceder al formulario de registro haciendo clic en **Todos los dispositivos** > **Agregar**, desplazándose hacia abajo hasta **Registro por código** y haciendo clic en **Registrarse**.

  Nota
  No salga del programa de instalación hasta confirmar el registro. Para iniciar el registro de nuevo, reinicie el programa de instalación y repita el proceso.

  Como resultado, la carga de trabajo se asignará a la cuenta que se utilizó para iniciar sesión en la consola de Cyber Protect.
- Registre el carga de trabajo manualmente mediante la línea de comando. Para obtener más información sobre cómo hacerlo, consulte "Registro y anulación de registro manual de cargas de trabajo" (p. 123).

9. [Si el agente está registrado en una cuenta cuyo inquilino está en el modo de Cumplimiento] Establezca la contraseña de cifrado.

Instalación de agentes de protección en Linux

Preparación

- Descargue el agente que necesite en el equipo que desee proteger. Consulte "Descarga de agentes de protección" (p. 79).
- Asegúrese de que los paquetes de Linux necesarios se han instalado en el equipo.
- Al instalar el agente en SUSE Linux, asegúrese de utilizar `su -` en lugar de `sudo`. De lo contrario, ocurre 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 visualización que mostrar.`
  Algunas distribuciones de Linux, como SUSE, no pasan la variable DISPLAY cuando se utiliza sudo, y el programa de instalación no puede abrir el navegador en la interfaz gráfica de usuario (GUI).

Instalación

Para instalar el agente para Linux necesita al menos 2 GB de espacio libre en disco.

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. Los agentes disponibles son los siguientes:
   - Agente para Linux
   - Agente para Virtuozzo
   - Agente para Oracle
   - Agente para MySQL/MariaDB

   Agente para Virtuozzo, Agente para Oracle y Agente para MySQL/MariaDB requieren que el Agente para Linux (de 64 bits) también esté instalado.
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.
5. Realice uno de los siguientes procedimientos:
   - Si inicia sesión con una cuenta de administrador de empresa, registre las cargas de trabajo para su empresa:
     a. Haga clic en **Registrar carga de trabajo**.
     b. En la ventana del navegador que se abrirá, inicie sesión en la consola de Cyber Protect y revise los detalles de registro.
     c. En la lista **Registrar para cuenta**, seleccione la cuenta de usuario en la que quiere registrar la carga de trabajo.
     d. Haga clic en **Comprobar código** y, a continuación haga clic en **Confirmar registro**.
   - Si inicia sesión con una cuenta de administración de partner, registre las cargas de trabajo para sus clientes:

a. Haga clic en **Registrar carga de trabajo**.

b. En la ventana del navegador que se abrirá, inicie sesión en la consola de Cyber Protect y revise los detalles de registro.

c. En la lista **Registrar para cuenta**, seleccione la cuenta de usuario de su cliente en la que quiere registrar la carga de trabajo.

d. Haga clic en **Comprobar código** y, a continuación haga clic en **Confirmar registro**.

- Haga clic en **Mostrar información de registro**. El programa de instalación mostrará el vínculo y el código de registro. Si no puede completar el registro de la carga de trabajo en el equipo actual, copie el código y el enlace de registro y, a continuación, siga los pasos de registro en un equipo diferente. En ese caso, deberá escribir el código de registro en el formulario de registro. El código de registro tiene una validez de una hora.

  También puede acceder al formulario de registro haciendo clic en **Todos los dispositivos** > **Agregar**, desplazándose hacia abajo hasta **Registro por código** y haciendo clic en **Registrarse**.

  Nota
  No salga del programa de instalación hasta confirmar el registro. Para iniciar el registro de nuevo, reinicie el programa de instalación y repita el proceso.

  Como resultado, la carga de trabajo se asignará a la cuenta que se utilizó para iniciar sesión en la consola de Cyber Protect.
- Registre el carga de trabajo manualmente mediante la línea de comando. Para obtener más información sobre cómo hacerlo, consulte "Registro y anulación de registro manual de cargas de trabajo" (p. 123).

6. [Si el agente está registrado en una cuenta cuyo inquilino está en el modo de Cumplimiento] Establezca la contraseña de cifrado.
7. Si el arranque seguro UEFI se habilita en el equipo, se le informará de que debe reiniciar el sistema tras la instalación. Asegúrese de que recuerda qué contraseña (la del usuario raíz o "acronis") debe utilizar.

   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 (Machine Owner Key), 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

Descargue el agente que necesite en la carga de trabajo que desee proteger. Consulte "Descarga de agentes de protección" (p. 79).

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.
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. Realice uno de los siguientes procedimientos:
   - Si inicia sesión con una cuenta de administrador de empresa, registre las cargas de trabajo para su empresa:
     a. Haga clic en **Registrar carga de trabajo**.
     b. En la ventana del navegador que se abrirá, inicie sesión en la consola de Cyber Protect y revise los detalles de registro.
     c. En la lista **Registrar para cuenta**, seleccione la cuenta de usuario en la que quiere registrar la carga de trabajo.
     d. Haga clic en **Comprobar código** y, a continuación haga clic en **Confirmar registro**.
   - Si inicia sesión con una cuenta de administración de partner, registre las cargas de trabajo para sus clientes:
     a. Haga clic en **Registrar carga de trabajo**.
     b. En la ventana del navegador que se abrirá, inicie sesión en la consola de Cyber Protect y revise los detalles de registro.
     c. En la lista **Registrar para cuenta**, seleccione la cuenta de usuario de su cliente en la que quiere registrar la carga de trabajo.
     d. Haga clic en **Comprobar código** y, a continuación haga clic en **Confirmar registro**.
   - Haga clic en **Mostrar información de registro**. El programa de instalación mostrará el vínculo y el código de registro. Si no puede completar el registro de la carga de trabajo en el equipo actual, copie el código y el enlace de registro y, a continuación, siga los pasos de

registro en un equipo diferente. En ese caso, deberá escribir el código de registro en el formulario de registro. El código de registro tiene una validez de una hora.

También puede acceder al formulario de registro haciendo clic en **Todos los dispositivos** > **Agregar**, desplazándose hacia abajo hasta **Registro por código** y haciendo clic en **Registrarse**.

Nota
No salga del programa de instalación hasta confirmar el registro. Para iniciar el registro de nuevo, reinicie el programa de instalación y repita el proceso.

Como resultado, la carga de trabajo se asignará a la cuenta que se utilizó para iniciar sesión en la consola de Cyber Protect.

- Registre el carga de trabajo manualmente mediante la línea de comando. Para obtener más información sobre cómo hacerlo, consulte "Registro y anulación de registro manual de cargas de trabajo" (p. 123).

10. [Si el agente está registrado en una cuenta cuyo inquilino está en el modo de 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. 86).

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 permisos al Agente de Connect:

- Grabación de pantalla: habilita la grabación de pantalla de la carga de trabajo de macOS mediante NEAR. Hasta que no se otorgue este permiso, se negarán 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 la carga de trabajo remota de macOS a la carga de trabajo local mediante NEAR. Para habilitar la función de redireccionamiento del sonido, se debe instalar un controlador de captura del sonido en la carga de trabajo. Para obtener más información, consulte "Redireccionamiento de sonido remoto" (p. 1051).
- Automatización: habilita la acción de vaciar papelera de reciclaje

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** para el agente de Cyber Protect, haga clic en **Configurar permisos del sistema**.
2. En el cuadro de diálogo **Permisos de sistema**, haga clic en **Solicitar permiso de grabación de pantalla**.
3. Haga clic en **Abrir preferencias del sistema**.
4. Seleccione **Agente de Connect**.

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** para el agente de Cyber Protect, haga clic en **Configurar permisos del sistema**.
2. En el cuadro de diálogo **Permisos de sistema**, haga clic en **Solicitar permiso de accesibilidad**.
3. Haga clic en **Abrir preferencias del sistema**.
4. Haga clic en el icono del candado en la esquina inferior izquierda de la ventana para que cambie a uno 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** para el diálogo Agente de Connect, haga clic en **Configurar permisos del sistema**.
2. En el cuadro de diálogo **Permisos de sistema**, haga clic en **Solicitar permiso de micrófono**.
3. Haga clic en **Aceptar**.

Nota
También debe instalar un controlador de captura de sonido en la carga de trabajo de macOS para dejar que el agente utilice el permiso otorgado y redirija el sonido de la carga de trabajo. Para obtener más información, consulte "Redireccionamiento de sonido remoto" (p. 1051).

Pasos para otorgar el permiso de automatización

1. En el cuadro de diálogo **Otorgar permisos de sistema obligatorios** para el diálogo Agente de Connect, haga clic en **Configurar permisos del sistema**.
2. En el cuadro de diálogo **Permisos de sistema**, haga clic en **Solicitar permiso de automatización**.

Cómo cambiar la cuenta de inicio de sesión en equipos Windows

En la pantalla **Seleccionar componentes**, 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.

  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.

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.

Privilegios necesarios para la cuenta de inicio de sesión

Los agentes de protección se ejecutan en un Managed Machine Service (MMS) de un equipo Windows. La cuenta con la que se ejecutará el agente debe tener derechos específicos para que el agente funcione correctamente. Por lo tanto, al usuario de MMS se le deberían asignar los siguientes privilegios:

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 otorgan permisos de **Control total** sobre la carpeta `%PROGRAMDATA%\Acronis` (en Windows XP y en Server 2003, `%ALLUSERSPROFILE%\Application Data\Acronis`) y en 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. Abra **Herramientas administrativas** del **Panel de control** (o haga clic en Win+R, escriba **herramientas de administración de control** y presione Intro) y abra **Política de seguridad local**.
3. Amplíe **Políticas locales** y haga clic en **Asignación de derechos de usuario.**
4. En el panel de la derecha, haga clic en **Inicio de 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 el usuario que quiera introducir y haga clic en **Aceptar**.
7. Haga clic en **Aceptar** en las propiedades **Inicio de 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**.

Tenga en cuenta que no es recomendable que cambie de cuentas de inicio de sesión manualmente cuando haya terminado la instalación.

Instalación dinámica y desinstalación de componentes

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

- Agente para el filtrado de URL: requerido para que funcione el filtrado de URL.
- Agente de protección antimalware: requerido para que funcione la protección antimalware.
- Agente para la prevención de pérdida de datos: requerido para que funcionen las características del 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 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 ya protección antimalware, filtrado de URL ni características del control de dispositivos, el correspondiente componente se desinstalará automáticamente.

La instalación o desinstalación dinámica de componentes tarda hasta 10 minutos después de cambiar el plan de protección. Sin embargo, si cualquiera de las siguientes operaciones se está ejecutando, la instalación o desinstalación dinámica comenzará cuando dicha operación termine:

- Copia de seguridad
- Recuperación
- Replicación de copias de seguridad
- Replicación 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

Instalación o desinstalación sin supervisión

Instalación o desinstalación sin supervisión 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. 93).

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. 93).

Ejemplos

- Instalar el agente para Windows, el agente antimalware, el agente para filtrado de URL, la herramienta de línea de comandos y el 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 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. 93).

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
   ```

   Para comprobar los parámetros disponibles y sus valores, consulte "Parámetros para una instalación desatendida (EXE)" (p. 93).

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.

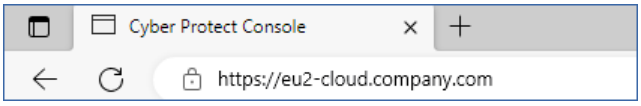
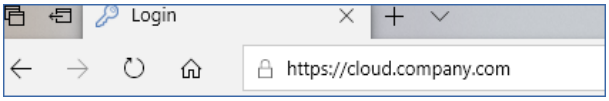
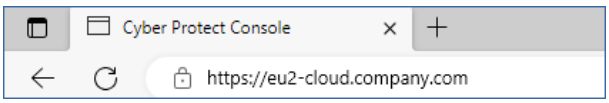
  ```
  C:\Program Files\Common Files\Acronis\BackupAndRecovery\Uninstaller.exe --anti-tamper-password=<password> --quiet --delete-all-settings
  ```

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. 98). 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.

Parámetros	Descripción
`--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`.
`--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.
Parámetros de registro	
`--registro=`{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

Parámetros	Descripción
	`--registration=by-credentials` sea opcional. Para registrar el agente con un token de registro, especifique `by-token` y utilice el parámetro `--reg-token`. 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

Parámetros	Descripción
	ser una cuenta de administrador de partners. Cuando use estos parámetros, especificar el parámetro `--registration` es opcional. 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. 173). 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. 88). 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	Descripción
Parámetros de vCenter/ESXi	
`--esxi-address=`<host>	El nombre del host o la dirección IP del vCenter Server o 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. 98). Si especifica varios componentes, sepárelos con comas. No añada espacios antes o después de la coma.

Parámetros	Descripción
	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**.
`--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. 93)"Parámetros para una instalación desatendida (MSI)" (p. 103)

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 contra malware y agente para 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

Nombre del valor	Descripción de componentes
`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.

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. 100). 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 "Implementación de agentes mediante la directiva de grupo" (p. 173).

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. 101).

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 desinstalación desatendida**.
2. En **Qué instalar**, seleccione los componentes que desea instalar y haga clic en **Listo**.
   Los paquetes de instalación de estos componentes se extraerán del programa de instalación como archivos CAB.
3. En **Configuración 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. 173).
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.

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 "Implementación de agentes mediante la directiva de grupo" (p. 173).

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. 99).
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. 99).

   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>
```

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. 103).

Ejemplos

- Instalar el agente para Windows, el agente antimalware, el agente para filtrado de URL, la herramienta de línea de comandos y el 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 "Contraseñas con caracteres especiales o espacios en blanco" (p. 127) 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.

```
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. 99).

   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. 103).

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. 99).

   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. 103).

Ejemplos

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

```
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
```

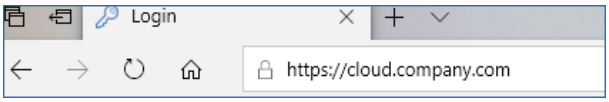
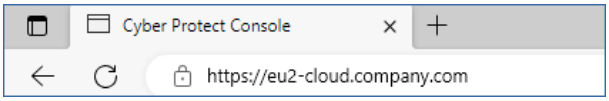
Parámetros para una instalación desatendida (MSI)

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. 107). 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. 99).
`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

Parámetros	Descripción
	componentes sin reiniciar el equipo.
`/l*v` <log file>	Especifique este parámetro para guardar un registro detallado. Este registro es necesario si tiene que 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}`	Utilice este parámetro para elegir si se debe comprobar que se ha instalado la actualización del soporte de firma de código SHA2 de Microsoft (KB4474419) en el equipo. La comprobación solo funciona en los sistemas operativos que requieren esta actualización. Para ver si es necesario para su sistema operativo, consulte "Sistemas operativos y entornos compatibles" (p. 23). Para omitir la verificación, establezca el valor `1` para este parámetro. 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.
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, `https://cloud.company.com`:

Parámetros	Descripción
	 • 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 "Contraseñas con caracteres especiales o espacios en blanco" (p. 127).
`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. 173). 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.
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**.

Parámetros	Descripción
	Para obtener más información sobre las cuentas de inicio de sesión, consulte "Cómo cambiar la cuenta de inicio de sesión en equipos Windows" (p. 88).
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=<nombre del servidor>	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={<list of components>|ALL}	Los componentes que se desinstalarán. 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.

Parámetros	Descripción
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=<contraseña>	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 para el parámetro ADDLOCAL. Para obtener más información, consulte "Parámetros para una instalación desatendida (MSI)" (p. 103).

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	BackupAndRecoveryAgent	32 bits / 64 bits
UrlFilteringAgentFeature	Agent for URL Filtering	BackupAndRecoveryAgent	32 bits / 64 bits
DlpAgentFeature	Agente para la prevención de la pérdida de datos	BackupAndRecoveryAgent	32 bits / 64 bits
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 o desinstalación sin supervisión 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.

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 (un archivo .i686 o .x86_64). Todos los parámetros disponibles y sus valores se describen en "Parámetros de instalación o desinstalación sin supervisión" (p. 110).
- 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
-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 activado en el equipo, se le informará de que debe reiniciar el sistema después de la instalación. Asegúrese de que recuerda qué contraseña (la del usuario root o "acronis") debe utilizar. Durante el reinicio del sistema, opte por la administración de la clave del propietario del equipo (MOK), elija **Registrar MOK** y, a continuación, registre la clave mediante la contraseña recomendada.

Si habilita el arranque seguro UEFI después de la instalación del agente, repita la instalación, incluido el paso 3. 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 (un archivo .i686 o .x86_64). Todos los parámetros disponibles y sus valores se describen en "Parámetros de instalación o desinstalación sin supervisión" (p. 110).

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.

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 .x86_64:

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

Sin este parámetro, se instalarán todos los componentes anteriores.

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

El paquete de instalación .i686 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=<ubicación>`

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

`--language=<ID de idioma>`

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, 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=}<nombre de usuario>` y `{-w|--password=}<contraseña>`

  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. Puede generar uno en la consola de Cyber Protect como se describe en "Implementación de agentes mediante la directiva de grupo".

  No puede usar el parámetro `--token` junto con los parámetros `--login`, `--password` y `--register-with-credentials`.

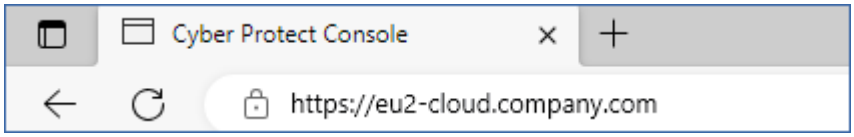
  - `{-C|--rain=}<dirección del servicio>`

    URL del servicio Cyber Protection.

    No es necesario que incluya este parámetro explícitamente cuando use los parámetros `--login` and `--password` para llevar a cabo el registro, porque el programa de instalación usa la dirección correcta de forma predeterminada y esta sería la que tiene que usar usted **para**

iniciar sesión en el servicio Cyber Protection. Por ejemplo:

Sin embargo, cuando use `{-C|--rain=}` con el parámetro `--token`, debe especificar la dirección exacta del centro de datos. Esta es la URL que ve **cuando ha iniciado sesión en** el servicio Cyber Protection. Por ejemplo:



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

- `--skip-registration`

Use este parámetro si tiene que instalar el agente y lo va a registrar más adelante en el servicio Cyber Protection. Para obtener más información sobre cómo hacerlo, consulte "Registro manual de equipos".

Parámetros adicionales

`--http-proxy-host=<dirección IP>` y `--http-proxy-port=<puerto>`

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=<nombre de usuario>` y `--http-proxy-password=<contraseña>`

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

`--tmp-dir=<ubicación>`

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.

`--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=}<ruta>`

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

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

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.

```
./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 sin supervisión e instalación en macOS

En esta sección se describe cómo instalar, registrar y desinstalar el agente de protección en el modo de 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. 116).

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 **Añadir** 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.
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

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. Se necesitan los siguientes permisos.

Requisitos para macOS 11 (Big Sur) y versiones posteriores

Pestaña	Sección	Campo	Valor

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

		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
		ACCESO	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
		ACCESO	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
		ACCESO	Permitir

	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
		ACCESO	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

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

		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
		ACCESO	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
		ACCESO	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
		ACCESO	Permitir

	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
		ACCESO	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	Extensiones del sistema del agente de ciberprotección de Acronis
		Tipos de extensiones del sistema	Identificadores de equipo permitidos

		Identificador de equipo	ZU2TV78AA6

Registro y anulación de registro manual de cargas de trabajo

Las cargas de trabajo se registran automáticamente en el servicio de Cyber Protection cuando instala en ellas el agente de protección. Cuando desinstale el agente de protección, se anulará automáticamente el registro de las cargas de trabajo y desaparecerán de la consola de Cyber Protect.

También puede registrar una carga de trabajo manualmente mediante la interfaz de líneas de comando. Es posible que deba usar el registro manual, por ejemplo, si falla el registro automático o si quiere mover una carga de trabajo a un nuevo inquilino o una nueva cuenta de usuario.

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

En Windows

En la línea de comando, 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:\ProgramFiles\BackupClient\RegisterAgentTool\register_agent.exe" -o register -t cloud
-a https://cloud.company.com -u johndoe -p johnspassword
```

En Linux

En la línea de comando, 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

En la línea de comando, 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
```

Nota
Utilice el nombre de usuario y la contraseña de la cuenta con la que quiere registrar la carga de trabajo. No puede ser una cuenta de administrador de partners.

La dirección del servicio es la URL que usa **para iniciar sesión** en el servicio Cyber Protection. Por ejemplo, `https://cloud.company.com`.

Importante
Si la contraseña contiene caracteres especiales o espacios en blanco, consulte "Contraseñas con caracteres especiales o espacios en blanco" (p. 127).

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.

Para registrar una carga de trabajo con un token de registro

En Windows

En la línea de comando, ejecute el siguiente comando:

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

Por ejemplo:

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

En Linux

En la línea de comando, 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

En la línea de comando, 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
```

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.

Virtual Appliance

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

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

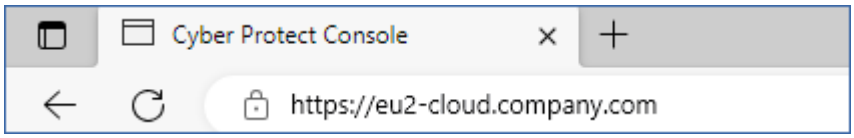
   Por ejemplo:

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

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

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 el** servicio de Cyber Protection. Por ejemplo, `https://eu2-cloud.company.com`.



No utilice `https://cloud.company.com` aquí.

El token de registro es una serie de 12 caracteres separados en tres segmentos por guiones. Para obtener más información sobre cómo generar uno, consulte "Generar un token de registro" (p. 173).

Para anular el registro de una carga de trabajo

En Windows

En la línea de comando, ejecute el siguiente comando:

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

Por ejemplo:

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

En Linux

En la línea de comando, ejecute el siguiente comando:

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

En macOS

En la línea de comando, 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 el símbolo del sistema, ejecute el siguiente comando:

   ```
   register_agent -o unregister
   ```

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

Mover una carga 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. 127).

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:

Plantilla de comando:

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

Ejemplo de comando:

```
"C:\ProgramFiles\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:

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

Cambio de registro de una carga de trabajo

Puede cambiar el registro actual 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.

Puede cambiar el registro de una carga de trabajo utilizando la línea de comando o el instalador de GUI. Cuando utiliza la línea de comando, no es necesario que desinstale el agente.

Cómo cambiar el registro de una carga de trabajo

Mediante la línea de comando

1. Anule el registro del agente de protección como se describe en "Para anular el registro de una carga de trabajo" (p. 126).
2. Registre el agente de protección en el nuevo inquilino o con la nueva cuenta de usuario como se describe en "Para registrar una carga de trabajo con un nombre de usuario y una contraseña" (p. 123) o "Para registrar una carga de trabajo con un token de registro" (p. 124).

Mediante el instalador de GUI

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" (p. 79).

Autodetección de equipos

Con la autodetección, puede:

- 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 y actualizar agentes de protección en varios equipos.
- 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.

Requisitos previos

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.

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.

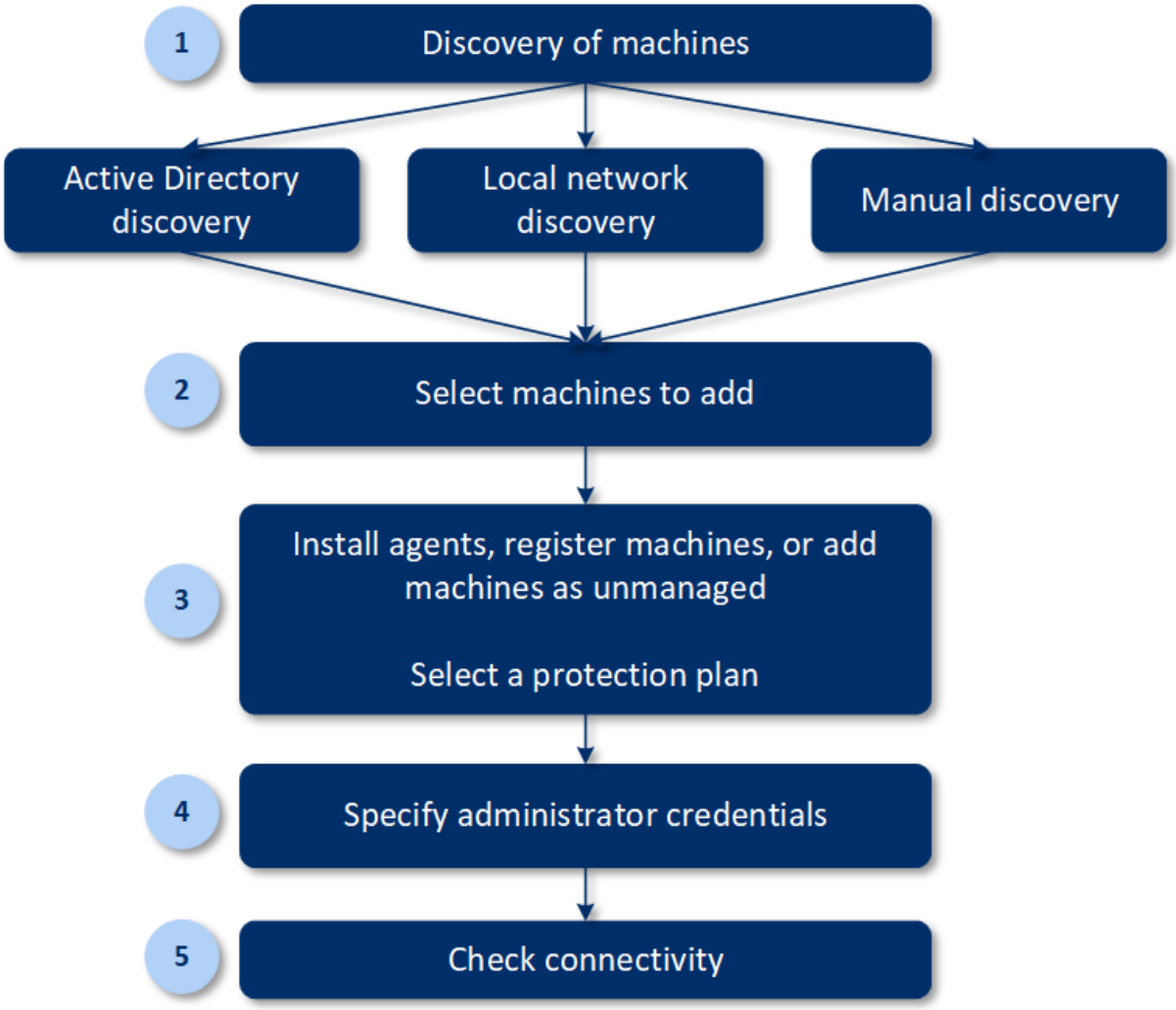
Cómo funciona la autodetección

Durante una detección de red local, el agente de detección recopila la siguiente información de cada equipo de la red mediante la detección de NetBIOS, Web Service Discovery (WSD) y la tabla del Protocolo de resolución de direcciones (ARP):

- Nombre (nombre corto del servidor o de NetBIOS)
- Nombre de dominio totalmente cualificado (FQDN)
- Dominio/grupo de trabajo
- Direcciones IPv4/IPv6
- Direcciones MAC
- Sistema operativo (nombre/versión/familia)
- Categoría del equipo (estación de trabajo/servidor/controlador de dominio)

Durante un análisis de Active Directory, el agente de detección, además de la lista anterior, recopila información sobre la unidad organizativa (UO) de los equipos e información más detallada sobre su nombre y sistema operativo. Sin embargo, no recopila las direcciones IP y MAC.

En el siguiente diagrama se resume el proceso de autodetección.



1. Seleccione el método de detección:
   - Detección de Active Directory
   - Detección de redes locales
   - Detección manual: si se utiliza la dirección IP de un equipo o el nombre del servidor, o si se importa una lista de equipos desde un archivo

   Los resultados de una detección de Active Directory o una red local excluyen los equipos con agentes de protección instalados.

   Durante una detección manual, los agentes de protección existentes se actualizan y se vuelven a registrar. Si ejecuta la autodetección empleando la misma cuenta en la que está registrado el agente, este solo se actualizará a la versión más reciente. Si utiliza otra cuenta para ejecutar la autodetección, el agente se actualizará a la versión más reciente y volverá a registrarse bajo el inquilino propietario de la cuenta.
2. Seleccione los equipos que desea añadir a su inquilino.
3. Seleccione cómo añadir estos equipos:
   - 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 **Equipos sin gestionar** sin instalar ningún agente de protección.

También puede aplicar un plan de protección existente a los equipos en los que instale un agente de protección o que haya registrado en la consola de Cyber Protect.

4. Proporcione las credenciales de administrador para los equipos seleccionados.
5. Compruebe que puede conectarse a los equipos con las credenciales proporcionadas.

Los equipos que se muestran en la consola de Cyber Protect pertenecen a las siguientes categorías:

- **Detectado**: equipos que se han detectado, pero en los que no está instalado un agente de protección.
- **Gestionado**: equipos en los que está instalado un agente de protección.
- **Sin protección**: equipos en los que no está aplicado un plan de protección. Los equipos sin protección incluyen tanto a los equipos detectados como a los gestionados en los que no hay ningún plan de protección aplicado.
- **Protegido**: equipos en los que está aplicado un plan de protección.

Cómo funciona la instalación remota de agentes

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 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.

Ejecutar la autodetección y la detección manual

Antes de comenzar la detección, asegúrese de que se cumplen los requisitos previos.

Nota
La autodetección no se admite para añadir controladores de dominio debido a que son necesarios otros permisos para que se ejecute el servicio de agente.

Pasos para detectar equipos

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 **Solo Windows**. Se abre el asistente de autodetección.
4. [Si hay unidades en su organización] Seleccione una unidad. A continuación, en **Agente de detección**, podrá seleccionar los agentes asociados a la unidad seleccionada y sus unidades secundarias.
5. Seleccione el agente de detección que llevará a cabo el análisis para detectar equipos.
6. Seleccione el método de detección:
   - **Buscar en Active Directory**. Asegúrese de que el equipo con el agente de detección esté en el miembro del dominio de Active Directory.
   - **Analizar red local**. Si el agente de detección seleccionado no encuentra ningún equipo, seleccione otro agente de detección.
   - **Especificar manualmente o importar desde un archivo**. Defina manualmente los equipos que quiere añadir o impórtelos desde un archivo de texto.
7. [Si se ha seleccionado el método de detección Active Directory] Seleccione cómo buscar equipos:
   - **En lista de unidades organizativas**. Seleccione el grupo de equipos que se va a añadir.
   - **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 **Filtrar** le permite especificar el criterio de selección de los equipos.
8. Dependiendo del método de detección que haya seleccionado, realice una de las siguientes acciones:

Método de detección	Acción
Buscar en Active Directory	En la lista de máquinas detectadas, seleccione las máquinas que desee añadir.
Analizar red local	En la lista de máquinas detectadas, seleccione las máquinas que desee añadir.

Especificar manualmente o importar desde un archivo	Especifique las direcciones IP o los nombres de host de las máquinas, o importe la lista de máquinas desde un archivo de texto. El archivo debe contener direcciones IP o nombres de host, uno por línea. Aquí le mostramos un ejemplo:
	`156.85.34.10`
	`156.85.53.32`
	`156.85.53.12`
	`EN-L00000100`
	`EN-L00000101`
	Cuando ya se han añadido las direcciones de los equipos manualmente o se han importado de un archivo, el agente intenta anclar los equipos añadidos y definir su disponibilidad.

9. Seleccione las acciones que deben realizarse después de la detección:

Opción	Descripción
Instalar agentes y registrar máquinas	Para seleccionar qué componentes desea instalar en las máquinas, haga clic en **Seleccionar componentes**. Para obtener más información, consulte "Selección de componentes para la instalación" (p. 136).
Cuenta de inicio de sesión para el servicio de agente	Esta configuración está disponible en la pantalla **Seleccionar componentes**. La configuración define la cuenta desde la que se ejecutarán los servicios. 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. Si elige la opción **Crear una cuenta nueva** o **Utilice la siguiente cuenta**, asegúrese de que las políticas de seguridad del dominio no afecten los derechos de las cuentas relacionadas. Si a una cuenta se le priva de los derechos de usuario asignados durante la instalación, el componente podría funcionar incorrectamente o no funcionar en absoluto.
Registrar máquinas con agentes instalados	Utilice esta opción si el agente ya está instalado en las máquinas y solo necesita registrarlas en Cyber Protection. Si no se encuentra ningún agente en las máquinas, se añadirán como máquinas **No administradas**.
Añadir como máquinas no administradas	Si selecciona esta opción, el agente no se instalará en las máquinas. Podrás verlas en la consola e instalar o registrar el agente más tarde.
Reiniciar la máquina si es necesario	Esta opción aparece cuando se selecciona **Instalar agentes y registrar máquinas**. Si selecciona esta opción, la máquina se reiniciará tantas veces como sea necesario para completar la instalación. Se puede requerir que se reinicie el equipo en uno de los siguientes casos: • La instalación de los requisitos previos se ha completado, y es necesario reiniciar para continuar con la instalación. • La instalación se ha completado, pero es necesario reiniciar, ya que algunos archivos han quedado bloqueados durante la instalación.

Opción	Descripción
	• La instalación se ha completado, pero es necesario reiniciar para el correcto funcionamiento de otro software previamente instalado.
No reiniciar si el usuario ha iniciado sesión	Esta opción aparece cuando se selecciona **Reiniciar la máquina si es necesario**. Al seleccionar esta opción, la máquina no se reiniciará automáticamente si el usuario ha iniciado sesión en el sistema. Por ejemplo, si un usuario está trabajando mientras la instalación requiere un reinicio, el sistema no se reiniciará. Si los requisitos previos se han instalado pero la máquina no se ha reiniciado porque un usuario había iniciado sesión, debe reiniciar la máquina y volver a iniciar la instalación para que esta pueda completarse. Si el agente se ha instalado pero no se ha reiniciado la máquina a continuación, debe reiniciar la máquina.
Usuario donde registrar las máquinas	[Si hay unidades en su organización] Seleccione la cuenta de usuario de la unidad o unidades subordinadas en las que desea registrar las máquinas. [Al ejecutar la autodetección en el nivel de inquilino partner] En la lista de inquilinos de cliente que administra, expanda la estructura de árbol y, a continuación, seleccione la cuenta de usuario en la que desea registrar las máquinas. [Al ejecutar la autodetección como administrador del cliente] Si ha seleccionado **Instalar agentes y registrar máquinas** o **Registrar máquinas con agentes instalados**, también existe la opción de aplicar el plan de protección a las máquinas. Si dispone de varios planes de protección, puede seleccionar cuál desea usar.

10. Especifique las credenciales del usuario con derechos de administrador para todos los equipos.

Importante
Tenga en cuenta que la instalación remota de agentes funciona sin ninguna preparación únicamente si especifica las credenciales en la cuenta de administrador integrada (la primera cuenta que se creó cuando asistan al sistema operativo). Si desea definir credenciales de administrador personalizadas, tiene que realizar preparaciones manuales adicionales como se describe en "Preparar un equipo para la instalación remota" (p. 134).

11. El sistema comprueba la conectividad a todos los equipos. Si la conexión a alguno de los equipos falla, puede cambiar las credenciales de esos equipos.

Cuando se inicie la detección de equipos, verá la tarea correspondiente en la actividad **Supervisión** > **Actividades** > **Detección de equipos**.

Preparar un equipo para la instalación remota

- 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** > **Windows Firewall** > **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.

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

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**

Selección de componentes para la instalación

En la siguiente tabla encontrará la descripción de los componentes obligatorios y los adicionales:

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	Este componente habilita el módulo de 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.
Agente para Hyper-V	Este agente realiza copias de seguridad de equipos virtuales Hyper-V y se instalará en servidores 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 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 y 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 y 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 equipos virtuales VMware y 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 y se instalará en máquinas Windows. Se instalará si se selecciona.
Agente para Oracle	Este agente realiza copias de seguridad de bases de datos Oracle y se instalará en equipos que ejecuten Oracle Database. Se instalará si se selecciona.
Cyber Protection Monitor	Este componente permite a un usuario supervisar las 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.

Gestión de equipos detectados

Cuando finalice el proceso de detección, encontrará todos los equipos detectados en **Dispositivos** > **Equipos sin gestionar**.

Esta sección se divide en dos subsecciones según el método de detección empleado. A continuación, encontrará una lista completa con los parámetros de los equipos (puede variar en función del método de detección):

Nombre	Descripción
Nombre	El nombre del equipo. La dirección IP se mostrará si no se puede detectar el nombre del equipo.
Dirección IP	La dirección IP del equipo.
Tipo de detección	El método de detección empleado para detectar el equipo.
Unidad	La unidad organizativa de Active Directory a la que pertenece el equipo. Esta columna

organizativa	se muestra si ve la lista de equipos en **Equipos sin gestionar** > **Active Directory**.
Sistema operativo	El sistema operativo instalado en el equipo.

Existe otra sección llamada **Excepciones** en la que se pueden añadir los equipos que se deban omitir durante el proceso de detección. Por ejemplo, si no necesita que se detecten los equipos exactos, puede añadirlos a esta lista.

Para añadir un equipo a **Excepciones**, selecciónelo en la lista y haga clic en **Añadir a excepciones**. Para eliminar un equipo de **Excepciones**, vaya a **Equipos sin gestionar** > **Excepciones**, seleccione el equipo y haga clic en **Eliminar de las excepciones**.

Puede instalar el agente de protección y registrar un lote de equipos detectados en Cyber Protection si los selecciona en la lista y hace clic en **Instalar y registrar**. Con el asistente de instalación que se ha abierto podrá asignar el plan de protección a un lote de equipos.

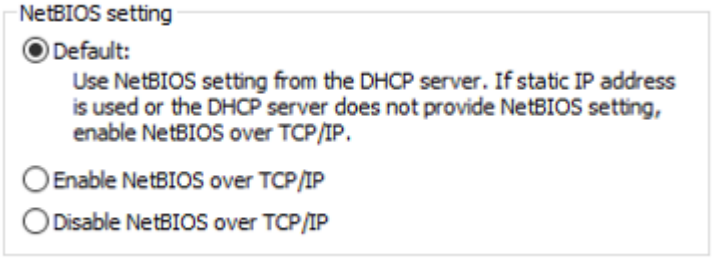
Cuando el agente de protección esté instalado en los equipos, estos aparecerán en la sección **Dispositivos** > **Equipos con agentes**.

Para comprobar el estado de su protección, vaya a **Supervisión** > **Información general** y añada uno de estos widgets: **Estado de la protección** o **Equipo detectado**.

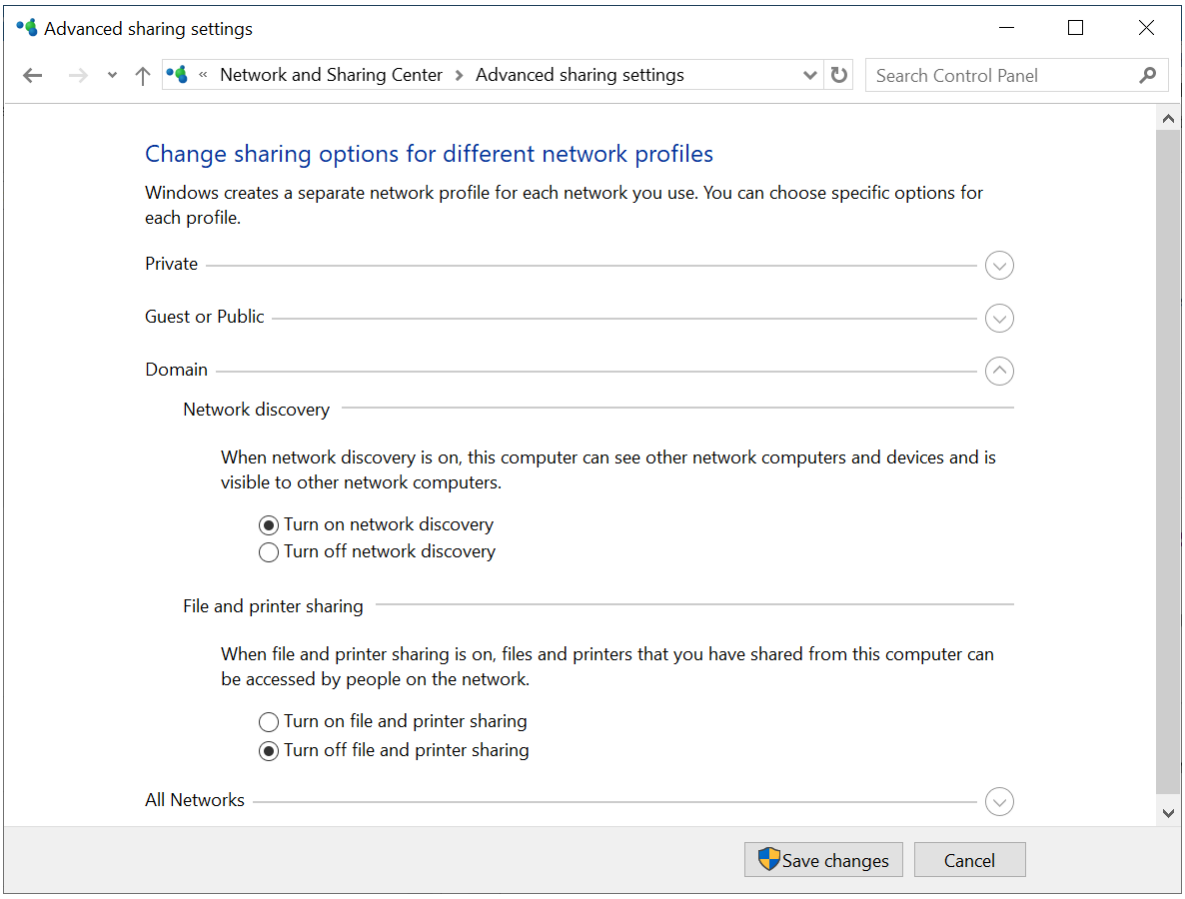
Solución de problemas

Si tiene algún problema relacionado con la funcionalidad de autodetección, intente comprobar lo siguiente:

- Compruebe que NetBIOS en TCP/IP esté habilitado o establecido como predeterminado.



- En "Panel de control\Centro de redes y recursos compartidos\Configuraciones compartidas avanzadas", active la detección de redes.



- Compruebe que el servicio Function Discovery Provider Host se esté ejecutando en el equipo que se encarga de las detecciones y en los equipos que se van a detectar.
- Compruebe que el servicio Function Discovery Resource Publication se esté ejecutando en los equipos que se van a detectar.

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 un almacenamiento conectado localmente" (p. 731).

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**.

Implementación de la plantilla OVF

1. Haga clic en**Todos los dispositivos** > **Añadir** > **VMware ESXi** > **Dispositivo virtual (OVF)**.
   El archivo .zip se descarga en su equipo.
2. Descomprímalo. La carpeta contiene un archivo .ovf y dos 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 **Cambiar** 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 **Cambiar** 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.

        Le recomendamos utilizar una cuenta dedicada para acceder al host de vCenter Server o ESXi en lugar de utilizar una cuenta existente con el rol de Administrador. Para obtener más información acerca de los privilegios necesarios para la cuenta dedicada, consulte "Agente para VMware: privilegios necesarios" (p. 738).
   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.
   - [Solo para inquilinos sin autenticación de doble factor] Registre el dispositivo en su interfaz gráfica.
     a. En **Opciones del agente**, en el campo **Servidor de administración**, haga clic en **Cambiar**.
     b. En el campo **Nombre del servidor o IP**, seleccione **Nube**.

        Aparecerá la dirección del servicio Cyber Protection. 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 en el servicio Cyber Protection. El dispositivo virtual y las máquinas virtuales que gestiona el dispositivo están registrados en esta cuenta.
     d. Haga clic en **Aceptar**.
   - Registre el dispositivo en la interfaz de la línea de comandos.

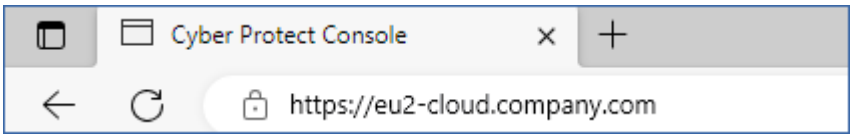
Nota
Con este método, necesita un token de registro. Para obtener más información sobre cómo generar uno, consulte "Generar un token de registro" (p. 173).

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>
```

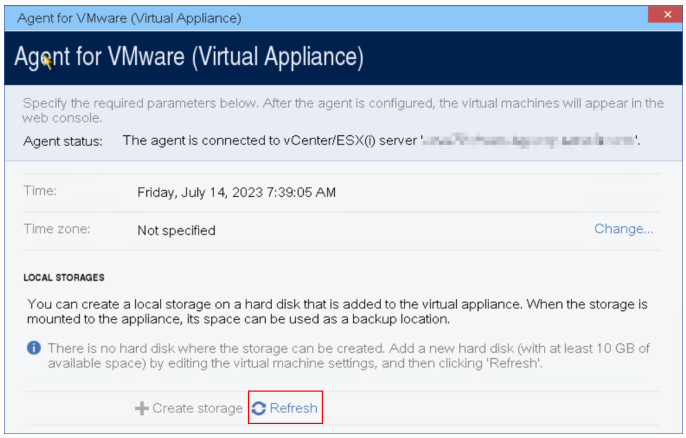
Nota
Cuando use un token de registro, debe especificar la dirección exacta del centro de datos. Esta es la URL que ve **al iniciar sesión** en la consola de Cyber Protect. Por ejemplo, `https://eu2-cloud.company.com`.



No utilice `https://cloud.company.com` aquí.

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

5. [Opcional] Añada almacenamiento local.
   a. En vSphere Client, adjunte un disco virtual al dispositivo virtual. El disco virtual debe tener al menos 10 GB de espacio libre.
   b. En la interfaz gráfica de usuario del dispositivo, haga clic en **Actualizar**.



   Se activará el botón **Crear almacenamiento**.
   c. Haga clic en **Crear almacenamiento**.
   d. Especifique una etiqueta para el almacenamiento y haga clic en **Aceptar**.
   e. Haga clic en **Sí** para confirmar su elección.
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:

   ```
   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.

¿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** > **Añadir** > **Scale Computing HC3**.
   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. 148).
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:
      - 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. 145).

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 **Cambiar** 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. 148).
   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.
   - [Solo para inquilinos sin autenticación de doble factor] Registre el dispositivo en su interfaz gráfica.
     a. En **Opciones del agente**, en el campo **Servidor de administración**, haga clic en **Cambiar**.
     b. En el campo **Nombre del servidor o IP**, seleccione **Nube**.

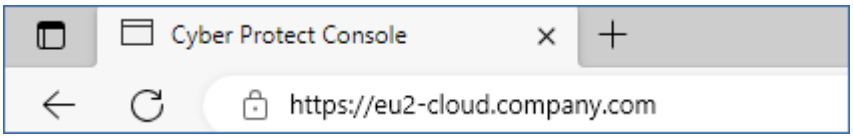
        Aparecerá la dirección del servicio Cyber Protection. No cambie esta dirección a menos que se le indique lo contrario.
     c. En los campos **Nombre de usuario** y **Contraseña**, especifique las credenciales de su cuenta en el servicio Cyber Protection. El dispositivo virtual y las máquinas virtuales que gestiona el dispositivo están registrados en esta cuenta.
     d. 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. 173).

     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 **Cambiar** 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 **Cambiar** y seleccione la zona horaria de su ubicación para asegurar que las operaciones planificadas se ejecutan en el momento apropiado.
8. [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`.

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 HC3**> <su clúster>, 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

	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 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 la Virtuozzo Hybrid Infrastructure. Dicha cuenta debe tener asignada la función de **Administrador** en el dominio **Predeterminado**. Para obtener más información acerca de los usuarios, consulte Gestionar los usuarios del panel de administración en la documentación de Virtuozzo Hybrid Infrastructure.

Asegúrese de haber otorgado a esta cuenta acceso a todos los proyectos del dominio **Predeterminado**.

Otorgar acceso a todos los proyectos del dominio Predeterminado

1. Cree un archivo de entorno para el administrador del sistema. Para ello, ejecute el siguiente script en el clúster de Virtuozzo Hybrid Infrastructure mediante la interfaz OpenStack Command-Line. Para obtener más información sobre cómo conectarse a esta interfaz, consulte Conectarse a la interfaz OpenStack Command-Line en la documentación de la Virtuozzo Hybrid Infrastructure.

   ```
   su - vstoradmin
   kolla-ansible post-deploy
   exit
   ```

2. Utilice el archivo de entorno para autorizar más comandos de OpenStack:

   ```
   . /etc/kolla/admin-openrc.sh
   ```

3. Ejecute los siguientes comandos:

   ```
   openstack --insecure user set --project admin --project-domain Default --domain
   Default <username>
   openstack --insecure role add --domain Default --user <username> --user-domain
   Default compute --inherited
   ```

   Aquí, <username> es la cuenta de la Virtuozzo Hybrid Infrastructure que tiene asignada la función de **Administrador** en el dominio **Predeterminado**. El dispositivo virtual utilizará esta cuenta para realizar la copia de seguridad y restaurar los equipos virtuales de cualquier proyecto secundario en el dominio **Predeterminado**.

Ejemplo

```
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
```

Para gestionar las copias de seguridad de los equipos virtuales de un dominio diferente al **Predeterminado**, ejecute también el siguiente comando.

Otorgar acceso a todos los proyectos de un dominio diferente

```
openstack --insecure role add --domain <domain name> --inherited --user <username> --
user-domain Default admin
```

Aquí, <domain name> es el dominio de los proyectos al que la cuenta <username> tendrá acceso.

Ejemplo

```
openstack --insecure role add --domain MyNewDomain --inherited --user johndoe --user-
domain Default admin
```

Después de conceder acceso a los proyectos, compruebe qué roles se asignan a la cuenta.

Pasos para comprobar los roles asignados

```
openstack --insecure role assignment list --user <username> --names
```

Aquí, <username> es la cuenta de Virtuozzo Hybrid Infrastructure.

Ejemplo

```
openstack --insecure role assignment list --user johndoe --names -c Role -c User -c
Project -c Domain
+--------------+-----------------+---------+-------------+
| Role         | User            | Project | Domain      |
+--------------+-----------------+---------+-------------+
| admin        | johndoe@Default |         | MyNewDomain |
| 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.

Para comprobar qué roles efectivos se asignan a la cuenta de todos los proyectos, ejecute también el siguiente comando.

Pasos para comprobar los roles efectivos de todos los proyectos

```
openstack --insecure role assignment list --user <username> --names --effective
```

Aquí, <username> es la cuenta de Virtuozzo Hybrid Infrastructure.

Ejemplo

```
openstack --insecure role assignment list --user johndoe --names --effective  -c Role -c
User -c Project -c Domain
+--------------+-----------------+-----------------+---------+
| Role         | User            | Project         | Domain  |
+--------------+-----------------+-----------------+---------+
| domain_admin | johndoe@Default |                 | Default |
| compute      | johndoe@Default | admin@Default   |         |
```

```
| compute      | johndoe@Default | service@Default |         |
| domain_admin | johndoe@Default | admin@Default   |         |
| domain_admin | johndoe@Default | service@Default |         |
| project_user | johndoe@Default | service@Default |         |
| member       | johndoe@Default | service@Default |         |
| reader       | johndoe@Default | service@Default |         |
| project_user | johndoe@Default | admin@Default   |         |
| member       | johndoe@Default | admin@Default   |         |
| reader       | johndoe@Default | admin@Default   |         |
| project_user | johndoe@Default |                 | Default |
| member       | johndoe@Default |                 | Default |
| reader       | johndoe@Default |                 | Default |
+--------------+-----------------+-----------------+---------+
```

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

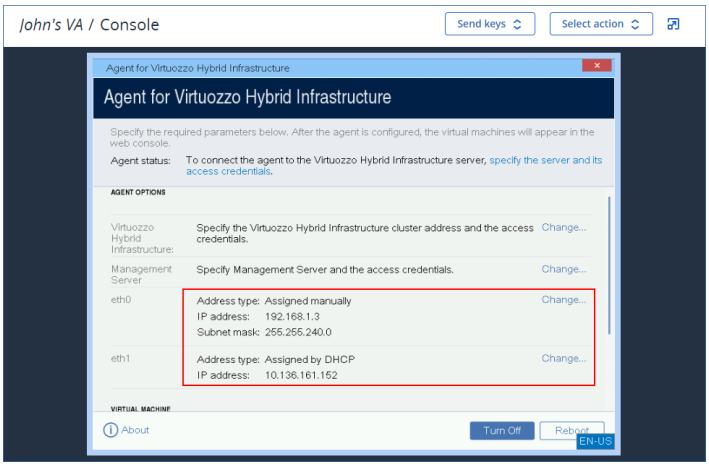
1. Inicie sesión en su cuenta de Cyber Protection.
2. Haga clic en **Dispositivos** > **Todos los dispositivos** > **Añadir** > **Virtuozzo Hybrid Infrastructure**.
   El archivo .zip se descarga en su equipo.
3. Descomprímalo. Contiene un archivo de imagen .qcow2.
4. Inicie sesión en su cuenta de la 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 **Añadir**.
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 **Añadir**, seleccione la red virtual de tipo *público* y, a continuación, haga clic en **Añadir**. Aparecerá en la lista de **Interfaces de red**.
     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

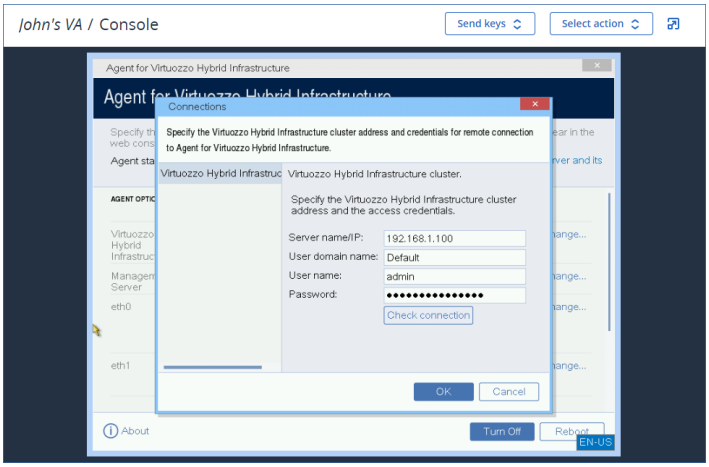
Después de implementar el agente para Virtuozzo Hybrid Infrastructure (dispositivo virtual), debe configurarlo de modo que pueda alcanzar tanto el clúster de Virtuozzo Hybrid Infrastructure que protegerá como el servicio en la nube de Cyber Protection.

Para configurar la aplicación virtual

1. Inicie sesión en su cuenta de la Virtuozzo Hybrid Infrastructure.
2. En la pestaña **Procesamiento** > **Equipos virtuales** > **Equipos virtuales**, seleccione el equipo virtual que ha creado. A continuación, haga clic en **Consola**.
3. Configure las interfaces de red del dispositivo. Puede haber una o más interfaces a configurar, 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.



4. Especifique la dirección y las credenciales del clúster de Virtuozzo:
   - Nombre DNS o dirección IP del clúster de la 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 el campo **Dominio de usuario**, especifique su dominio en la Virtuozzo Hybrid Infrastructure. Por ejemplo, **Predeterminado**.
     El nombre del dominio distingue entre mayúsculas y minúsculas.
   - En los campos **Nombre de usuario** y **Contraseña**, introduzca las credenciales de la cuenta de usuario de la Virtuozzo Hybrid Infrastructure que tenga asignada la función **Administrador** en el dominio especificado. Para obtener más información sobre usuarios, funciones y dominios, consulte Configurar cuentas de usuario en la Virtuozzo Hybrid Infrastructure.



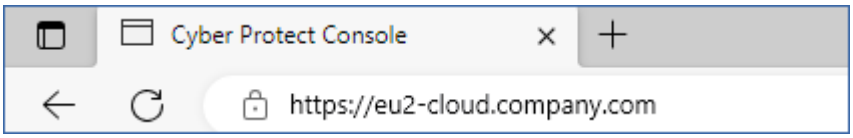
5. Registre el dispositivo en el servicio de Cyber Protection mediante uno de los siguientes métodos.
   - [Solo para inquilinos sin autenticación de doble factor] Registre el dispositivo en su interfaz gráfica.
     a. En **Opciones del agente**, en el campo **Servidor de administración**, haga clic en **Cambiar**.
     b. En el campo **Nombre del servidor o IP**, seleccione **Nube**.
        Aparecerá la dirección del servicio Cyber Protection. 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 en el servicio Cyber Protection. El dispositivo virtual y las máquinas virtuales que gestiona el dispositivo están registrados en esta cuenta.
     d. 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. 173).

     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. [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`.

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>
```

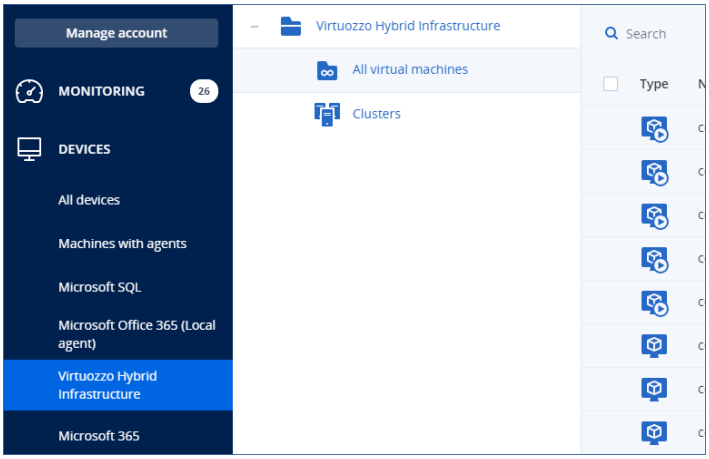
Por ejemplo:

```
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 su cuenta de Cyber Protection.
2. Vaya a **Dispositivos** > **Virtuozzo Hybrid Infrastructure** > <su clúster> > **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 se implementa en el centro de datos de Red Hat Virtualization/oVirt. El dispositivo contiene un agente de protección que le permite administrar la ciberprotección de todas las máquinas virtuales del centro de datos.

Requisitos del sistema para el agente

De forma predeterminada, la máquina virtual que contiene el agente utiliza 2 vCPU y 4 GiB de RAM. Esta configuración es suficiente para la mayoría de operaciones, pero puede editarla en el Portal de administración de Red Hat Virtualization/oVirt.

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 8 GiB.

¿Cuántos agentes necesito?

Un agente puede proteger todo el centro de datos. Sin embargo, puede tener más de un agente en el centro de datos si necesita distribuir la carga del ancho de banda del tráfico de copias de seguridad.

Si tiene más de un agente en un centro de datos, las máquinas virtuales se distribuyen automáticamente entre ellos, de modo que cada agente gestiona 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 centro de datos. El servidor de gestión asignará los equipos más adecuados al nuevo agente. La carga de los agentes anteriores se reducirá. Cuando retira un agente, 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 Portal de administración de Red Hat Virtualization/oVirt. 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 **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

1. Inicie sesión en su cuenta de Cyber Protection.
2. Haga clic en **Dispositivos** > **Todos los dispositivos** > **Añadir** > **Red Hat Virtualization (oVirt)**. El archivo .zip se descarga en su equipo.
3. Descomprímalo. Contiene un archivo .ova.
4. Cargue el archivo .ova a un servidor del centro de datos de Red Hat Virtualización/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. 163).
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 **Fuente**, seleccione **Dispositivo Virtual (OVA)**.

c. En **Servidor**, seleccione el servidor 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.
   - [Opcional] En la pestaña **General**, cambie el nombre predeterminado de la máquina virtual con el agente.

La implementación se completará. A continuación, debe configurar el dispositivo virtual. Para obtener más información sobre cómo hacerlo, consulte "Configuración del dispositivo virtual" (p. 160).

Nota
Si necesita más de un dispositivo virtual en su centro de datos, repita los pasos anteriores e implemente dispositivos virtuales adicionales. No clone un dispositivo virtual existente mediante la opción **Clonar máquina virtual** del Portal de administración de Red Hat Virtualización/oVirt.

Para excluir el dispositivo virtual de las copias de seguridad de un grupo dinámico, deberá excluirlo también de la lista de máquinas virtuales de la consola de Cyber Protect. Para excluirlo, seleccione la máquina virtual con el agente en el Portal de administración de Red Hat Virtualización/oVirt y, a continuación, asígnele la etiqueta `acronis_virtual_appliance`.

Configuración del dispositivo virtual

Después de implementar el dispositivo virtual, debe configurarlo de modo que pueda alcanzar tanto el motor oVirt 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 **Cambiar** para especificar la dirección del motor oVirt 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 Virtualización/oVirt. Para obtener más información sobre estos roles, consulte "Agente para oVirt: roles y puertos necesarios" (p. 163).

      Si Keycloak es el proveedor de inicio de sesión único (SSO) para el motor oVirt (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.
   - [Solo para inquilinos sin autenticación de doble factor] Registre el dispositivo en su interfaz gráfica.
     a. En **Opciones del agente**, en el campo **Servidor de administración**, haga clic en **Cambiar**.
     b. En el campo **Nombre del servidor o IP**, seleccione **Nube**.

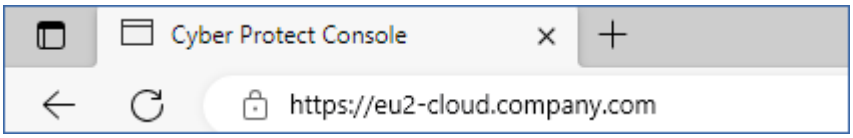
        Aparecerá la dirección del servicio Cyber Protection. No cambie esta dirección a menos que se le indique lo contrario.
     c. En los campos **Nombre de usuario** y **Contraseña**, especifique las credenciales de su cuenta en el servicio Cyber Protection. El dispositivo virtual y las máquinas virtuales que gestiona el dispositivo están registrados en esta cuenta.
     d. 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. 173).

     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 **Cambiar** 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 **Cambiar** 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.
   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 Virtualización/oVirt

1. Inicie sesión en su cuenta de Cyber Protection.
2. Vaya a **Dispositivos** > **oVirt**> <su clúster>, o busque sus máquinas en **Dispositivos** > **Todos los dispositivos**.
3. Seleccione los equipos y aplíqueles un plan de protección.

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

Puertos necesarios

El Agente para oVirt se conecta al motor oVirt 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 del motor de oVirt	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.

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 copia de seguridad, validación y limpieza. Para obtener más información acerca de estas operaciones, consulte "Procesamiento de datos fuera del host" (p. 205).

Nota
El Agente para Synology solo admite dispositivos NAS con procesadores x86_64. Los procesadores ARM no son compatibles.

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 incluir 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

* 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.

Limitaciones

- El Agente para Synology solo admite dispositivos NAS con procesadores x86_64. Los procesadores ARM no son compatibles.
- 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 Cyber Protect, vaya a **Dispositivos** > **Todos los dispositivos**.
2. En la esquina superior derecha, haga clic en **Añadir**.

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 Cyber Protect, vaya a **Dispositivos** > **Todos los dispositivos**.
2. En la esquina superior derecha, haga clic en **Añadir**.
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.

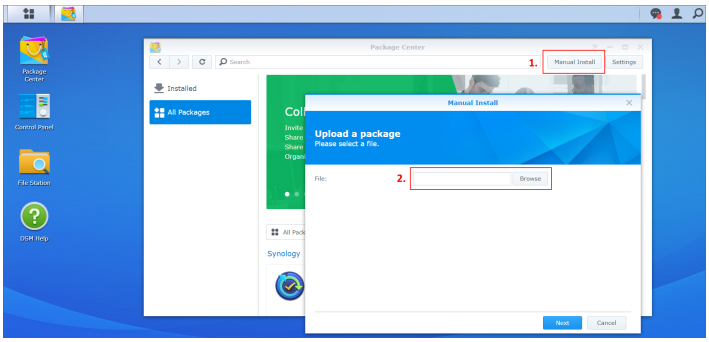
Agente para Synology 7.x

Requisitos previos

- 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.

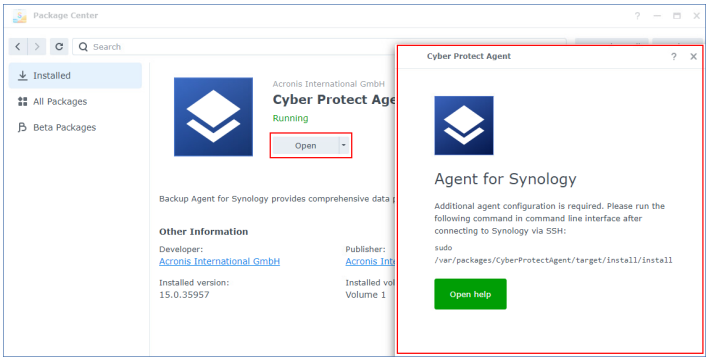
Pasos para instalar Agente para Synology

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**.

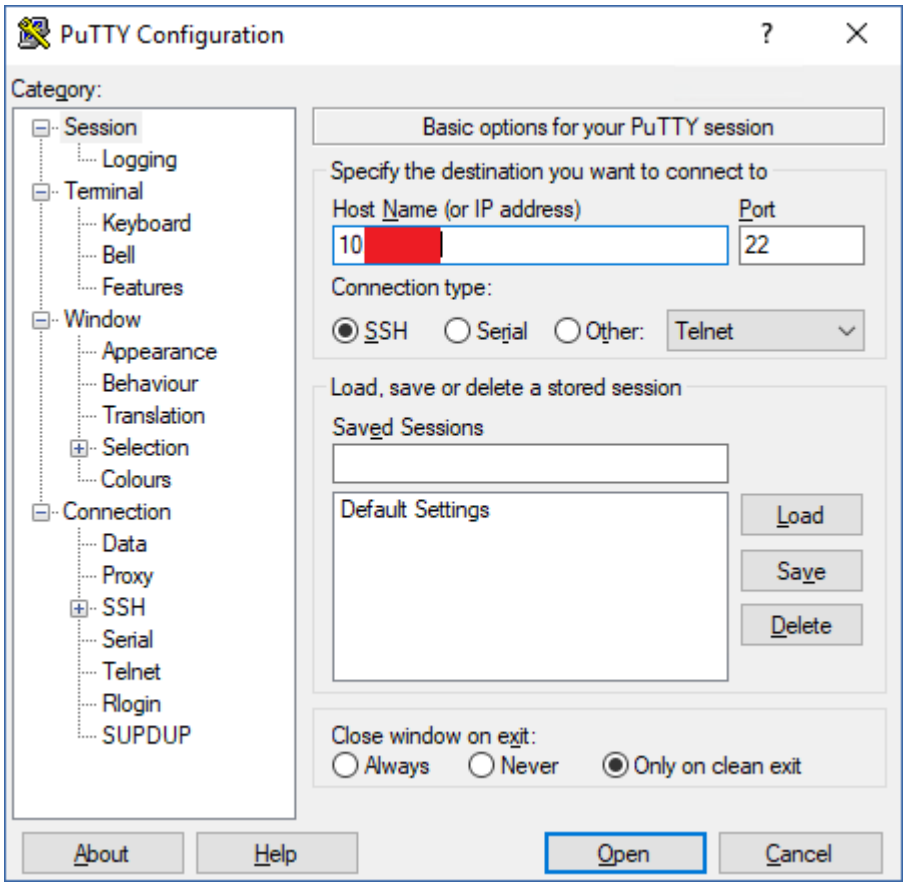
   Se muestra una advertencia de que va a instalar un paquete de software de terceros. Este mensaje forma parte del procedimiento de instalación estándar.
5. Para confirmar que desea instalar el paquete, haga clic en **Aceptar**.
6. Seleccione el volumen en el que desee instalar el agente y, a continuación, 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.



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.



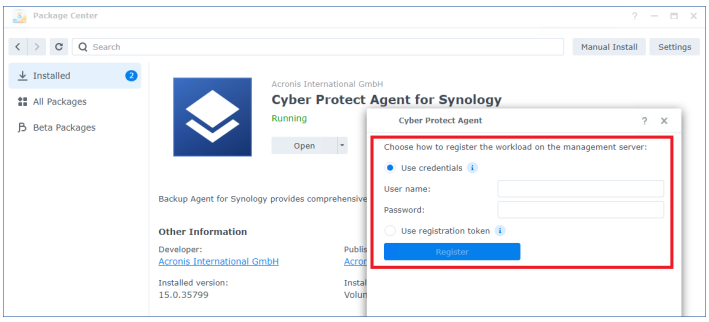
b. Haga clic en **Abrir** e inicie sesión como administrador de Synology DSM.

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.



- [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. 173).

14. Haga clic en **Registrar**.

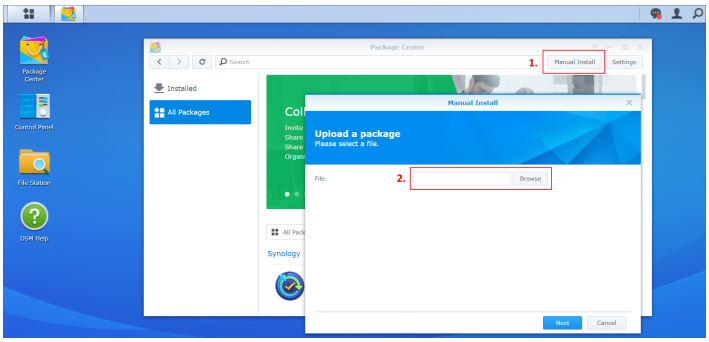
Agente para Synology 6.x

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

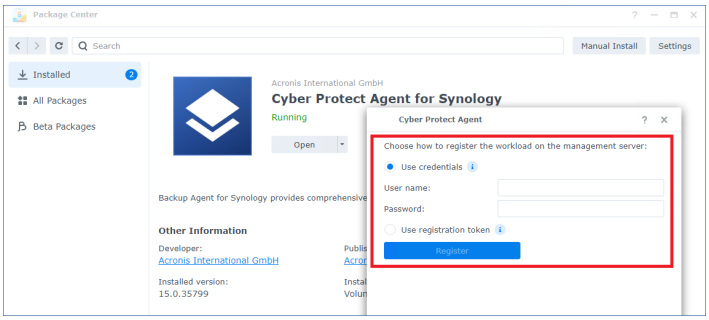
1. Inicie sesión en Synology DiskStation Manager.
2. Abra el **Centro de paquetes**.
3. Haga clic en **Instalación manual** y, a continuación, haga clic en **Examinar**.



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.

    Para obtener más información sobre cómo generar un token de registro, consulte "Generar un token de registro" (p. 173).

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.

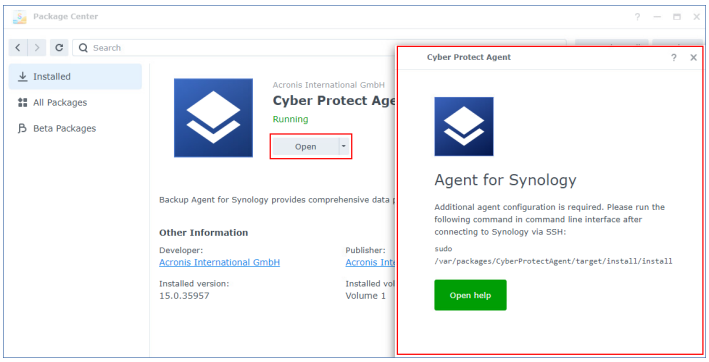
Agente para Synology 7.x

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.

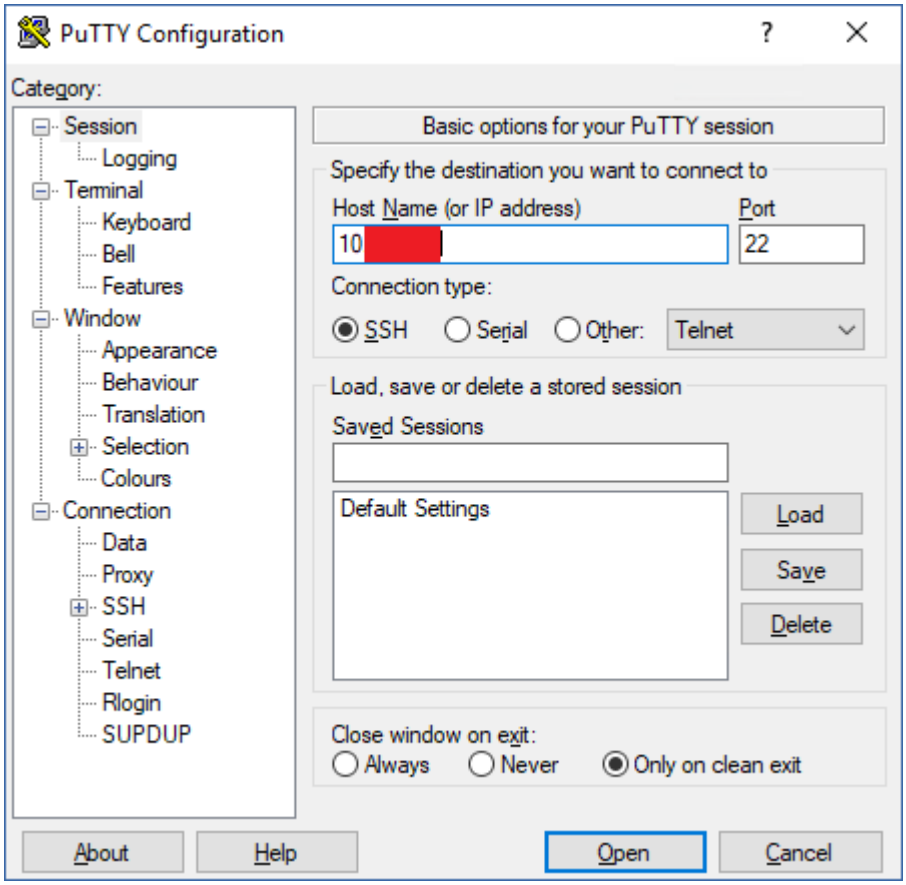
Pasos para actualizar Agente para Synology

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.



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
```

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**.

Implementación de agentes mediante 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. 173).
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. 177).
3. Configure el objeto de directiva de grupo como se describe en "Configurar el objeto de directiva de grupo" (p. 177).

Generar un token de registro

Un token de registro transmite la identidad de un usuario al programa de configuración del agente, sin almacenar las credenciales del usuario para la consola Cyber Protect. Esto permite a los usuarios

registrar cualquier número de máquinas en su cuenta o aplicar planes de protección a sus cargas de trabajo sin tener que iniciar sesión.

Nota
Los planes de protección no se aplican automáticamente durante el registro de la máquina. Aplicar un plan de protección es una tarea independiente.

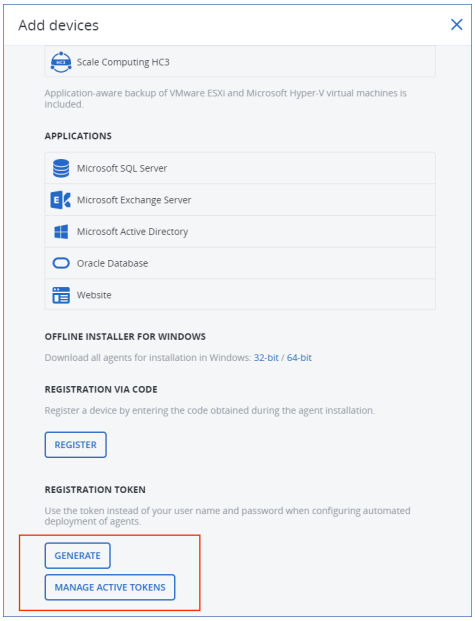
Por motivos de seguridad, los tokens tienen una vida útil limitada que puede ajustar. La vida útil predeterminada es de 3 días.

Los usuarios solo pueden generar tokens de registro para sus propias cuentas. Los administradores pueden generar tokens de registro para todas las cuentas de usuarios del inquilino que gestionen.

Para generar un token de registro

Como usuario

1. Inicie sesión en la consola de Cyber Protect.
2. Haga clic en **Dispositivos** > **Todos los dispositivos** > **Añadir**.
   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.

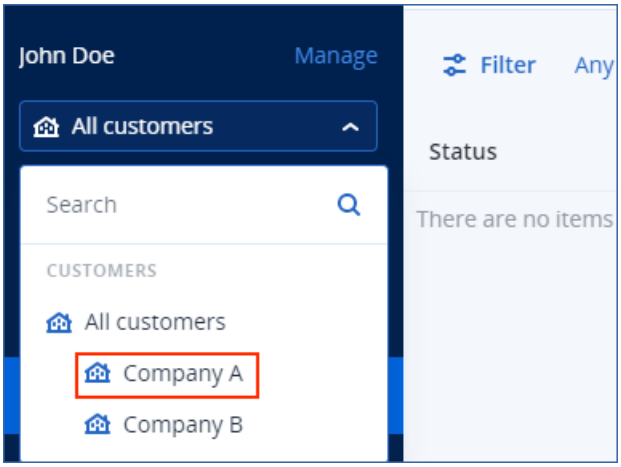
Como administrador

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**.

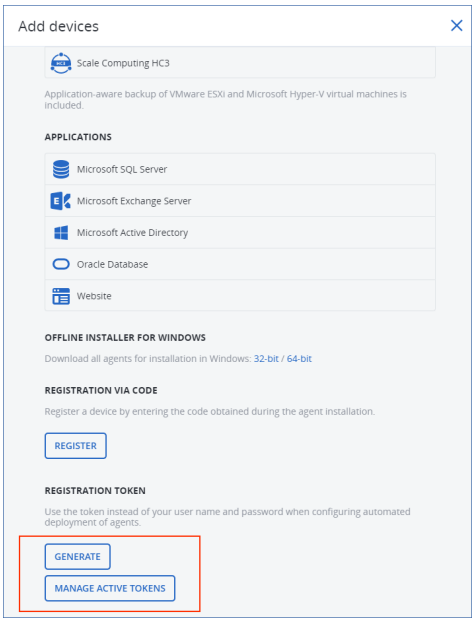
   [Para administradores de partner que gestionen inquilinos de cliente] En la consola de Cyber Protect, seleccione el inquilino con el usuario para el que desea generar un token. No puede generar un token en el nivel **Todos los clientes**.

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

   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.
   Tenga en cuenta que tendrá que ejecutar una secuencia de comandos que aplique o revoque un plan de protección en las cargas de trabajo añadidas. Consulte este artículo de la base de conocimientos para obtener más información.
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.

Pasos para ver o eliminar los tokens de registro

1. Inicie sesión en la consola de Cyber Protect.
2. Haga clic en **Dispositivos** > **Todos los dispositivos** > **Añadir**.
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 su inquilino.

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

4. [Para eliminar un token] Seleccione el token y luego haga clic en **Eliminar**.

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. 173).

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 **Configuración 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. 177).

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. 177) 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

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 **Añadir** 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**.

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. 179).

Nota
Recomendamos que detenga Secure Shell cuando no utilice la conexión SSH.

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. 179).

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.

Actualizar agentes

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

Para actualizar un agente automáticamente o de forma manual mediante la consola de Cyber Protect, se necesitan 4,2 GB de espacio libre en la siguiente ubicación:

- Para Linux: el directorio raíz
- Para Windows: el volumen en el que está instalado el agente

Para actualizar un agente en macOS, se necesitan 5 GB de espacio libre en el directorio raíz.

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
```

Actualización de agentes de forma manual

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

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** > **Añadir**.

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

1. Haga clic en **Configuración** > **Agentes**.

   El software muestra la lista de equipos. Los equipos con versiones de agentes obsoletas tienen un signo de exclamación naranja.
2. Seleccione los equipos en los que desea actualizar los agentes. Los equipos deben estar conectados.
3. Haga clic en **Actualizar agente**.

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

Cómo actualizar el Agente para VMware (dispositivo virtual) con una versión anterior a la 12.5.23094

1. Haga clic en **Configuración** > **Agentes** > el agente que desee actualizar > **Detalles** y examine la sección **Equipos virtuales asignados**. Tendrá que volver a introducir esta configuración tras la actualización.
   a. Anote la posición del conmutador **Asignación automática**.
   b. Para descubrir qué equipos virtuales se han asignado manualmente al agente, haga clic en el enlace **Asignado:**. El software muestra la lista de equipos virtuales asignados. Anote los equipos que tengan el símbolo `(M)` después del nombre del agente en la columna **Agente**.
2. Elimine Agente para VMware (dispositivo virtual), tal como se describe en "Desinstalación de agentes". En el paso 5, elimine el agente de **Configuración** > **Agentes** aunque tenga previsto volver a instalarlo.
3. Implemente Agente para VMware (dispositivo virtual), tal como se describe en "Implementación de la plantilla OVF".
4. Configure Agente para VMware (dispositivo virtual), tal como se describe en "Configuración del dispositivo virtual".

   Si quiere reconstruir el almacenamiento adjunto de forma local, haga lo siguiente en el paso 7:
   a. Añada el disco que contenga el almacenamiento local al dispositivo virtual.
   b. Haga clic en **Actualizar** > **Crear almacenamiento** > **Montar**.
   c. El software mostrará la **letra** y la **etiqueta** originales del disco. No las modifique.
   d. Haga clic en **Aceptar**.
5. Haga clic en **Configuración** > **Agentes** > el agente que desee actualizar > **Detalles** y vuelva a establecer la configuración que anotó en el paso 1. Si se asignaron equipos virtuales manualmente al agente, vuelva a asignarlos tal y como se describe en "Enlace de equipos virtuales".

   En cuanto se haya terminado de configurar el agente, los planes de protección aplicados al agente anterior se volverán a aplicar automáticamente al agente nuevo.
6. Los planes con la copia de seguridad que detecta aplicaciones activada requieren que se vuelvan a introducir las credenciales del SO invitado. Edite estos planes y vuelva a introducir las credenciales.

7. Los planes que incluyen la copia de seguridad de la configuración ESXi requieren que se vuelva a introducir la contraseña "raíz". Edite estos planes y vuelva a introducir la contraseña.

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

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 automáticamente

Para facilitar la gestión de varias cargas de trabajo, 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 15.0.26986 (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.

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. 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.

Tras habilitar las actualizaciones automáticas, puede configurar las siguientes opciones:

- **Actualizar canal**
  Define la versión de los agentes que se utilizará, la más actualizada o la más reciente de los agentes de la versión anterior.
- **Ventana de mantenimiento**
  La ventana de mantenimiento define cuándo se instalarán las actualizaciones. Si la ventana de mantenimiento está deshabilitada, las actualizaciones se llevarán a cabo en cualquier momento.
  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
  - Replicación de copias de seguridad
  - Replicación 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

Personalizar los ajustes de actualizaciones automáticas

1. En la consola de Cyber Protect, vaya a **Configuración** > **Agentes**.
2. Seleccione el ámbito de los ajustes:
   - Para cambiar los ajustes de todos los equipos, haga clic en **Editar la configuración predeterminada de la actualización del agente**.

- Para cambiar los ajustes para equipos específicos, seleccione los equipos que desee y haga clic en **Configuración de la actualización del agente**.

3. Configure los ajustes según sus necesidades y, a continuación, haga clic en **Aplicar**.

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 **Editar 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 **Aplicar**.

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**.

Actualización de agentes en cargas de trabajo protegidas por 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:

- 23.12.36943, lanzado en diciembre de 2023

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.

Evitar la desinstalación o modificación de agentes no autorizadas

Puede proteger el agente para Windows contra la desinstalación o modificación no autorizadas al habilitar la configuración **Protección con contraseña** en un plan de protección. Esta configuración está disponible solo si se habilita la configuración **Autoprotección**.

Para habilitar la Protección con contraseña

1. En un plan de protección, amplíe el módulo **Protección antivirus y antimalware** (módulo **Active Protection** para ediciones Cyber Backup).
2. Haga clic en **Autoprotección** y asegúrese de que el interruptor **Autoprotección** está habilitado.
3. Habilite el interruptor **Protección con contraseña**.
4. En la ventana que se abre, copie la contraseña que necesita para desinstalar o modificar los componentes de un agente para Windows protegido.
   Esta contraseña es única y no podrá recuperarla cuando cierre esta ventana. Si pierde u olvida la contraseña, puede editar el plan de protección y crear una nueva.
5. Haga clic en **Cerrar**.
6. En el panel **Autoprotección**, haga clic en **Listo**.
7. Guarde el plan de protección.

Se habilitará la protección por contraseña para los equipos a los que se aplique este plan de protección. La protección por contraseña solo está disponible para la versión del agente para Windows *15.0.25851* o posterior. Los equipos deben estar conectados.

Puede aplicar un plan de protección con protección por contraseña habilitada a un equipo que ejecute macOS, pero no se le ofrecerá protección. No puede aplicar ese plan a un equipo que ejecute Linux.

Tampoco puede aplicar más de un plan de protección con protección por contraseña habilitada a un mismo equipo Windows. Para obtener información sobre cómo resolver un posible conflicto, consulte Resolución de conflictos entre planes.

Pasos para cambiar la contraseña de un plan de protección existente

1. En el plan de protección, amplíe el módulo **Protección antivirus y antimalware** (módulo **Active Protection** para la edición Cyber Backup).
2. Haga clic en **Autoprotección**.
3. Haga clic en **Crear nueva contraseña**.

4. En la ventana que se abre, copie la contraseña que necesita para desinstalar o modificar los componentes de un agente para Windows protegido.
   Esta contraseña es única y no podrá recuperarla cuando cierre esta ventana. Si pierde u olvida la contraseña, puede editar el plan de protección y crear una nueva.
5. Haga clic en **Cerrar**.
6. En el panel **Autoprotección**, haga clic en **Listo**.
7. Guarde el plan de protección.

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. 348).

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

Pasos para desinstalar un agente

Windows

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**.
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 vSpehere 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 copias de seguridad** > **Ubicaciones** y, después, elimine la ubicación correspondiente al almacenamiento conectado localmente.

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.

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.
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.

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:

- 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.

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**.

Cambiar la cuota de servicio de equipos

Una cuota de servicio se asigna automáticamente cuando se aplica un plan de protección a un equipo por primera vez.

Se asigna la cuota más apropiada, según el tipo de equipo protegido, 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 **Servidor de alojamiento web**, pero no está disponible, se asignará la cuota **Servidor**.

Ejemplos de asignación de cuotas:

- A un equipo físico que ejecuta un sistema operativo Windows Server o un sistema operativo de un servidor Linux (como Ubuntu Server) se le asigna la cuota **Servidor**.
- A un equipo físico que ejecuta un sistema operativo de escritorio Windows o Linux (como Ubuntu Desktop) se le asigna la cuota de **Estación de trabajo**.

- A un equipo físico que ejecuta Windows 10 con el rol Hyper-V habilitado se le asigna la cuota **Estación 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 **Equipo virtual**. Este tipo de equipo también puede utilizar la cuota **Estación de trabajo** si la cuota **Equipo virtual** 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 **Equipo virtual**.
- A un servidor Hyper-V o vSphere se le asigna la cuota **Servidor**.
- A un servidor con cPanel o Plesk se le asigna la cuota **Servidor de alojamiento web**. También puede utilizar la cuota **Equipo virtual** o la cuota **Servidor**, según el tipo de equipo en el que se ejecute el servidor web, si la cuota **Servidor de alojamiento web** no está disponible.
- La copia de seguridad con información de aplicaciones requiere la cuota **Servidor**, incluso para una estación de trabajo.

Puede cambiar manualmente la asignación original más adelante. Por ejemplo, para aplicar un plan de protección más avanzado al mismo equipo, es posible que tenga que mejorar la cuota de servicio del mismo. 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 **Estación de trabajo**. Después de adquirir una cuota de **Equipos virtuales**, puede asignarla manualmente al equipo en lugar de la cuota **Estación de trabajo** original.

También puede liberar la cuota de servicio asignada actualmente para asignarla a otro equipo.

Puede cambiar la cuota de servicio de un equipo individual o de un grupo de equipos.

Pasos para cambiar la cuota de servicio de un equipo individual

1. En la consola de Cyber Protect, vaya a **Dispositivos**.
2. Seleccione el equipo que desee y haga clic en **Detalles**.
3. En la sección **Cuota de servicio**, haga clic en **Cambiar**.
4. En la ventana **Cambiar cuota**, seleccione la cuota de servicio deseada o **Sin cuota** y, a continuación, haga clic en **Cambiar**.

Pasos para cambiar la cuota de servicio de un grupo de equipos

1. En la consola de Cyber Protect, vaya a **Dispositivos**.
2. Seleccione más de un equipo y haga clic en **Asignar cuota**.
3. En la ventana **Cambiar cuota**, seleccione la cuota de servicio deseada o **Sin cuota** y, a continuación, haga clic en **Cambiar**.

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.

De forma predeterminada, la información del registro está optimizada para los últimos tres días, pero puede cambiar este período.

Para recoger registros de agentes

1. Realice uno de los siguientes procedimientos:
   - En **Dispositivos**, seleccione el equipo del que quiera recoger los registros y luego haga clic en **Actividades**.

- En **Configuración** > **Agentes**, seleccione el equipo del 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.

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 realizar una conmutación por error (ejecutar la máquina virtual de 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**.

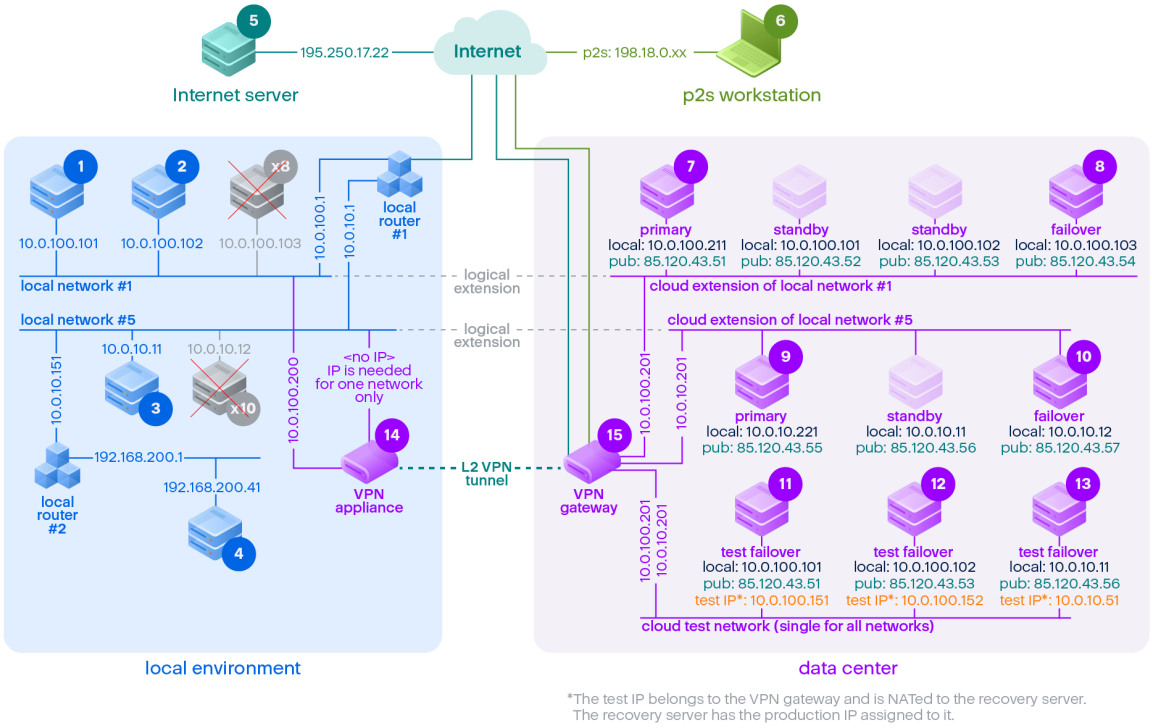
Nota
La configuración de red del servidor siempre muestra la **Dirección IP en la red de producción** (ya que el servidor de prueba refleja cómo se vería el servidor de producción). Esto ocurre porque la dirección IP de prueba no pertenece al servidor de prueba, sino a la puerta de enlace VPN, y se traduce 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 la recuperación ante desastres:
   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 la recuperación ante desastres (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 la recuperación ante desastres.
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)
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:**.

	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	a través	a través	no	a través	a través	a través	a través	a través del	a través del	a través del	directo	no

	Para:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
				del enrutador local 1	del enrutador local 2	del enrutador local 1 y de Internet		del túnel: local a través del enrutador local 1 y de Internet: pub	del túnel: local a través del enrutador local 1 y de Internet: pub	del túnel: local a través del enrutador local 1 y de Internet: pub	del túnel: local a través del enrutador local 1 y de Internet: pub	túnel: NAT (servidor VPN) a través del enrutador local 1 y de Internet: pub	túnel: NAT (servidor VPN) a través del enrutador local 1 y de Internet: pub	enrutador local 1 y del túnel: NAT (servidor VPN) a través del enrutador local 1 y de Internet: pub		
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 través del enrutador local 1 y de Internet:	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:	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 Inter	directo	no

	Para:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
								pub		pub				net: 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 del enrutador 2 y del enrutador 1 locales	a través del enrutador 2 y del enrutador 1 locales	a través del enrutador local 2		a través del enrutador 2 y del enrutador 1 locales y de Internet	no	a través del enrutador local 2 y del túnel: local	a través del enrutador local 2 y del túnel: local a trav	a través del enrutador local 2 y del túnel: local	a través del enrutador local 2 y del túnel: local a trav	a través del túnel: NAT (servidor VPN) a través del enrutador 2 y del enrut	a través del túnel: NAT (servidor VPN) a través del enrutador 2 y del enrut	a través del túnel: NAT (servidor VPN) a través del enrutador 2 y del enrut	a través del enrutador local 2	no

	Para:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
								a través del enrutador 2 y del enrutador 1 locales y de Internet: pub	és del enrutador 2 y del enrutador 1 locales y de Internet: pub	a través del enrutador 2 y del enrutador 1 locales y de Internet: pub	és del enrutador 2 y del enrutador 1 locales y de Internet: pub	ador 1 locales y de Internet: pub	ador 1 locales y de Internet: pub	ador 1 locales y de Internet: pub		
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
6	p2s	no	no	no	no	a través de Internet		a través de VPN p2s (servidor VPN):	a través de VPN p2s (servidor VPN): local	a través de VPN p2s (servidor VPN):	a través de VPN p2s (servidor VPN): local	a través de VPN p2s: NAT (servidor VPN) a través	a través de VPN p2s: NAT (servidor VPN) a través	a través de VPN p2s: NAT (servidor VPN) a través	no	no

	Para:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
								local a través de Internet: pub	a través de Internet: pub	local a través de Internet: pub	a través de Internet: pub	s de Internet: pub	s de Internet: pub	s de Internet: pub		
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 por error	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

	Para:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
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	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

	Para:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
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
15	servidor VPN	no	no	no	no	no	no	no	no	no	no	no	no	no	no	

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 Licencias en la guía del usuario de Cyber Protect.

Definición de cómo y qué proteger

La pestaña Administración

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

Todos los planes que ha creado están disponibles en la pestaña **Administración** de la consola de Cyber Protect.

Están disponibles las siguientes secciones:

- **Planes de protección**
- **Planes de administración remota**
- **Planes de programación**
- **Planes de supervisión**
- **Depósito de secuencia de comandos**
- **Copia de seguridad de aplicaciones en la nube**
- **Análisis de copia de seguridad**
- **Réplica de copia de seguridad**
- **Validación**
- **Limpieza**
- **Conversión a equipo virtual**
- **Replicación de equipos virtuales**

Estados del plan

Para los planes de protección y planes de replicación de máquinas virtuales, una barra de estado muestra los siguientes estados con códigos de color:

- Correcto (verde)
- Advertencia (naranja)
- Error (naranja oscuro)
- Crítico (rojo)
- El plan se está ejecutando (azul)
- El plan está deshabilitado (gris)

Haga clic en la barra de estado para ver detalles sobre los estados del plan en todas las cargas de trabajo a las que se aplica dicho plan.

Haga clic en un estado específico para ver una lista de todas las cargas de trabajo con este estado.

Planes de protección

En la pestaña **Administración** > **Planes de protección**, puede consultar información sobre sus planes de protección existentes, realizar acciones con ellos y crear nuevos planes.

Para obtener más información sobre los planes de protección, consulte "Planes de protección y módulos" (p. 223).

Planes de copias de seguridad para aplicaciones en la nube

La pestaña **Administración** > **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 copia 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.

Análisis de planes 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. 915).

Pasos para crear un plan de análisis de copias de seguridad

1. En la consola de Cyber Protect, vaya a **Administración** > **Análisis de copia de seguridad**.
2. Haga clic en **Crear plan**.
3. Especifique el nombre del plan y los siguientes parámetros:
   - **Tipo de análisis**:
     - **En la nube**: esta opción no se puede cambiar. Un agente de la nube seleccionado automáticamente realizará el análisis de la copia de seguridad.
   - **Copias de seguridad para analizar**:
     - **Ubicaciones**: seleccione las ubicaciones en las que se encuentren los conjuntos de copias de seguridad que quiera analizar.
     - **Copias de seguridad**: seleccione los conjuntos de copias de seguridad que desee analizar.
   - **Analizar para**:
     - **Malware**: esta opción no se puede cambiar. El análisis comprueba los conjuntos de copias de seguridad seleccionados en busca de malware (incluido el ransomware).
   - **Cifrado**: para analizar los conjuntos de copias de seguridad cifrados, especifique la contraseña de cifrado. Si selecciona una ubicación o varios conjuntos de copias de seguridad y la contraseña especificada no coincide con un conjunto de copia de seguridad, se crea una alerta.
   - **Planificación**: esta opción no se puede cambiar. El análisis se inicia automáticamente en el almacenamiento en la nube.
4. Haga clic en **Crear**.

Como resultado, se crea un plan de análisis de copias de seguridad y un agente de la nube analizará las ubicaciones o los conjuntos de copia de seguridad que especifique en busca de malware.

Procesamiento 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.
- 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.

Replicación de copias 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 replicación 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 replicación de copia de seguridad.

La replicación de copia de seguridad también puede formar parte de un plan de protección. Para obtener más información sobre esta opción, consulte "Replicación" (p. 459).

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 Cyber Protect, haga clic en **Administración** > **Replicación de copias 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.
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. 208).
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 **Reglas 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.

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 (archivo único)** 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 (archivo único)	**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	Todas las copias de seguridad	Una copia de seguridad por semana*	Una copia de seguridad por mes*

	Siempre incremental (archivo único)	Siempre completa	Completa semanal, incremental diaria	Completa mensual, diferencial semanal, incremental diaria (GFS)
	completa			
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 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 compatibles

La tabla siguiente resume las ubicaciones de copias de seguridad admitidas por los planes de réplica de copia de seguridad.

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.

Al validar una copia de seguridad, verifica que puede recuperar los datos con su ayuda.

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 sobre cómo crear una, acceda a "Creación de un plan de validación" (p. 211).

Están diosponibles los siguientes métodos de validación:

- Verificación de suma de comprobación
- Ejecutar como equipo virtual
  - Latido del equipo virtual
  - Validación de captura de pantalla

Puede seleccionar uno o varios de estos métodos. Cuándo hace más de one método is seleccionado, the operaciones for cada validación método run consecutively. Para obtener más información acerca de los métodos, acceda a "Latido del equipo virtual" (p. 214).

Puede validar conjuntos de copias de seguridad o ubicaciones de copias de seguridad. La validación de una ubicación de copia de seguridad valida todas las copias de seguridad almacenadas en la ubicación.

Ubicaciones compatibles

La siguiente tabla muestra las ubicaciones de copias de seguridad y los métodos de validación compatibles.

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	–	–	–

Validación del estado

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. La validación no se completa correctamente incluso cuando solo falla uno de los métodos de validación utilizados. En algunos casos, esto puede ser el resultado de una mala configuración del plan de validación: por ejemplo, utilizar el método **Latido del equipo virtual** para máquinas virtuales en un host erróneo.

El estado de validación de una copia de seguridad se actualiza con cada nueva operación de validación. El estado de cada método de validación se actualiza por separado. Ese es el motivo por el que una copia de seguridad en la que ha fallado un método, se mostrará como fallida hasta que ese mismo método de validación funcione, incluso si las últimas operaciones de validación ya no utilizan el método que fallo y la validación ya se ha completado correctamente.

Si quiere obtener más información sobre cómo comprobar el estado de validación, acceda a "Comprueba el estado de validación de una copia de seguridad" (p. 217).

Creación de un plan de validación

Para validar un conjunto de copias de seguridad como una operación de procesamiento de datos fuera del host, se crea un plan de validación.

Si quiere crear un plan de validación

1. En la consola de Cyber Protect, haga clic en **Administración** > **Validación**.
2. Haga clic en **Crear plan**.
   Se abrirá la plantilla del Nuevo plan de validación.
3. [Opcional] Para modificar el nombre del plan, haga clic en el nombre predeterminado.
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, seleccione una máquina con Agente para VMware o Agente para Hyper-V. De lo contrario, seleccione cualquier equipo que tenga acceso a la ubicación de la copia de seguridad.
5. En **Elementos para validar**, seleccione los conjuntos de copias de seguridad que quiera validar.
   a. Seleccione el ámbito del plan: conjuntos de copias de seguridad individuales o ubicaciones completas, haciendo clic en **Ubicaciones** o **Copias de seguridad** en la esquina superior izquierda.
      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.
   b. Haga clic en **Agregar**.
   c. Según el ámbito del plan de validación, seleccione ubicaciones o una ubicación y conjuntos de copias de seguridad y, a continuación, 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 conjuntos de copias de seguridad. 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**

   Para obtener más información acerca de los métodos, acceda a "Latido del equipo virtual" (p. 214).
8. [Si seleccionó **Verificación de suma de comprobación**] Haga clic en **Listo**.
9. [Si seleccionó **Ejecutar como equipo virtual**]. Configure los ajustes para este método.
   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 los dos métodos de validación que proporciona **Ejecutar como equipo virtual**:
      - **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 la plantilla del plan de validación, haga clic en **Planificación** y, a continuación, configúrela.
11. [Si las copias de seguridad seleccionadas en **Elementos para validar** están cifradas], 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, su plan de validación estará listo y se ejecutará de acuerdo con la planificación que haya configurado. Para ejectuar el plan de manera inmediata, selecciónelo en **Administración** > **Validación** y, a continuación, haga clic en **Ejecutar ahora**.

Tras el inicio del plan, puede supervisar las actividades en ejecución y desglosar sus detalles en la consola de Cyber Protect, desde **Supervisión** > **Actividades**.

Un plan de validación puede incluir varias copias de seguridad y una copia de seguridad se puede validar mediante varios planes de validación.

Nota
Todas las copias de seguridad se procesan secuencialmente, una por una, por una única tarea de validación.

Solo una tarea de validación puede ejecutarse a la vez en un agente dado. Varias tareas de validación pueden ejecutarse en paralelo si las ejecutan diferentes agentes: dos tareas simultáneas requieren dos agentes; tres tareas, tres agentes; y así sucesivamente.

La siguiente tabla resume los posibles estados de la actividad de validación.

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

Métodos de validación

En un plan de validación, están disponibles lo siguientes métodos de validación:

- Verificación de suma de comprobación
- Ejecutar como equipo virtual
  - Latido del equipo virtual
  - Validación de captura de pantalla

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 guardados en la copia de seguridad.

La validación por suma de verificación es un proceso que lleva bastante tiempo, incluso para copias de seguridad incrementales o diferenciales de pequeño tamaño. El motivo es que la operación de validación no solo comprueba los datos que están contenidos físicamente en una copia de seguridad concreta, sino que todos los datos que se necesita recuperar, es decir, se necesita validar también otras copias de seguridad anteriores.

Una correcta validación por suma de verificación conlleva una alta probabilidad de recuperar los datos. Sin embargo, la validación mediante este método no comprueba todos los factores que afectan 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.

Ejecutar como equipo virtual

Este método solo funciona para copias de seguridad a nivel de discos que contienen un sistema operativo. Para usar este método, necesita un servidor ESXi o Hyper-V y un agente de protección (Agente para VMware o Agente para Hyper-V) que gestione el host.

El método de validación **Ejecutar como equipo virtual** está diposnible para las siguientes variantes:

- Latido del equipo virtual
- Validación de captura de pantalla

Debe seleccionar al menos un método.

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 servicos 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 falla.

Independientemente del número de planes de validación y copias de seguridad validadas, el agente que realiza la validación ejecuta un equipo virtual cada vez. En cuanto el resultado de la validación esté disponible, el agente elimina el equipo virtual y ejecuta el siguiente.

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

Mediante este método de validación, el agente ejecuta una máquina virtual a partir de la copia de seguridad y, mientras la máquina virtual arranca, se realizan capturas de pantalla. Un módulo de inteligencia automática (MI) comprueba las capturas de pantalla y, si hay una pantalla de inicio de sesión en ellas, marca la copia de seguridad como validada.

La captura de pantalla está anexada al punto de recuperación y puede descargarla desde la Cyber Protect de la consola durante el año posterior a la validación. Para obtener más información acerca de cómo comprobar las capturas de pantalla, consulte "Comprueba el estado de validación de una copia de seguridad" (p. 217).

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. Si quiere obtener más información acerca de las notificaciones, acceda a 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 pantalla de inicio.

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 compartido de red
- Cinco minutos: para copias de seguridad almacenadas en la nube

Puede cambiar esto editando el archivo de configuración para el Agente para VMware o el Agente para Hyper-V.

Pasos para cambiar el tiempo de espera

1. Abra el archivo de configuración para editarlo. Puede encontrar el archivo 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. 178).
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>
   <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 la máquina virtual con el agente.

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**.

Comprueba el estado de validación de una copia de seguridad

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**.

También puede ver el estado de cada métdo de validación y descargar una captura de pantalla tomada por el método de validación de capturas de pantalla.

Para obtener más información sobre cómo funcionan los estados, consulte "Validación del estado" (p. 210).

Compruebe el estado de validación de una copia de seguridad

Dispositivos

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Todos los dispositivos**.
2. Seleccione la carga de trabajo de la que quiera comprobar el estado de validación de la copia de seguridad y, a continuación, 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 de la que quiere comprobar el estado.

Almacenamiento de copias de seguridad

1. En la consola de Cyber Protect, vaya a **Almacenamiento de la copia de seguridad**.
2. Seleccione la ubicación donde está almacenado su conjunto de copias de seguridad.
3. Seleccione el conjunto de copias de seguridad y, a continuación, haga clic en **Mostrar copias de seguridad**.
4. Seleccione la copia de seguridad de la que quiere comprobar el estado de validación.

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 Cyber Protect, haga clic en **Administración** > **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 **Reglas 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**.

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. 220).

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 **Administración** > **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:
   - [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.

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.

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.

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 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. 774). 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.

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 **Administración** > **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 sobre posibles conflictos, consulte "Resolución de conflictos entre planes" (p. 230).

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. 461).

Administración > Planes de protección

1. En la consola de Cyber Protect, vaya a **Administración** > **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.
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. 226).

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. 461).

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 "Crear un plan de protección de recuperación ante desastres" (p. 781).

Para obtener más información sobre el módulo de control de dispositivos, consulte "Cómo trabajar con el módulo de control de dispositivos" (p. 379).

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.
  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
  Puede importar planes de protección creados en Cyber Protection 9.0 (lanzada en marzo de 2020) o versiones posteriores. Los planes creados en las versiones anteriores no son compatibles con las versiones 9.0 y posteriores de Cyber Protection.

- 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 **Administración** > **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**.
4. Se muestra una lista con los planes de protección disponibles.
5. 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 **Administración** > **Planes de protección**.
2. Seleccione el plan de protección que desee aplicar.
3. Haga clic en **Editar**.
4. Haga clic en **Gestionar dispositivos**.

5. En la ventana **Dispositivos**, haga clic en **Añadir**.
6. Seleccione las cargas de trabajo a las que quiera aplicar el plan y, a continuación, haga clic en **Añadir**.
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. 377).

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 **Administración** > **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

1. En la consola de Cyber Protect, vaya a **Administración** > **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 **Administración** > **Planes de protección** afecta a todas las cargas de trabajo a las que se aplica ese plan.

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 **Administración** > **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 **Administración** > **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 **Administración** > **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

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 **Administración** > **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 **Administración** > **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 **Administración** > **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**.

Resolución de conflictos entre planes

Puede aplicar varios planes de protección a una misma carga de trabajo. Por ejemplo, puede aplicar un plan de protección en el que habilite y configure solo el módulo **Antivirus y antimalware**, y otro plan de protección en el que habilite y configure solo el módulo **Copia de seguridad**.

Puede combinar planes de protección en los que haya distintos módulos habilitados. También puede combinar varios planes de protección en los que solo el módulo **Copia de seguridad** esté habilitado. Sin embargo, si hay un módulo habilitado en más de un plan, se produce un conflicto. Para aplicar el plan, primero deberá resolver el conflicto.

Conflicto entre un plan nuevo y otro existente

Si un plan entra en conflicto con otro existente, puede resolverlo de cualquiera de estas formas:

- Cree un nuevo plan, aplíquelo y deshabilite el plan existente que entre en conflicto con el nuevo.
- Cree un plan nuevo y deshabilítelo.

Conflicto entre un plan individual y uno grupal

Si un plan de protección individual entra en conflicto con un plan grupal que se aplica a un grupo de dispositivos, puede resolverlo de cualquiera de estas formas:

- Elimine la carga de trabajo del grupo de dispositivos y, a continuación, aplíquele el plan de protección individual.
- Edite el plan grupal existente o aplique un nuevo plan grupal al grupo de dispositivos.

Problemas con las licencias

El módulo de un plan de protección puede requerir que se asigne una cuota de servicio específica a la carga de trabajo protegida. Si la cuota de servicio asignada no es adecuada, no podrá ejecutar, actualizar ni aplicar el plan de protección en el que se ha habilitado el módulo correspondiente.

Para resolver un problema relacionado con las licencias, realice uno de los siguientes procedimientos:

- Deshabilite el módulo que no sea compatible con la cuota de servicio asignada actualmente y siga usando el plan de protección.
- Cambie la cuota de servicio asignada manualmente. Para obtener información al respecto, consulte "Cambiar la cuota de servicio de equipos" (p. 191).

Planes de protección predeterminados

Un plan de protección predeterminado es una plantilla preconfigurada que puede aplicar a sus cargas de trabajo, con lo cual se garantiza la protección rápida. Al utilizar un plan de protección predeterminado, no tiene que crear nuevos planes de protección desde cero.

Cuando aplica un plan de protección predeterminado por primera vez, la plantilla se copia a su inquilino y puede editar los módulos en el plan y su configuración.

Están disponibles los siguientes planes predeterminados:

- Cyber Protect Essentials
  Este plan ofrece una funcionalidad de protección básica y copia de seguridad a nivel de archivos.
- Trabajadores en remoto
  Este plan está optimizado para usuarios que trabajan de forma remota. Ofrece más tareas frecuentes (como copia de seguridad, protección antimalware y evaluación de vulnerabilidades), acciones de protección más estrictas, y opciones de energía y rendimiento optimizadas.
- Trabajadores en la oficina (antivirus de terceros)
  Este plan está optimizado para usuarios que trabajan en oficinas y prefieren usar un software antivirus de terceros. En este plan, el módulo **Protección antivirus y antimalware** está deshabilitado.
- Trabajadores en la oficina (Acronis Antivirus)
  Este plan está optimizado para usuarios que trabajan en oficinas y prefieren usar el software antivirus de Acronis.

Comparación de los planes de protección predeterminados

Módulos y opciones	**Planes de protección predeterminados**			
	Cyber Protect Essentials	**Trabajadores en remoto**	**Trabajadores en la oficina (antivirus de terceros)**	**Trabajadores en la oficina (Acronis Antivirus)**
Copia de seguridad	Disponible	Disponible	Disponible	Disponible
Qué incluir en la copia de seguridad Elementos que se incluirán en la copia de seguridad	Archivos/carpetas [Carpeta Todos los perfiles]	Todo el equipo	Todo el equipo	Todo el equipo
Protección continua de datos (CDP)	Deshabilitado	Habilitado	Deshabilitado	Deshabilitado
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 23:00	De lunes a viernes, a las 00:00 Otras opciones y condiciones de	De lunes a viernes, a las 23:00	De lunes a viernes, a las 23:00

Módulos y opciones	Planes de protección predeterminados			
	Cyber Protect Essentials	**Trabajadores en remoto**	**Trabajadores en la oficina (antivirus de terceros)**	**Trabajadores en la oficina (Acronis Antivirus)**
		inicio habilitadas: • Si el equipo está apagado, ejecutar las 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		
Esquema de copias de seguridad	Siempre incremental	Siempre incremental	Siempre incremental	Siempre incremental
Cuánto tiempo se conservarán	Mantener las copias de seguridad indefinidamente	Mensualmente: 12 meses Semanalmente: 4 semanas Diariamente: 7 días	Mensualmente: 12 meses Semanalmente: 4 semanas Diariamente: 7 días	Mensualmente: 12 meses Semanalmente: 4 semanas Diariamente: 7 días
Opciones de copia de seguridad	Opciones predeterminadas	Opciones predeterminadas, más: • Ventana de copia de seguridad y	Opciones predeterminadas	Opciones predeterminadas

Módulos y opciones	Planes de protección predeterminados			
	Cyber Protect Essentials	**Trabajadores en remoto**	**Trabajadores en la oficina (antivirus de terceros)**	**Trabajadores en la oficina (Acronis Antivirus)**
		rendimiento (el conjunto verde): Prioridad de la CPU: Bajo Velocidad de salida: 50 %		
Protección antivirus y antimalware	Disponible	Disponible	No disponible	Disponible
Active Protection	Desactivado	Desactivado	–	Desactivado
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
Protección en tiempo real	Cuarentena	Cuarentena	–	Cuarentena
Planificar análisis	Análisis rápido: Cuarentena	Análisis rápido: Desactivado	–	Análisis rápido: Cuarentena

Módulos y opciones	Planes de protección predeterminados			
	Cyber Protect Essentials	**Trabajadores en remoto**	**Trabajadores en la oficina (antivirus de terceros)**	**Trabajadores en la oficina (Acronis Antivirus)**
	De domingo a sábado, a las 14:20 Análisis completo: Desactivado	Análisis completo: Cuarentena De domingo a sábado, a las 13:55 Otras opciones y condiciones de inicio habilitadas: • Si el equipo está apagado, ejecutar las 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		De domingo a sábado, a las 14:20 Análisis completo: Desactivado
Exclusiones	Ninguno	Ninguno	–	Ninguno
Filtrado de URL	Disponible	Disponible	Disponible	Disponible
Acceso a sitio web malicioso	Preguntar siempre al usuario	Bloquear	Preguntar siempre al usuario	Preguntar siempre al usuario
Categorías que se pueden filtrar	Opciones predeterminadas	Opciones predeterminadas	Opciones predeterminadas	Opciones predeterminadas
Exclusiones	Ninguno	Ninguno	Ninguno	Ninguno
Evaluación de	Disponible	Disponible	Disponible	Disponible

Módulos y opciones	Planes de protección predeterminados			
	Cyber Protect Essentials	**Trabajadores en remoto**	**Trabajadores en la oficina (antivirus de terceros)**	**Trabajadores en la oficina (Acronis Antivirus)**
vulnerabilidades				
Ámbito de evaluación de vulnerabilidades	Productos de Microsoft, productos de terceros a Windows	Productos de Microsoft, productos de terceros a Windows	Productos de Microsoft, productos de terceros a Windows	Productos de Microsoft, productos de terceros a Windows
Planificación	A las 13:15, solo los lunes	A las 14:20, solo los lunes	A las 13:15, solo los lunes	A las 13:15, solo los lunes
Gestión de parches	Disponible	Disponible	Disponible	Disponible
Productos de Microsoft	Todas las actualizaciones	Todas las actualizaciones	Todas las actualizaciones	Todas las actualizaciones
Productos de terceros a Windows	Solo actualizaciones importantes	Solo actualizaciones importantes	Solo actualizaciones importantes	Solo actualizaciones importantes
Planificación	A las 15:10, solo los lunes	De lunes a viernes, a las 14:20	A las 15:10, solo los lunes	A las 15:10, solo los lunes
Copia de seguridad anterior a la actualización	Desactivado	Activado	Desactivado	Desactivado
Mapa de protección de datos	No disponible	Disponible	Disponible	Disponible
Extensiones y reglas de excepción	–	Opciones predeterminadas y las siguientes extensiones adicionales: **Imágenes** • .jpeg • .jpg • .png • .gif	Opciones predeterminadas (66 extensiones a detectar)	Opciones predeterminadas (66 extensiones a detectar)

Módulos y opciones	Planes de protección predeterminados			
	Cyber Protect Essentials	**Trabajadores en remoto**	**Trabajadores en la oficina (antivirus de terceros)**	**Trabajadores en la oficina (Acronis Antivirus)**
		• .bmp • .ico • .wbmp • .xcf • .psd • .tiff • .dwg **Audio y vídeo** • .avi, • .mov, • .mpeg, • .mpg, • .mkv • .wav • .aif • .aifc • .aiff • .au • .snd • .mid • .midi • .mpga • .mp3 • .oga • .flac • .opus • .spx • .ogg • .ogx • .mp4		
Planificación	–	De lunes a viernes, a las 15:35	De lunes a viernes, a las 15:40	De lunes a viernes, a las 15:40

Nota
El número de módulos en un plan de protección predeterminado puede variar según su licencia de Cyber Protection.

Aplicar un plan de protección predeterminado

Los planes de protección predeterminados iniciales son plantillas cuya configuración no puede editarse. Cuando aplica un plan predeterminado por primera vez, la plantilla se copia a su inquilino como un plan de protección preconfigurado y se habilita en las cargas de trabajo seleccionadas.

El plan de protección aparece en la pestaña **Administración** > **Planes de protección** y puede gestionarlo desde allí.

Pasos para aplicar un plan de protección predeterminado por primera vez

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Todos los dispositivos**.
2. Seleccione las cargas de trabajo que desea proteger.
3. Haga clic en **Proteger**.
4. Seleccione uno de los planes predeterminades y pulse **Aplicar**.

Editar un plan de protección predeterminado

Puede editar un plan de protección predeterminado después de aplicarlo por primera vez.

Pasos para editar un plan de protección predeterminado aplicado

1. En la consola de Cyber Protect, vaya a **Administración** > **Planes de protección**.
2. Seleccione el plan que desea editar y, a continuación, haga clic en **Editar**.
3. Modifique los módulos que se incluyen en este plan, o sus opciones, y después haga clic en **Guardar**.

   Importante
   Algunas de las opciones no se pueden modificar.

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.

#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 antimalware instalado en un equipo.	Hallazgos: • Tiene la protección antimalware habilitada (+275 puntos) • 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.	275: hay software antimalware instalado en un 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	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	100: el cortafuegos público de Windows está habilitado 75: el cortafuegos privado de Windows está habilitado 175: el

	Windows y la protección de red para ver si hay activado algún 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.	(0 puntos) Recomendaciones de #CyberFit Score: Le recomendamos que habilite un firewall 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 firewall 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	cortafuegos público y privado de Windows está habilitado 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	75: la VPN está habilitada y en funcionamiento 0: la VPN no está habilitada

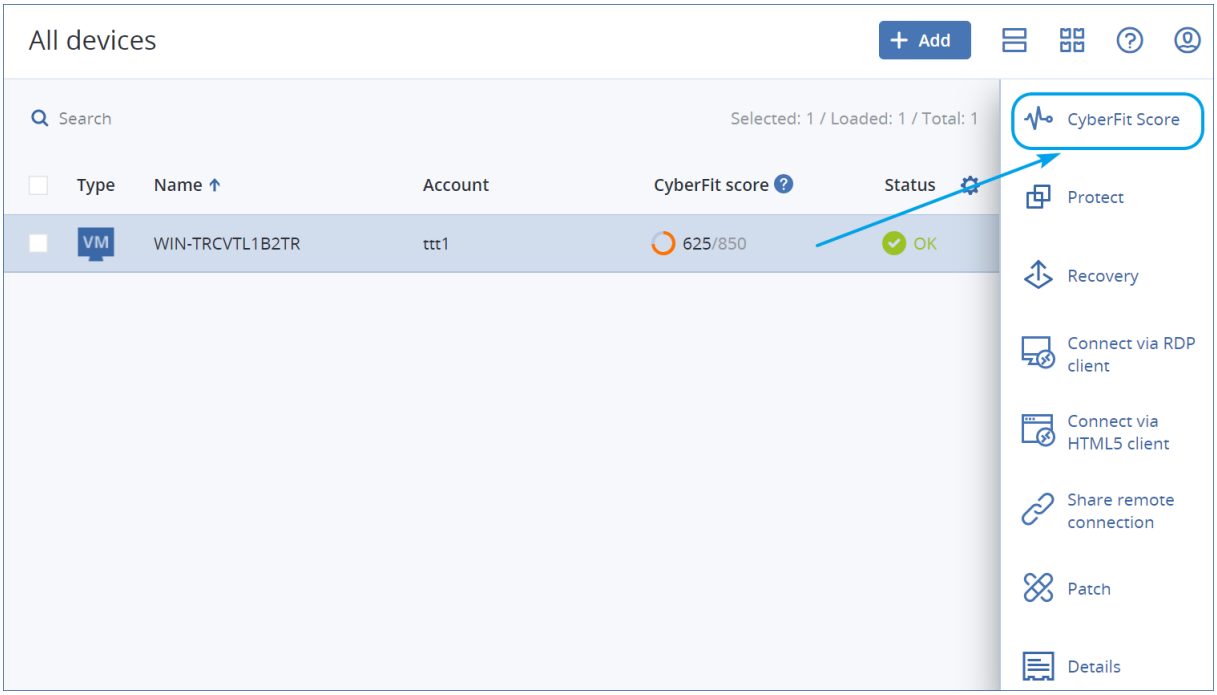
		• Cisco AnyConnect • NordVPN • TunnelBear • ExpressVPN • PureVPN • CyberGhost VPN • Perimeter 81 • VyprVPN • IPVanish VPN • Hotspot Shield VPN • Fortigate VPN • ZYXEL VPN • SonicWall GVPN • LANCOM VPN	
Cifrado de disco	El agente comprueba si un equipo tiene habilitado el cifrado de disco. El agente comprueba 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	25: el tráfico NTLM saliente está establecido en DenyAll 0: el tráfico NTLM saliente está establecido en otro valor

		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 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.

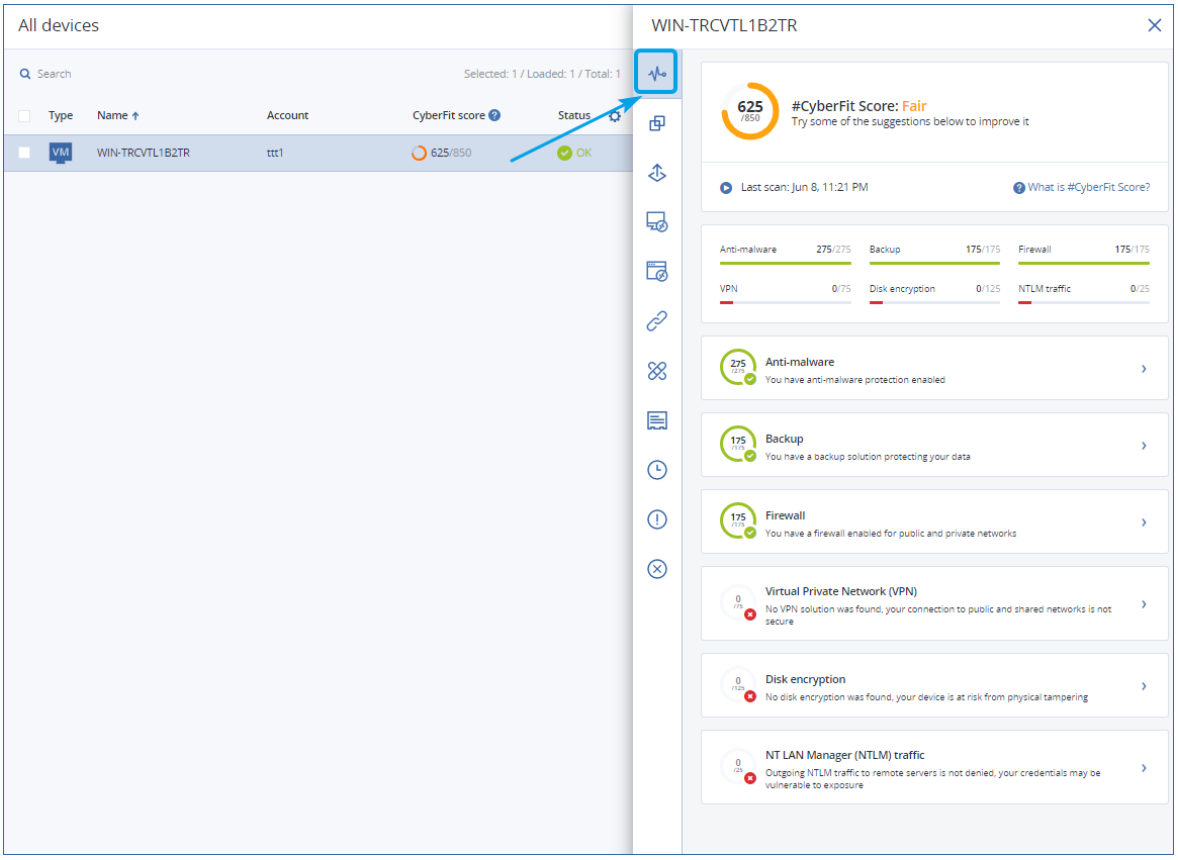


También puede obtener información sobre el #CyberFit Score en el widget y en las páginas del informe.

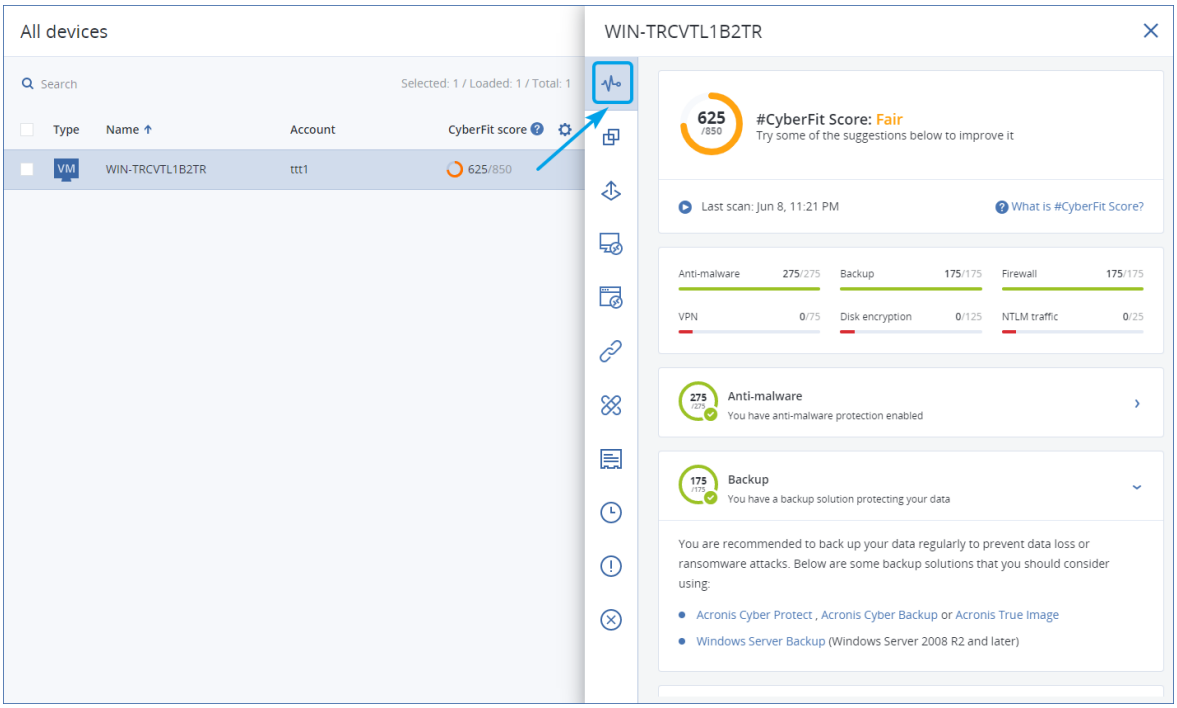
Ejecución de un análisis #CyberFit Score

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**.
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.



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 "Compatibilidad con varios inquilinos" (p. 341).

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. 256).

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. 246).

Requisitos previos

- La funcionalidad de Cyber Scripting requiere el paquete de Advanced Management.
- 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

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 en su propio inquilino y en los inquilinos secundarios correspondientes. No pueden ver objetos en un nivel de administración más alto, si los hay, ni acceder a ellos.

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.

Rol	Objeto	Estado de la secuencia de comandos		
		Borrador	**Probando**	**Aprobado**
Administrador de cibernética **Administrador de**	Plan de programación	Editar (Eliminar un borrador de secuencia de comandos de un	Crear Editar Aplicar	Crear Editar Aplicar

la empresa		plan) Eliminar Revoque Deshabilitar Detener	Habilitar Ejecutar Eliminar Revoque Deshabilitar Detener	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 Revoque Deshabilitar Detener	Vista Cancelar ejecución	Crear Editar Aplicar Habilitar Ejecutar Eliminar Revoque Deshabilitar Detener
	Secuencia de comandos	Crear Editar Clonar Eliminar Cancelar ejecución	Vista Clonar Cancelar ejecución	Ejecutar Clonar Cancelar 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 **Administración** > **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.

Rango	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.

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. 256).

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 **Administración** > **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.

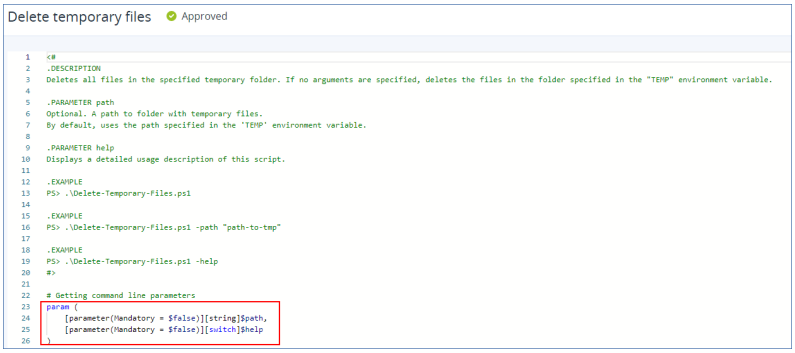
4. Especifique la configuración de la secuencia de comandos.

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. • **Mac OS** [Para secuencias de comandos generadas por IA] Esta configuración se realiza antes de la generación de la secuencia de comandos.
Rango	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

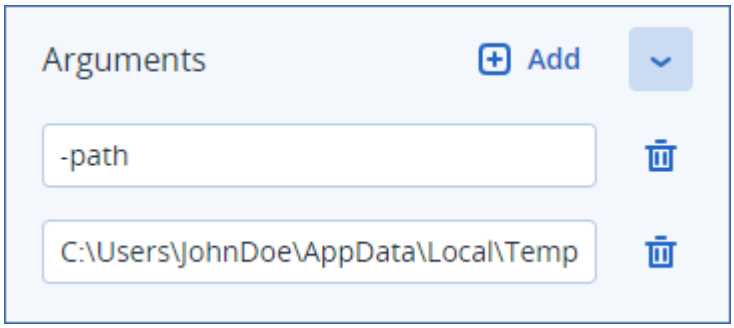
Configuración	Descripción
	planes de programación. Solo los administradores con el rol de **Administrador de cibernética** pueden cambiar el estado de una secuencia de comandos o eliminar una secuencia de comandos aprobada. Para obtener más información, vea "Cambio del estado de la secuencia de comandos" (p. 256).
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.

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. 256).

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. 254).

Creación de una secuencia de comandos con IA

Nota
Esta funcionalidad requiere el paquete de Advanced Management.

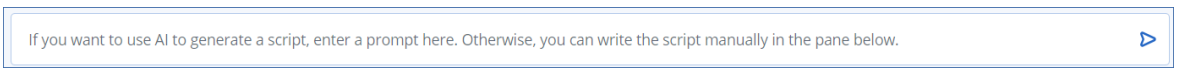
Puede usar la IA para transformar indicaciones en secuencias de comandos potentes, lo que le ahorrará tiempo y esfuerzo. Puede usar la funcionalidad de las siguientes maneras:

- 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 **Administración** > **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 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. • **Mac OS** [Para secuencias de comandos generadas por IA] Esta configuración se realiza antes de la generación de la secuencia de comandos.
Rango	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**

Configuración	Descripción
	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. 256).
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.

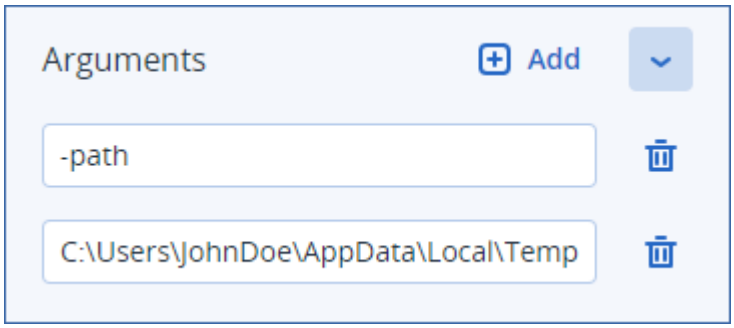
8. [Opcional] [Solo para las secuencias de comandos que requieran credenciales] Especifique las credenciales.

   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.

   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. 256).

    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. 254).

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

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 a los que se ha aplicado el paquete Advanced Management.

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. 246).

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**.

   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. 257).

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.

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. 246).

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

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. 256).

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: `salida estándar` y `error estándar`. En `salida estándar`, puede ver los resultados de una operación de programación completada correctamente. El archivo `error estándar` 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 **Administración**. 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
  - Rango
  - Idioma
  - 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 **Administración** > **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
- 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. 246).

Pasos para gestionar un plan de programación

1. En la consola de Cyber Protect, vaya a **Administración** > **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 **Administración** > **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**.

   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. 246).

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 directiva, 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 **Administración** > **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 un grupo de dispositivos en el nivel de partner, consulte "Pestaña Dispositivos" (p. 336).

   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.
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. 246).
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 directiva, 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

  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	La secuencia de comandos se ejecutará cuando la carga de trabajo de destino se conecte 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	Con esta condición, puede posponer un plan de programación planificado hasta que el usuario de la carga de trabajo de destino cierre sesión.
Coincidir con intervalo	Con esta condición, solo se ejecutará un plan de programación dentro del intervalo de tiempo especificado. Por ejemplo, puede usarla para limitar la condición **El usuario cerró la sesión**.
Ahorrar batería	Con esta condición, podrá asegurarse de que el plan de programación 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	Esta condición evita que el plan se inicie si la carga de trabajo de destino accede a Internet mediante una conexión de uso medido.
No iniciar con conexiones a las siguientes redes Wi-Fi	Esta condición evita que el plan se inicie si la carga de trabajo de destino se conecta a cualquiera de las redes inalámbricas especificadas. Para utilizar esta condición, debe especificar el SSID de la red prohibida. La restricción se aplica 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	Esta condición evita que el plan se inicie si alguna de las direcciones IP de la carga de trabajo de destino está dentro o fuera del rango de direcciones IP especificado.

Condición	Descripción
	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	Esta opción le permite establecer el intervalo de tiempo tras el cual se ejecutará el plan independientemente del resto de condiciones. El plan comenzará tan pronto como se cumplan el resto de las condiciones o termine el periodo máximo de tiempo, lo que suceda primero. Esta opción no está disponible si configura el plan de programación para que se ejecute solo una vez.

Administración de cargas de trabajo de destino para un plan

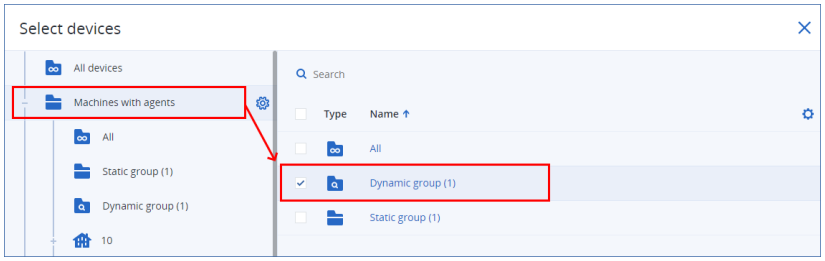
Puede seleccionar las cargas de trabajo o los grupos de dispositivos a los que desea aplicar un plan de programación cuando cree el plan o más adelante.

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 estático o dinámico en el nivel de partner, consulte "Pestaña Dispositivos" (p. 336).

Pasos para añadir cargas de trabajo iniciales a un plan

1. En la consola de Cyber Protect, vaya a **Administración** > **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**.
4. Seleccione las cargas de trabajo o los grupos de dispositivos que desee y haga clic en **Añadir**.

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.

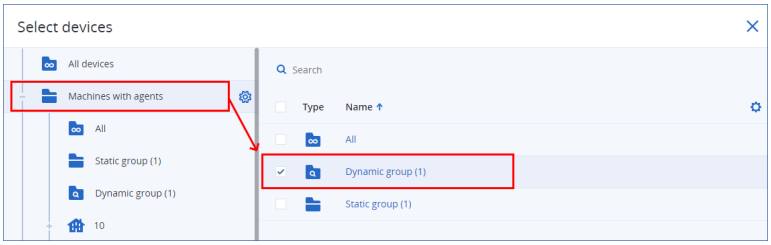
Pasos para gestionar cargas de trabajo existentes para un plan

1. En la consola de Cyber Protect, vaya a **Administración** > **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 **Añadir**.
     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.

Planes en diferentes niveles de administración

La siguiente tabla resume qué planes pueden ver y gestionar los administradores de diferentes niveles.

Administrador	Nivel de administración	Planes	Derechos
Administrador de socios	Nivel de partner	Planes propios	Acceso completo
		Planes de cliente (incluidos los planes de las unidades)	Acceso completo
		Planes de unidad	Acceso completo
	Nivel de cliente (para clientes gestionados	Planes de partner que se aplican a las cargas de trabajo de este cliente	Sólo lectura

Administrador	Nivel de administración	Planes	Derechos
	por el proveedor de servicios)		
		Planes de cliente (incluidos los planes de las unidades)	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	Acceso completo
Administrador de la compañía	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)	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	Acceso completo
Administrador de la unidad	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	Acceso completo

Importante
El propietario de un plan es el inquilino en el que se creó el plan. Por ello, si un administrador de partners creó un plan en el nivel de inquilino de cliente, el inquilino de cliente es el propietario de ese plan.

Problemas de compatibilidad con planes de programación

En algunos casos, aplicar un plan de programación en una carga de trabajo podría causar problemas de compatibilidad. Es posible que observe los siguientes problemas de compatibilidad:

- El sistema operativo es incompatible: este problema aparece cuando el sistema operativo de la carga de trabajo no es compatible.
- Agente no compatible: este problema aparece cuando la versión del agente de protección de la carga de trabajo está obsoleta y no es compatible con la funcionalidad de secuencia de comandos cibernética.
- Cuota insuficiente: este problema aparece cuando no hay una cuota de servicio suficiente en el inquilino para asignarla a las cargas de trabajo seleccionadas.

Si se aplica el plan de programación hasta 150 cargas de trabajo seleccionadas individualmente, se le pedirá que resuelva los conflictos existentes antes de guardar el plan. Para resolver un conflicto, elimine la causa raíz o las cargas de trabajo afectadas desde el plan. Para obtener más información, consulte "Resolver problemas de compatibilidad con planes de programación" (p. 267). Si guarda el plan sin resolver los conflictos, se deshabilitará automáticamente para las cargas de trabajo no compatibles y se mostrarán alertas.

Si se aplica el plan de programación a más de 150 cargas de trabajo o grupos de dispositivos, se guardará y, después, se comprobará la compatibilidad. El plan se deshabilitará automáticamente para las cargas de trabajo incompatibles y se mostrarán las alertas.

Resolver problemas de compatibilidad con planes de programación

Según la causa de los problemas de compatibilidad, puede ejecutar diferentes acciones para resolverlos como parte del proceso de creación de un nuevo plan de programación.

Nota
Al resolver un problema de compatibilidad mediante la eliminación de cargas de trabajo de un plan, no puede eliminar las cargas de trabajo que son parte de un grupo de dispositivos.

Pasos para resolver problemas de compatibilidad

1. Haga clic en **Revise los problemas**.
2. [Para resolver problemas de compatibilidad con sistemas operativos no compatibles]
   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 resolver problemas de compatibilidad con agentes no compatibles mediante la eliminación de cargas de trabajo desde el plan]

a. En la pestaña **Agentes no compatibles**, 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**.

4. [Para resolver problemas de compatibilidad con agentes no compatibles mediante la actualización de la versión del agente] Haga clic en **Ir a la lista de agentes**.

   Nota
   Esta opción solamente está disponible para los administradores de clientes.

5. [Para resolver problemas de compatibilidad con una cuota insuficiente mediante la eliminación de cargas de trabajo desde el plan]

   a. En la pestaña **Cuota insuficiente**, 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**.

6. [Para resolver problemas de compatibilidad con una cuota insuficiente mediante el aumento de la cuota del cliente]

   Nota
   Esta opción solamente está disponible para los administradores de partner.

   a. En la pestaña **Cuota insuficiente**, haga clic en **Ir al portal de administración**.

   b. Aumentar la cuota de servicio para el cliente.

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 que admita la funcionalidad de Ejecución rápida de la secuencia de comandos. Además, debe habilitar el paquete Advanced Management 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. 246).

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 **Administración** > **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

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 **Administración** > **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 **Añadir**.
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**.

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.

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 correcciones** 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

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. 316))

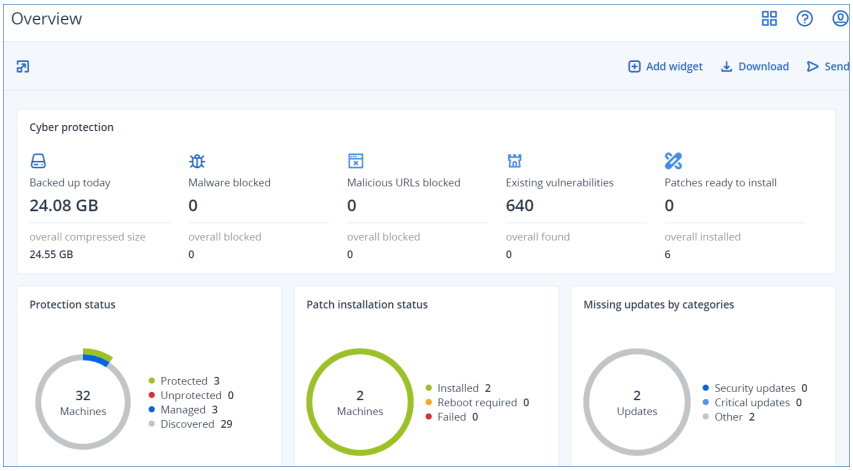
Panel de control de Información general

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.



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 **Actividades** proporciona información general de las actividades actuales y pasadas. De forma predeterminada, el período de retención es de 90 días.

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:

- **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:

- **Rango**
  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 **Alertas** muestra todas las alertas actuales. Las alertas enumeradas son críticas o alertas de errores y suelen estar relacionadas con tareas, como una copia de seguridad que haya fallado por cualquier motivo.

Pasos para filtrar alertas en el panel de control

1. En la lista desplegable **Ver**, seleccione uno de los siguientes criterios:
   - **Gravedad de la alerta**
   - **Categoría de alertas**
   - **Tipo de alerta**
   - **Tipo de supervisión**
   - **Rango de fechas: de... a...**
   - **Carga de trabajo**
   - **Plan**
   - **Cliente**
2. Si ha seleccionado la **Categoría de alertas**, en la lista desplegable **Categoría**, seleccione la categoría de alertas que desee ver.
3. Si desea ver todas las alertas sin filtrarlas, haga clic en **Todos los tipos de alerta**.

En cada alerta, puede hacer lo siguiente:

- Acceder al dispositivo que corresponde a la alerta haciendo clic en el enlace **Dispositivos**.
- Lea e intente seguir algunos de los consejos de la sección **Solución de problemas** de la alerta.
- Acceda a la documentación y al artículo de la base de conocimientos correspondientes haciendo clic en **Buscar solución**. La funcionalidad **Buscar una solución** rellenará automáticamente la solicitud con los detalles actuales de la alerta para facilitarle el proceso.

Para filtrar alertas en el panel de control

En la tabla de alertas, haga clic en el botón de la flecha junto a uno de los nombres de columna siguientes:

- **Gravedad de la alerta**
- **Tipo de alerta**
- **Creada**
- **Categoría de alertas**

- **Carga de trabajo**
- **Plan**

Si el servicio de Advanced Automation 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 a la alerta.
   Si se cierra una alerta, el ticket relacionado con ella se cerrará automáticamente.

Nota
Solo puede crear un ticket por alerta.

Tipos de alerta

Se generarán alertas de los tipos siguientes:

- Alertas de copia de seguridad
- Alertas de recuperación ante desastres
- Alertas de protección antimalware

- Alertas de licencias
- Alertas de filtrado de URL
- Alertas de EDR
- Alertas de control de dispositivos
- Alertas del sistema

Alertas de copia de seguridad

Alerta	Descripción	Cómo resolver la alerta
Error al realizar copia de seguridad	Se genera una alerta cuando falla la copia de seguridad durante la ejecución o se interrumpe al apagarse el sistema y se puede resolver el error.	Compruebe el registro de la operación de copia de seguridad fallida: seleccione la carga de trabajo y haga clic en **Actividades** para buscar el aviso en el registro. El mensaje debería dirigirle a la causa raíz del problema que le notifica el software.
Copia de seguridad completada con advertencias	Se genera una alerta cuando se completa la copia de seguridad con avisos.	Compruebe los registros de conversión a planes de máquina virtual, replicación o validación. Cualquier problema durante estas operaciones genera una alerta de "Actividad fallida" o "Actividad completada con aviso".
Se ha cancelado la copia de seguridad	Se genera una alerta cada vez que el usuario cancela manualmente una actividad de copia de seguridad.	Puede iniciar la copia de seguridad manualmente haciendo clic en Ejecutar ahora o esperar a que se ejecute a la próxima hora programada.
Copia de seguridad cancelada debido al cierre de una ventana de copia de seguridad	Se genera una alerta cuando se salta la actividad de copia de seguridad porque no quedaba tiempo en la ventana especificada en las opciones de copia de seguridad.	Vuelva a configurar la planificación o edite las opciones del plan de copias de seguridad en la ventana **Rendimiento y copia de seguridad**. Amplíe la sección de su producto para ver las instrucciones.
La copia de seguridad está en espera	Esta alerta se genera siempre que haya un conflicto de programación y se inicien dos tareas de copia de seguridad al mismo tiempo. En este caso, la segunda tarea de copia de seguridad se pondrá en cola hasta que finalice o se detenga	Asegúrese de que las copias de seguridad se ejecutan en los intervalos establecidos y según la planificación, y evite los conflictos de programación siempre que sea posible.

Alerta	Descripción	Cómo resolver la alerta
	la primera.	
La copia de seguridad no responde	Se genera una alerta cuando la copia de seguridad en curso lleva un tiempo sin mostrar progresos y podría estar congelada.	El problema podría deberse a un bloqueo. Siga este artículo para recopilar la información necesaria de solución de problemas.
La copia de seguridad no se ha iniciado	Se genera una alerta cuando no se puede iniciar la copia de seguridad programada por un motivo desconocido.	Asegúrese de estar usando la última compilación 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 nueva tarea de copia de seguridad también hace saltar la alerta, póngase en contacto con el Soporte de Acronis para obtener asistencia. • Si el agente estaba offline: 1. No apague el equipo a la hora de la copia de seguridad. 2. Si el equipo no estaba apagado, asegúrese de que se está ejecutando Acronis Managed Machine Service: Inicio -> Búsqueda -> services.msc -> busque Acronis Managed Machine Service. Póngase en contacto con el Soporte de Acronis si necesita asistencia.
Se desconoce el estado de la copia de seguridad	Se genera una alerta cuando el agente de copia de seguridad estaba offline a la hora programada para la copia de seguridad. No se conocerá el estado de las copias de seguridad de recursos hasta	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 debía estar offline, asegúrese de que se está

Alerta	Descripción	Cómo resolver la alerta
	que el agente esté en línea.	ejecutando Acronis Managed Machine Service: Inicio -> Búsqueda -> services.msc -> busque Acronis Managed Machine Service y compruebe su estado. Inicie el servicio si se había detenido.
Falta la copia de seguridad	Se genera una alerta cuando no se realiza una copia de seguridad correcta desde hace más de [Días desde la última copia de seguridad] días.	
La copia de seguridad está dañada	Se genera una alerta 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 dañadas. Si necesita asistencia para identificar la causa raíz del archivo comprimido dañado, póngase en contacto con el Soporte de Acronis.
Ha fallado la protección continua de datos	Se genera una alerta si falla 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 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 realizan cambios en una carpeta protegida local desde un

Alerta	Descripción	Cómo resolver la alerta
		origen de red (por ejemplo, cuando los usuarios acceden a la carpeta desde la red), la CDP no los detectará. 6. Si se está usando un archivo, por ejemplo, cuando se realizan cambios en un archivo Excel, la CDP no detectará los cambios. Para que la CDP detecte los cambios, debe guardarlos y cerrar el archivo.
La configuración de los servidores Hyper-V no es válida	Se genera una alerta cuando hay dos o más agentes para Hyper-V instalados en hosts Hyper-V que tienen el mismo nombre de host, algo que no está permitido en el mismo nivel de cuenta.	Para evitar conflictos, debe registrar estos agentes para Hyper-V en distintas unidades secundarias de esta cuenta.
La validación ha fallado	Se genera una alerta cuando no se puede completar el proceso de validación de su copia de seguridad.	Compruebe el registro de la operación fallida: seleccione el equipo y haga clic en **Actividades** para buscar el aviso en el registro. El mensaje debería dirigirle a la causa raíz del problema que le notifica el software.
Las copias de seguridad presentes en el almacenamiento en el cloud no se han podido migrar al formato nuevo	Se genera una alerta cuando no se pueden migrar las copias de seguridad presentes en el almacenamiento en la nube al formato nuevo.	La migración de los archivos comprimidos de Acronis Cyber Backup Advanced se describe aquí. La migración de los archivos comprimidos de Acronis Cyber Backup se describe aquí. Antes de ponerse en contacto con el Soporte de Acronis, recopile los siguientes informes con la herramienta migrate_archives: **migrate_archives.exe --account=<cuenta de Acronis> --password=<contraseña> --subaccounts=All > report1.txt** **migrate_archives.exe --cmd=finishUpgrade --account=<cuenta de Acronis> --**

Alerta	Descripción	Cómo resolver la alerta
		password=<contraseña> > report2.txt
No se encuentra la contraseña de cifrado	Se genera una alerta 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	Se genera una alerta si la comprobación programada determina que el servicio de envío físico al archivo comprimido de la nube de este plan de copias de seguridad no se ha cargado al almacenamiento.	
Error en la recuperación de la copia de seguridad	Se genera una alerta 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

Alerta	Descripción	Cómo resolver la alerta
Se ha superado la cuota de almacenamiento	Se genera una alerta cuando se supera la cuota flexible para el almacenamiento de recuperación ante desastres	Aumente la cuota o elimine algunos archivos comprimidos del almacenamiento en la nube.
Se ha alcanzado la cuota	Se genera una alerta cuando: • Se supera la cuota flexible para los servidores de la nube. • Se supera la cuota flexible para el punto de cálculo. • Se supera la cuota flexible para direcciones IP públicas.	

Alerta	Descripción	Cómo resolver la alerta
Se ha superado la cuota de almacenamiento	Se genera una alerta cuando se supera la cuota estricta para el almacenamiento de recuperación ante desastres. Este almacenamiento lo usan los servidores principales y los de recuperación. Si se alcanza el uso por encima del límite para esta cuota, no se podrán crear servidores principales ni de recuperación ni agregar o extender discos de los servidores principales existentes. Si se supera el uso por encima del límite para esta cuota, no se podrá iniciar una conmutación por error ni simplemente iniciar un servidor detenido. Los servidores en ejecución siguen funcionando.	
Se ha superado la cuota	Se genera una alerta cuando: • Se supera la cuota estricta para los servidores de la nube. • Se supera la cuota estricta para el punto de cálculo. • Se supera la cuota estricta para direcciones IP públicas.	Plantéese comprar cuotas de dispositivos adicionales o deshabilite las tareas de copia de seguridad en los dispositivos que ya no necesita proteger.
Error de conmutación por error	Se genera una alerta cuando se produce un problema en el sistema después de enviar una acción de conmutación por error.	1. Haga clic en **Editar** en el servidor de recuperación. Para obtener más información, consulte Creación de un servidor de recuperación. 2. Reduzca la CPU/RAM para el servidor de recuperación. 3. Vuelva a intentar la conmutación por error.
Error en prueba de conmutación por error	Se genera una alerta cuando se produce un problema en el sistema después de enviar una acción de prueba.	1. Haga clic en **Editar** en el servidor de recuperación. Para obtener más información, consulte Creación de un servidor de recuperación.

Alerta	Descripción	Cómo resolver la alerta
		2. Reduzca la CPU/RAM para el servidor de recuperación. 3. Vuelva a intentar la conmutación por error. **Nota** Asegúrese de que la dirección IP de la red de producción coincida con la que se ha configurado en el servidor DHCP.
Error de conmutación por recuperación	Se genera una alerta cuando se produce un problema en el sistema después de iniciar 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 la consola de Cyber Protect, vaya a Almacenamiento de la 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.
Se ha cancelado la conmutación por recuperación	Se genera una alerta cuando el usuario cancela la conmutación tras recuperación.	Descarte manualmente la alerta de la consola.
Error de conexión VPN	Se genera una alerta cuando falla la conexión de la VPN por motivos que no dependen de las acciones del usuario. El informe de estado del dispositivo VPN está obsoleto.	Si tiene problemas para desplegar o conectar el dispositivo VPN de Acronis, póngase en contacto con el Soporte de Acronis. Incluya la siguiente información en el correo electrónico: • Capturas de pantalla de los mensajes de error (si los hubiera)

Alerta	Descripción	Cómo resolver la alerta
		• Captura de pantalla de la interfaz de CLI del dispositivo VPN de Acronis • Su centro de datos y nombre del grupo de Acronis Backup Cloud.
(VPN no accesible) La puerta de enlace de conectividad no es accesible	Se genera una alerta cuando el servicio de recuperación ante catástrofes no puede acceder a la puerta de enlace de conectividad. El informe de estado de la puerta de enlace de conectividad está obsoleto.	Si tiene problemas para desplegar o conectar el dispositivo VPN de Acronis, póngase en contacto con el Soporte de Acronis. Incluya la siguiente información en el correo electrónico: • Capturas de pantalla de los mensajes de error (si los hubiera) • Captura de pantalla de la interfaz de CLI del dispositivo VPN de Acronis • Su centro de datos y nombre del grupo de Acronis Backup Cloud
Es necesario reasignar la IP de recuperación ante catástrofes	Se genera una alerta si el dispositivo VPN detecta cambios en la red.	Reasigne la dirección IP. Para obtener más información, consulte Reasignación de direcciones IP.
Fallo de la puerta de enlace de conectividad	Se genera una alerta cuando no se puede desplegar el servidor VPN en la nube.	Utilice la herramienta de verificación de la conexión y compruebe si hay errores en el resultado. Permita el acceso al software de Acronis en el control de la aplicación de sus firewalls y software antimalware.
Fallo al crear el servidor principal	Se genera una alerta cuando no se puede crear el servidor principal debido a un error.	
Fallo al crear el servidor de recuperación	Se genera una alerta cuando no se puede crear el servidor de recuperación debido a un error.	Asegúrese de que el servidor de recuperación cumple con los Requisitos de software.
Eliminar servidor principal	Se genera una alerta cuando se elimina un servidor principal.	

Alerta	Descripción	Cómo resolver la alerta
Fallo de recuperación del servidor	Se genera una alerta cuando no se puede recuperar el servidor principal o de recuperación.	Consulte los detalles. Si el mensaje de error es genérico o ambiguo (por ejemplo, "Error interno", vaya a **Recuperación ante desastres → Servidores**, seleccione el equipo afectado y haga clic en **Actividades**. Haga clic en una actividad, mantenga presionado ctrl y haga clic con el botón izquierdo en la actividad. Ahora podrá ver los puntos suspensivos (...) junto a cada actividad. Haga clic y seleccione **Información de la actividad de tarea**.
Error al realizar copia de seguridad	Se genera una alerta cuando falla la copia de seguridad del servidor de la nube (principal o servidor en estado de conmutación por error de producción).	1. Compruebe la conexión de 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	Se genera una alerta cuando se alcanza el número máximo de redes en la nube (5 redes).	
Error de runbook	Se genera una alerta cuando falla la ejecución del runbook.	No afecta a la funcionalidad del producto y se puede ignorar sin comprometer la seguridad. Para obtener más información, consulte Creación de un runbook.
Aviso de runbook	Se genera una alerta cuando se completa la ejecución del runbook con avisos.	No afecta a la funcionalidad del producto y se puede ignorar sin comprometer la seguridad. Para obtener más información, consulte Creación de un runbook.
Se requiere la interacción del usuario en el runbook	Se genera una alerta cuando hay pendiente una interacción del usuario en el runbook.	No afecta a la funcionalidad del producto y se puede ignorar sin comprometer la seguridad. Para obtener más información, consulte Creación de un runbook.
Tráfico de Internet bloqueado	Se genera una alerta cuando el administrador bloquea el tráfico	

Alerta	Descripción	Cómo resolver la alerta
	de Internet.	
Tráfico de Internet desbloqueado	Se genera una alerta cuando el administrador desbloquea el tráfico de Internet.	
Superposición de redes locales	Se genera una alerta cuando se detectan redes locales idénticas o superpuestas.	
Cuota de servidores insuficiente para cambio de licencia	Se genera una alerta cuando la cuota de servidores en la nube no es suficiente.	• Asegúrese de que el inquilino y el usuario tienen disponible una cuota de servidores o servidores de alojamiento web para un servidor físico. • Asegúrese de que el inquilino y el usuario tienen disponible una cuota de servidores de alojamiento web o máquinas virtuales para un servidor virtual. No se puede utilizar la cuota de servidores para un servidor virtual.
Artículo de oferta insuficiente para cambio de licencia	Se genera una alerta cuando el artículo de oferta del almacenamiento de recuperación ante desastres está deshabilitado.	Para obtener más información, consulte Cuotas de recuperación ante desastres.
Error de cambio de licencia	Se genera una alerta cuando se produce un error en la actualización de recuperación ante desastres.	
Puntos de cálculo insuficientes para cambio de licencia	Se genera una alerta cuando no hay puntos de cálculo disponibles.	En el portal de administración, comprueba y aumenta la cuota estricta para los puntos de cálculo.
Artículos de oferta de servidores insuficientes para cambio de licencia	Se genera una alerta cuando el artículo de oferta de los servidores de la nube está deshabilitado.	
La directiva no ha podido crear el servidor de recuperación	Se genera una alerta cuando se produce un error al configurar la infraestructura de recuperación ante desastres.	Cree manualmente el servidor de recuperación sin la propiedad de acceso a Internet. Para obtener más información, consulte Creación

Alerta	Descripción	Cómo resolver la alerta
		de un servidor de recuperación
Reprogramación de la conmutación por error de prueba automatizada del procesador de copias de seguridad	Se genera una alerta cuando se reprograma la ejecución de la conmutación por error de prueba automatizada.	
Tiempo de espera agotado en la conmutación por error de prueba automática del procesador de copias de seguridad	Se genera una alerta cuando vence la operación de conmutación por error de prueba automatizada. **Nota** Cada ejecución de la conmutación por error de prueba automatizada consume puntos de cálculo de pago.	
Fallo general de la conmutación por error de prueba automatizada del procesador de copias de seguridad	Se genera una alerta cuando falla la última conmutación por error de prueba automatizada programada del servidor de recuperación.	1. 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. 2. Espere a la siguiente fecha programada para la ejecución de la conmutación por error de prueba automatizada
Error de transferencia de datos durante la conmutación tras recuperación	Se genera una alerta cuando falla la transferencia de datos durante la conmutación tras recuperación.	
Fallo de conmutación tras recuperación	Se genera una alerta cuando se produce 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 al

Alerta	Descripción	Cómo resolver la alerta
		almacenamiento de 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. Vuelva a intentar la conmutación por error.
Fallo al confirmar la conmutación tras recuperación	Se genera una alerta cuando falla la confirmación de la conmutación tras recuperación.	
El equipo de conmutación tras recuperación está listo para el cambio	Se genera una alerta cuando el equipo está listo para el cambio.	
Cambio de conmutación tras recuperación finalizado	Se genera una alerta cuando se completa el cambio correctamente.	Descarte manualmente la alerta de la consola.
Agente de destino de la conmutación tras recuperación offline	Se genera una alerta cuando el agente está offline.	

Alertas de protección antimalware

Alerta	Descripción	Cómo resolver la alerta
Se ha detectado una actividad de conexión remota sospechosa	Se genera una alerta cuando se detecta ransomware proveniente de una conexión remota.	Descarte manualmente la alerta de la consola.
Actividad sospechosa detectada	Se genera una alerta cuando se detecta 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 saber qué proceso está cifrando los archivos y cuáles son

Alerta	Descripción	Cómo resolver la alerta
		los archivos afectados. Si decide que el proceso que cifra los archivos está sancionado (alerta por falso positivo), añádalo 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, empezando por la letra de unidad de disco. Por ejemplo: C:\Windows\Temp\er76s7sdkh.exe.
Actividad de criptominería detectada	Se genera una alerta 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	Se genera una alerta cuando se detecta ransomware en la carga de trabajo (específicamente si el ransomware modifica la partición de MBR/GPT).	Descarte manualmente la alerta de la consola.
Se ha especificado una ruta de red no compatible	Se genera una alerta cuando la ruta de recuperación que ha proporcionado el administrador no es una ruta a una carpeta local.	Especifique la ruta local para la protección de la carpeta de red (ruta de recuperación). Descarte manualmente la alerta de la consola
El proceso crítico se añade como dañino en el plan de Active Protection	Se genera una alerta cuando se añade un proceso crítico como un proceso bloqueado a la lista de exclusiones de protección.	Descarte manualmente la alerta de la consola.
No se ha podido aplicar la directiva Active Protection	Se genera una alerta cuando no se puede aplicar la directiva 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	Se genera una alerta cuando se detecta ransomware en la carga de trabajo	Descarte manualmente la alerta de la consola.

Alerta	Descripción	Cómo resolver la alerta
autorizada	(específicamente si el ransomware modifica la partición de ASZ).	
No se está ejecutando el servicio Active Protection	Se genera una alerta cuando se bloquea o no se está ejecutando el servicio Active Protection.	Compruebe el mensaje de error para ver por qué no se está ejecutando el servicio Active Protection.
El servicio Active Protection no está disponible	Se genera una alerta 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 la protección en tiempo real de Acronis, desinstale el antivirus de terceros del equipo. **Solución 2**: Si quiere usar el antivirus de terceros, deshabilite la protección en tiempo real de Acronis, el filtrado de URL y el antivirus de Windows Defender en el plan de protección.
La acción de cuarentena ha fallado	Se genera una alerta cuando el antimalware no puede 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	Se genera una alerta cuando el motor de comportamiento detecta un malware (tipo de proceso). Se pone en cuarentena el malware detectado.	Descarte manualmente la alerta de la consola.
Se ha detectado un proceso malicioso, pero no se ha puesto en cuarentena	Se genera una alerta 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)	Se genera una alerta cuando el análisis programado detecta un malware. Se pone	Descarte manualmente la alerta de la consola.

Alerta	Descripción	Cómo resolver la alerta
	en cuarentena el malware detectado.	
Se ha detectado y bloqueado malware (RTP)	Se genera una alerta 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	Se genera una alerta cuando se detecta un malware durante el análisis de copias de seguridad.	Descarte manualmente la alerta de la consola.
Conflicto detectado entre la protección antimalware en tiempo real y el producto de seguridad	Se genera una alerta cuando el antimalware no puede registrarse con el Centro de seguridad de Windows.	Deshabilite o desinstale el producto de seguridad de terceros, o deshabilite la protección antimalware en tiempo real en el plan de protección.
No se ha podido ejecutar el módulo Microsoft Security Essentials	Se genera una alerta cuando no se puede ejecutar el módulo 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	Se genera una alerta cuando no se puede activar la protección en tiempo real porque un antivirus de terceros aún la tiene habilitada.	Deshabilite o desinstale el producto de seguridad de terceros, o deshabilite la protección antimalware en tiempo real en el plan de protección.
La protección en tiempo real no está disponible porque falta un controlador o este no es compatible	Se genera una alerta cuando la protección en tiempo real no está disponible porque falta un controlador o este no es compatible.	Compruebe el mensaje de error para ver por qué Acronis no ha podido instalar el controlador en la carga de trabajo.
El servicio Cyber Protection (o Active Protection) no responde	Se genera una alerta cuando el servicio de ciberprotección responde a un aviso de comprobación del estado de la consola.	Descarte manualmente la alerta de la consola.
No se ha podido actualizar la definición de seguridad	Se genera una alerta cuando no se puede actualizar la definición de seguridad.	Compruebe el mensaje de error para ver por qué no se ha podido actualizar la definición de seguridad.

Alerta	Descripción	Cómo resolver la alerta
La Protección contra alteraciones está habilitada	Se genera una alerta cuando no se puede 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	Se genera una alerta cuando no se puede ejecutar el módulo de Windows Defender.	Compruebe el mensaje de error para ver por qué no se ha podido ejecutar el módulo de Windows Defender.
Windows Defender está bloqueado por el software antivirus de un tercero	Se genera una alerta cuanndo Windows Defender está bloqueado porque hay un antivirus de terceros instalado en el equipo.	Deshabilite o desinstale el producto de seguridad de terceros.
Conflicto de directiva de grupo	Se genera una alerta cuando no se puede cambiar la configuración de Microsoft Defender porque está controlada por una directiva de grupo.	Deshabilite 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	Se genera una alerta cuando Microsoft Security Essential elimina o pone en cuarentena un malware.	Descarte manualmente la alerta de la consola.
Microsoft Security Essentials ha detectado malware	Se genera una alerta cuando Microsoft Security Essentials detecta malware u otro software potencialmente no deseado.	Descarte manualmente la alerta de la consola.

Alertas de licencias

Alerta	Descripción	Cómo resolver la alerta
Casi se ha alcanzado la cuota de almacenamiento	Se genera una alerta cuando el uso está por debajo del 80 % (después de una limpieza o una actualización de cuota).	Plantéese comprar más almacenamiento o liberar espacio en el almacenamiento en la nube.
Se ha superado la cuota de almacenamiento	Se genera una alerta cuando se ha utilizado el 100 % de la cuota de	Compre más espacio de almacenamiento. Para obtener

Alerta	Descripción	Cómo resolver la alerta
	almacenamiento.	más información sobre cómo hacerlo, consulte la guía para comprar más almacenamiento en la nube.
Cuota de carga de trabajo alcanzada	Se genera una alerta 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	Se genera una alerta cuando el uso del artículo de oferta es superior a la cuota más el exceso.	
La carga de trabajo no tiene ninguna cuota para aplicar un plan de copias de seguridad (el recurso no tiene cuotas de servicio)	Se genera una alerta cuando: • La cuota se elimina manualmente: **Dispositivo** > **Detalles** > **Cuota de servicio**, haga clic en **Cambiar** y seleccione la opción **Sin cuota**. • Se deshabilita el artículo de oferta de la consola de administración. • El valor de la cuota más el exceso de la consola de administración del artículo de oferta es inferior al uso actual.	
No se puede proteger una carga de trabajo con una cuota asignada	Se genera una alerta cuando el artículo de oferta no es suficiente y necesita tener: • un grupo dinámico. • un plan de copias de seguridad asignado a dicho grupo. • ha añadido un recurso que se incluye en dicho grupo dinámico, pero tiene algunas cualidades que no permiten aplicarle el mismo plan de copias de seguridad.	
La licencia de suscripción ha caducado	Se genera una alerta cuando la comprobación diaria de alertas de vencimiento de licencias/mantenimiento pregunta al servidor de licencias y la respuesta es que la licencia ha vencido.	Cuando vence una suscripción, se bloquean todas las funcionalidades del producto salvo la recuperación hasta que se renueve. Los datos de las copias de seguridad siguen estando disponibles para su recuperación. Compre una

Alerta	Descripción	Cómo resolver la alerta
		licencia nueva. **Nota** Si ha comprado recientemente una nueva suscripción, pero sigue recibiendo el mensaje de que ha vencido la suscripción, debe importar la nueva suscripción desde la cuenta de Acronis: en la consola de administración, vaya a Configuración -> Licencias y haga clic en Sincronizar en la esquina superior derecha. Se sincronizarán las suscripciones.
La licencia de suscripción caducará próximamente	Se genera una alerta cuando la comprobación diaria de alertas de vencimiento de licencias/mantenimiento pregunta al servidor de licencias y la respuesta es que la licencia vencerá en menos de 30 días.	Plantéese comprar una suscripción nueva.

Alertas de filtrado de URL

Alerta	Descripción	Cómo resolver la alerta
Se ha bloqueado una URL maliciosa	Se genera una alerta cuando el filtrado de URL bloquea una URL maliciosa.	Compruebe la configuración del filtrado de URL. El filtrado de URL bloquea las páginas que se deben bloquear según la configuración del filtrado de URL.
Se ha ignorado una advertencia de URL maliciosa	Se genera una alerta 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	Se genera una alerta 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.
La URL del sitio web está bloqueada	Se genera una alerta cuando una URL cumple todos los criterios especificados en la categoría	Compruebe la configuración del filtrado de URL.

Alerta	Descripción	Cómo resolver la alerta
	bloqueada del filtrado de URL.	

Alertas de EDR

Alerta	Descripción	Cómo resolver la alerta
Incidente detectado	Se genera una alerta cuando se crea un incidente o cuando se actualiza el estado de un incidente existente.	Esta alerta le informa sobre un nuevo incidente o si se ha actualizado un incidente antiguo. Cuando haya visto la alerta, puede cerrarla. Puede abrir el incidente para saber más si es necesario.
Indicador de compromiso (IOC) detectado	Se genera una alerta cuando el servicio de búsqueda de amenazas IOC de la EDR detecta un nuevo indicador de compromiso.	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	Se genera una alerta 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	Se genera una alerta 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 cortafuegos de Windows Defender	Se genera una alerta cuando se modifica la configuración del firewall en el equipo aislado.	Esta alerta le informa de que se han modificado los detalles del firewall en el equipo aislado. Es una alerta meramente informativa y puede cerrarla cuando la haya visto.

Alertas de control de dispositivos

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)	Se genera una alerta cuando se inicia el agente DeviceLock en un equipo físico con CPU compatible con la tecnología CET.	Deshabilite la opción en los equipos afectados para evitar más alertas.

Alerta	Descripción	Cómo resolver la alerta
La funcionalidad de control de dispositivos aún no es compatible con macOS Ventura	Se genera una alerta 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	Se genera una alerta cuando se permite la transferencia de contenido confidencial.	
Transferencia justificada de datos confidenciales	Se genera una alerta cuando se justifica la transferencia de contenido confidencial.	
Transferencia denegada de datos confidenciales	Se genera una alerta cuando se bloquea la transferencia de contenido confidencial.	
Revisar los resultados del modo de observación de la prevención de pérdida de datos	Se genera una alerta cuando toca revisar los resultados de 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 aplicado a al menos una 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	Se genera una alerta cuando se actualiza un SID para un nombre de usuario conocido. Esto puede ocurrir cuando se reinstala el SO en un equipo que no es del dominio.	
El acceso al dispositivo periférico está bloqueado	Se genera una alerta cuando se bloquean algunas acciones (operaciones de lectura/escritura) en dispositivos compatibles.	

Alerta	Descripción	Cómo resolver la alerta
No es posible conectar con un recurso SSL remoto.	Se genera una alerta 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

Alerta	Descripción	Cómo resolver la alerta
El agente está obsoleto	Se genera una alerta cuando la versión del agente está obsoleta.	Vaya a la lista de agentes e inicie la actualización del agente.
Actualización automática fallida	Se genera una alerta cuando falla la actualización automática del agente.	Intente realizar una actualización manual.
Debe reiniciar el dispositivo tras instalar un nuevo agente	Se genera una alerta cuando es necesario reiniciar después de completar una instalación remota.	Reinicie la carga de trabajo.
Fallo en la actividad	Se genera una alerta cuando falla una actividad.	Reinicie todos los servicios de Acronis en el equipo.
La actividad se completó con advertencias	Se genera una alerta cuando se completa una actividad, pero se generan avisos.	
La actividad no responde	Se genera una alerta cuando una actividad en curso no responde.	
No se ha podido implementar el plan	Se genera una alerta cuando falla el despliegue del plan de protección.	
No se pudo convertir el nombre de usuario en SID	Se genera una alerta cuando falla la conversión del SID de planificación.	

Widgets de alertas

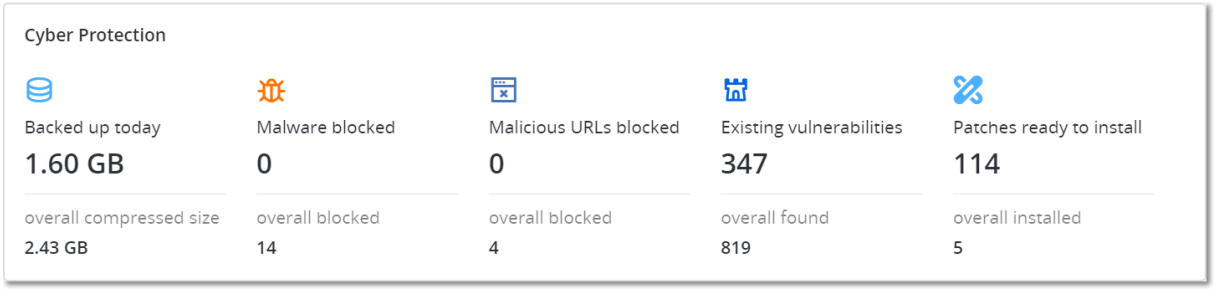
En los widgets de alertas, puede ver la siguiente información de alertas relacionada con su carga de trabajo:

Campo	Descripción
widget de 5 últimas	Una lista de las cinco últimas alertas.

Campo	Descripción
alertas	
Resumen del historial de alertas	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.



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 bloqueados**: 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:

- 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

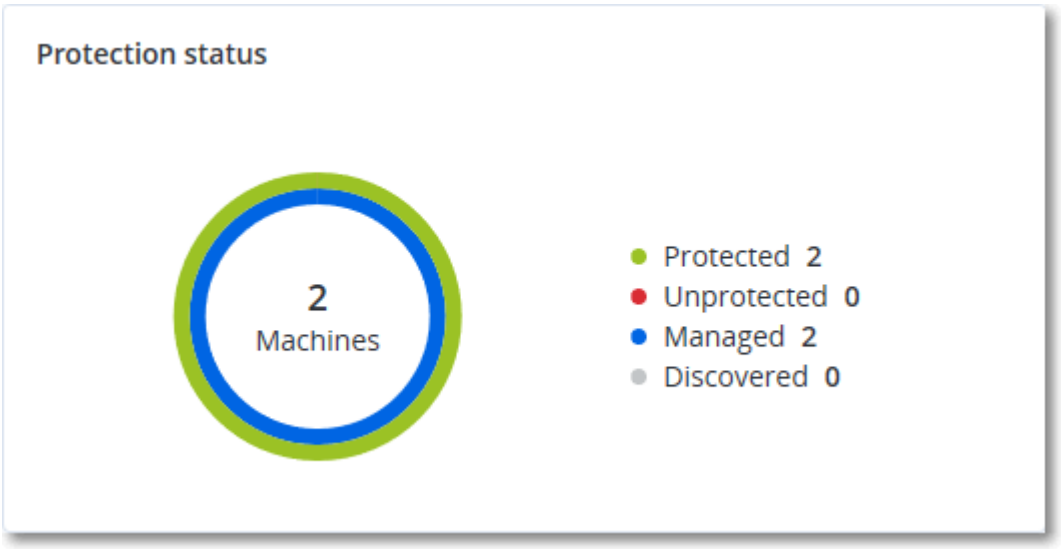
Estado de la protección

Este widget muestra el estado de protección actual de todos los equipos.

Un equipo puede encontrarse en uno de los siguientes estados:

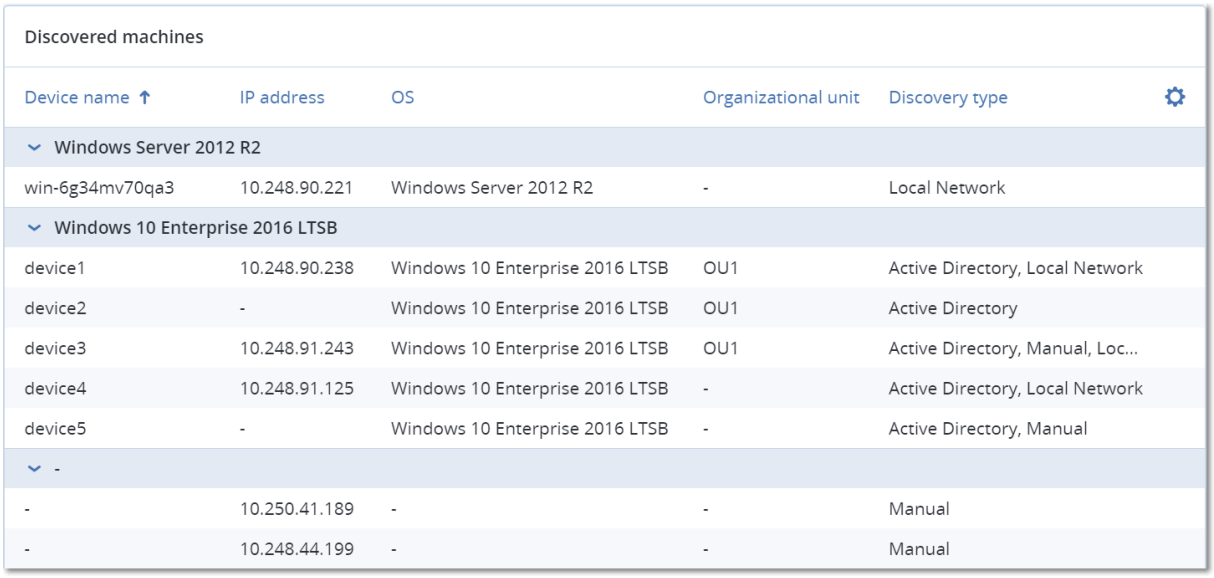
- **Protegido**: equipos con un plan de protección aplicado.
- **Sin protección**: equipos sin un plan de protección aplicado. Incluyen tanto a los equipos detectados como a los gestionados en los que no hay ningún plan de protección aplicado.
- **Gestionado**: equipos en los que está instalado un agente 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.



Equipos detectados

Este widget muestra la lista de equipos detectados en el intervalo de tiempo especificado.



Discovered machines

Device name	IP address	OS	Organizational unit	Discovery type
Windows Server 2012 R2				
win-6g34mv70qa3	10.248.90.221	Windows Server 2012 R2	-	Local Network
Windows 10 Enterprise 2016 LTSB				
device1	10.248.90.238	Windows 10 Enterprise 2016 LTSB	OU1	Active Directory, Local Network
device2	-	Windows 10 Enterprise 2016 LTSB	OU1	Active Directory
device3	10.248.91.243	Windows 10 Enterprise 2016 LTSB	OU1	Active Directory, Manual, Loc...
device4	10.248.91.125	Windows 10 Enterprise 2016 LTSB	-	Active Directory, Local Network
device5	-	Windows 10 Enterprise 2016 LTSB	-	Active Directory, Manual
-				
-	10.250.41.189	-	-	Manual
-	10.248.44.199	-	-	Manual

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. 954)).

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

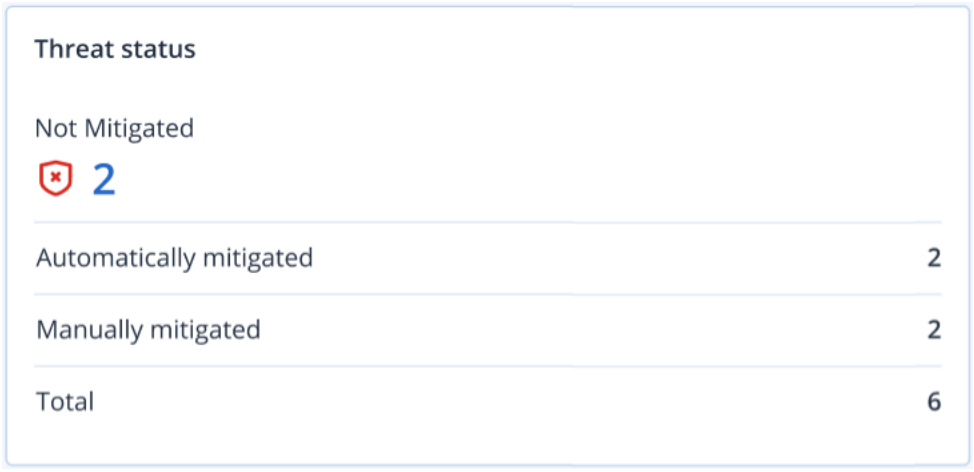
Este widget muestra las cinco cargas de trabajo con más incidentes (haga clic en **Mostrar todo** para volver a la lista de incidentes, que se filtra según los ajustes del widget).

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.

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).

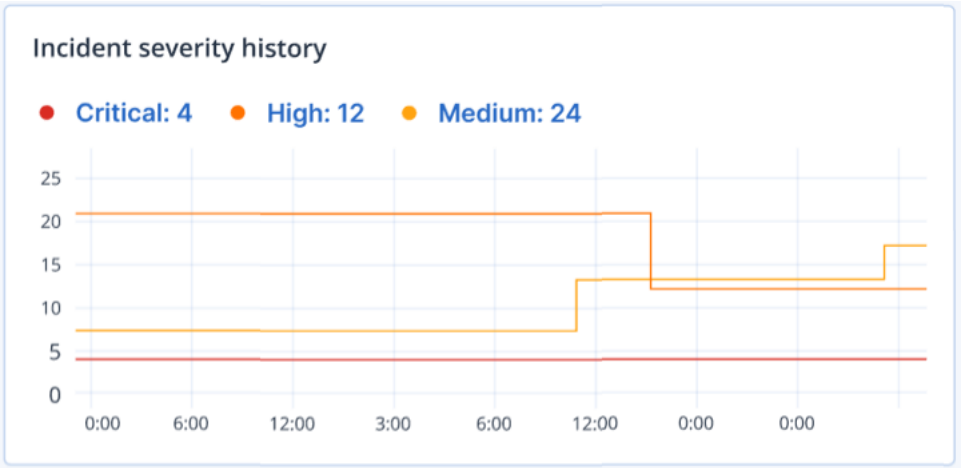
Haga clic en el número **No mitigado** para filtrar la lista de incidentes de manera que se muestren aquellos que no se han mitigado.



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.



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.

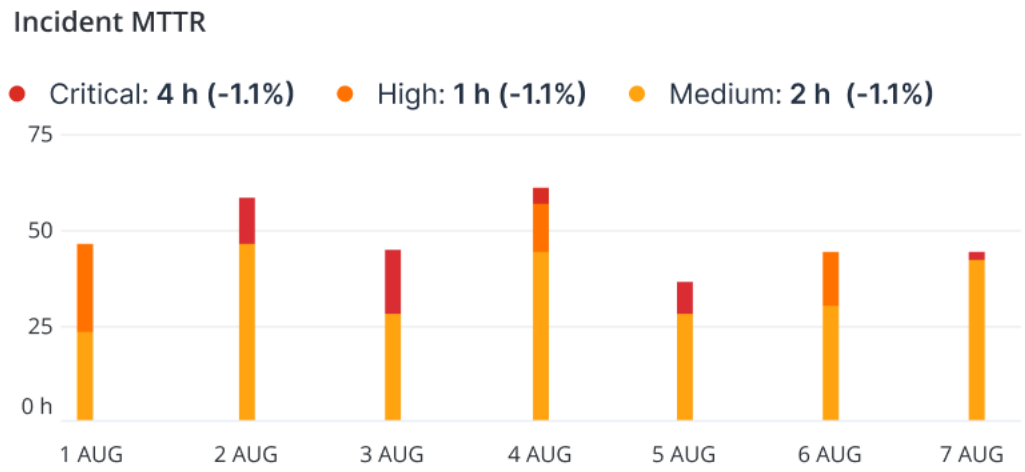
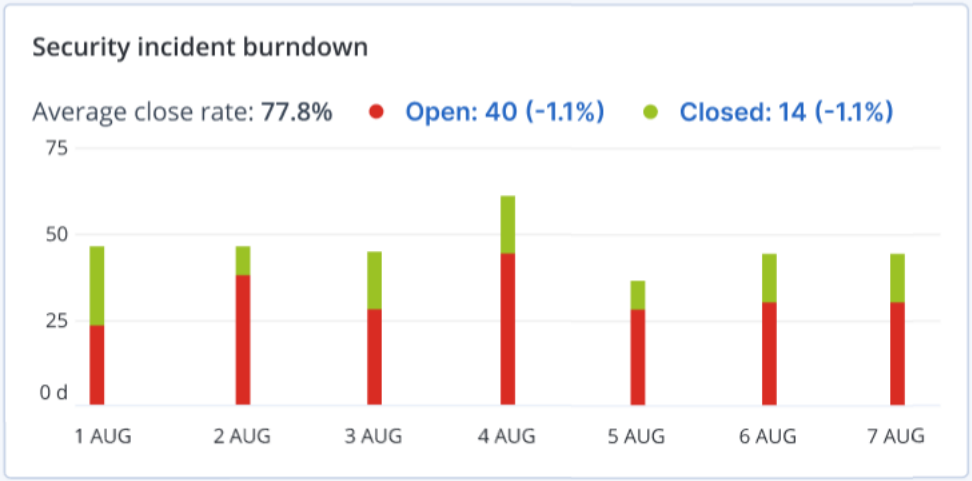


Gráfico de quemado de incidentes de seguridad

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**).

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.

Detection by tactics

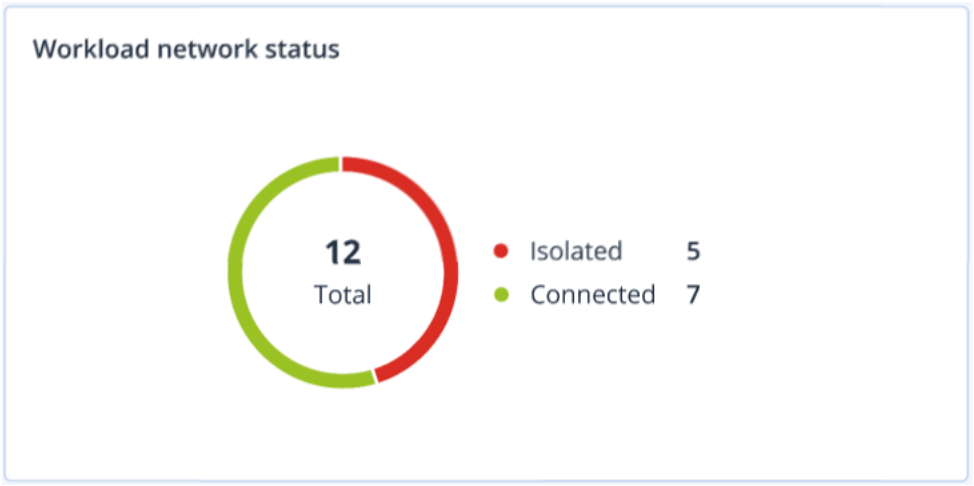
Initial Access	3	Discovery	3
Execution	7	Lateral Movement	0
Persistence	15	Collection	15
Priviledge Escalation	31	Command and Control	31
Defense Evasion	23	Exfiltration	23
Credential Access	7	Discovery	0
Impact	0	Resouce Development	0

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

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.



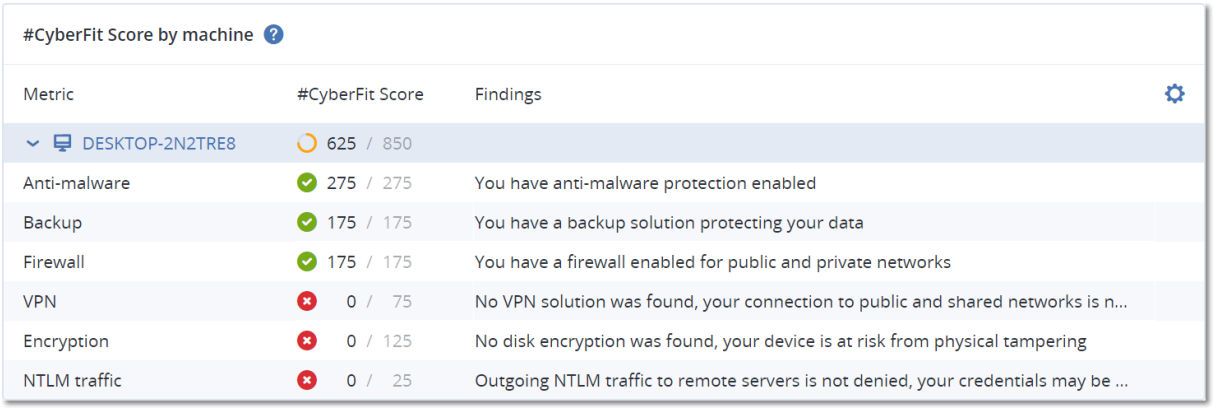
#CyberFit Score por equipo

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".



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.

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

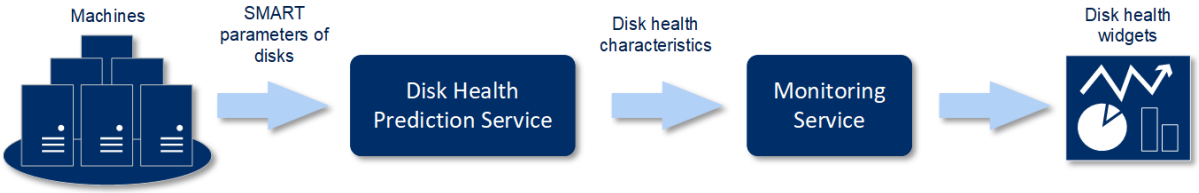
El servicio de predicción de estado del disco utiliza un modelo de predicción basado en la inteligencia artificial.

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.
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

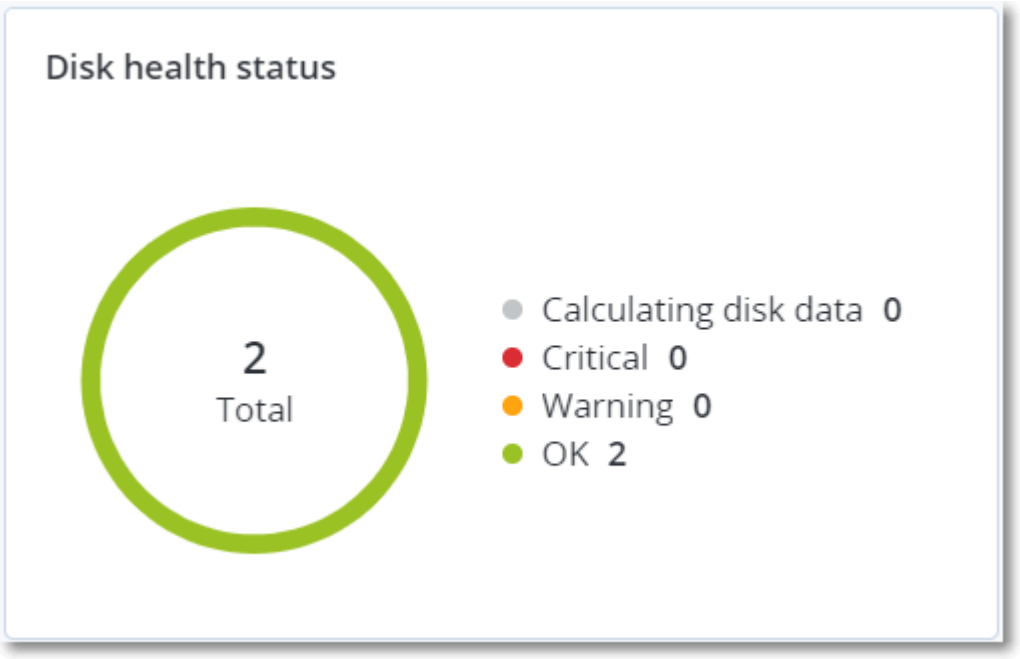
Los resultados de la supervisión del estado del disco se muestran en los siguientes widgets que están disponibles en la consola de Cyber Protect.

- **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.

- 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

- Mejorará

- **Estado del disco**: Es un widget con gráfico circular en el que se muestra el número de discos de cada estado.



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:

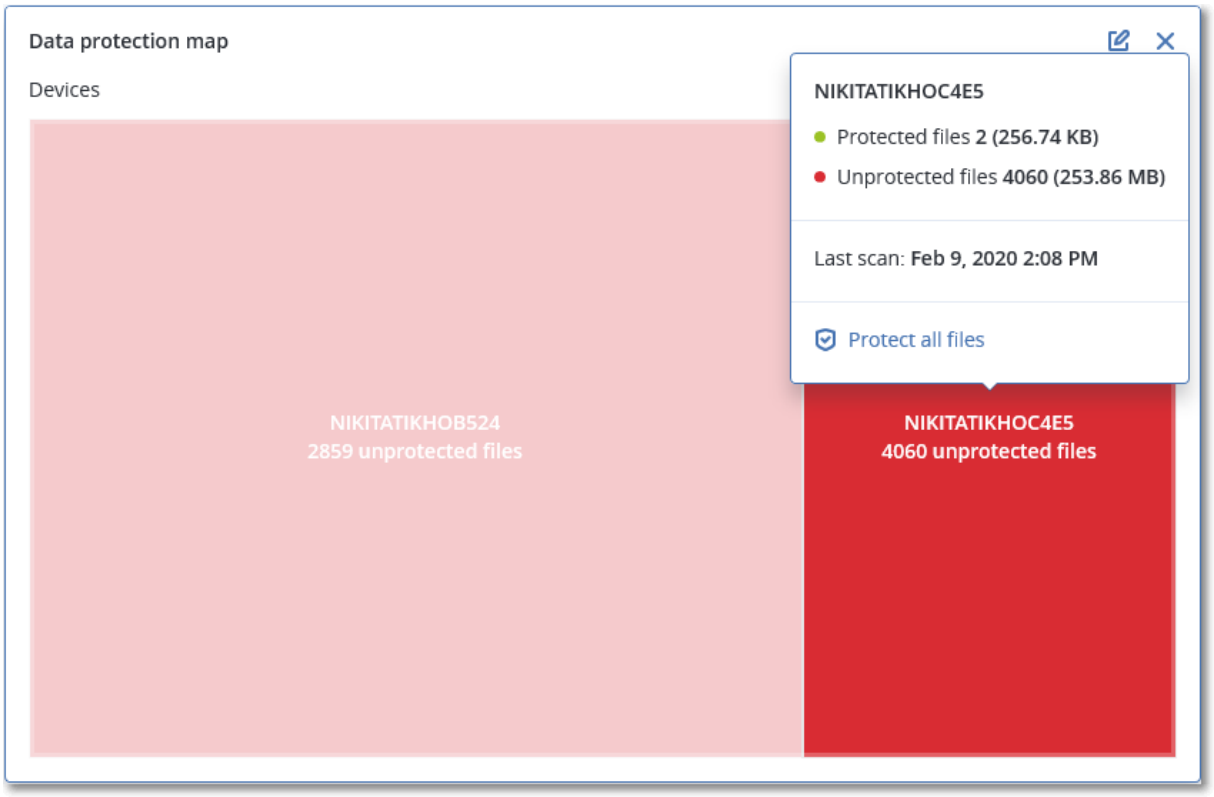
- **Crítico**: hay entre un 51 y un 100 % de archivos sin proteger con las extensiones que ha especificado de los que no se está realizando ni se va a realizar ninguna copia de seguridad con la configuración de copias de seguridad existentes para la ubicación, el inquilino cliente o el equipo seleccionado.
- **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

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.

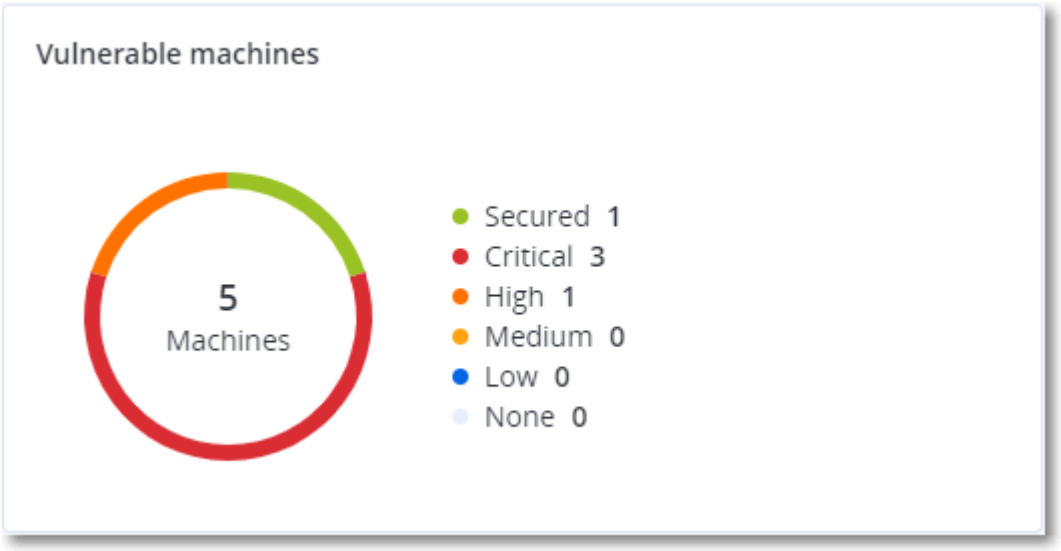
Widgets de evaluación de vulnerabilidades

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



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.

Existing vulnerabilities

Machine name	Vendor	Product	Vulnerability name/ID	Severity	Last detected	First detected
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-7096	Critical	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0856	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0688	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0739	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0752	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0753	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0806	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0810	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0812	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0829	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM

More

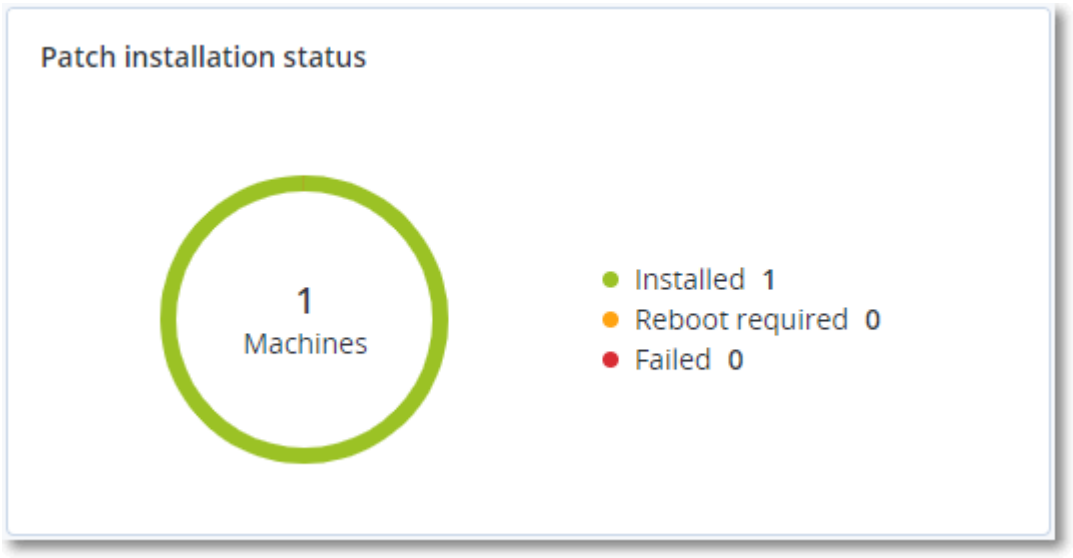
Widgets de instalación de parches

Hay cuatro widgets relacionados con la funcionalidad de gestión de parches.

Estado de instalación del parche

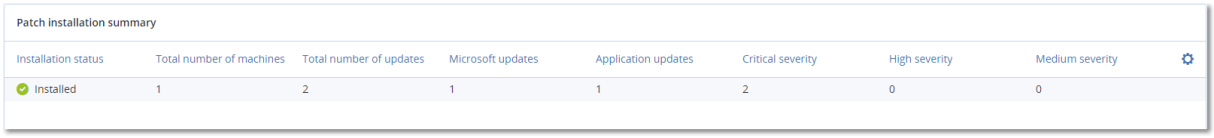
Este widget muestra el número de equipos agrupados por estado de instalación de parches.

- **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.



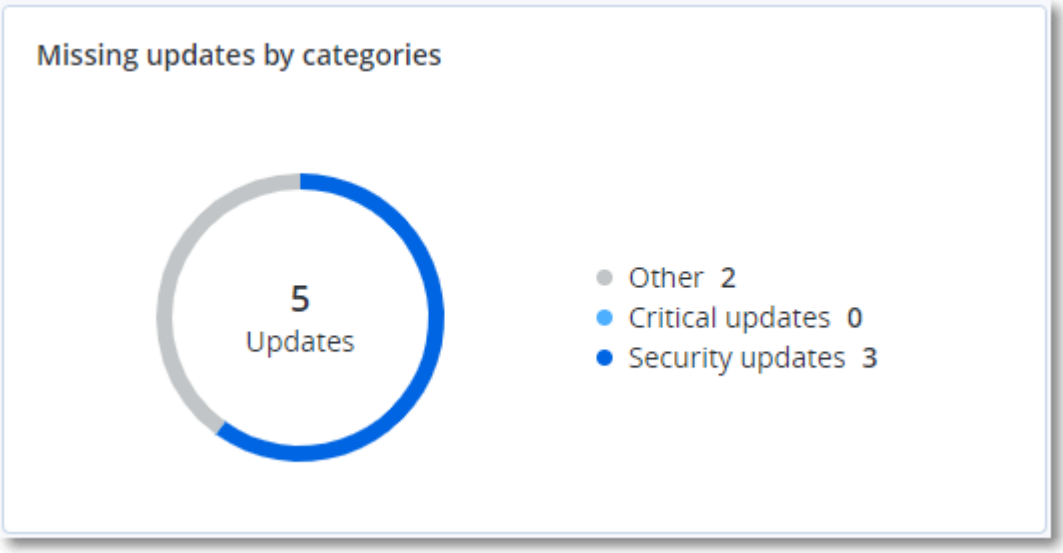
Historial de instalación de parches

Este widget muestra información detallada sobre los parches que hay en los equipos.

Actualizaciones que faltan por categoría

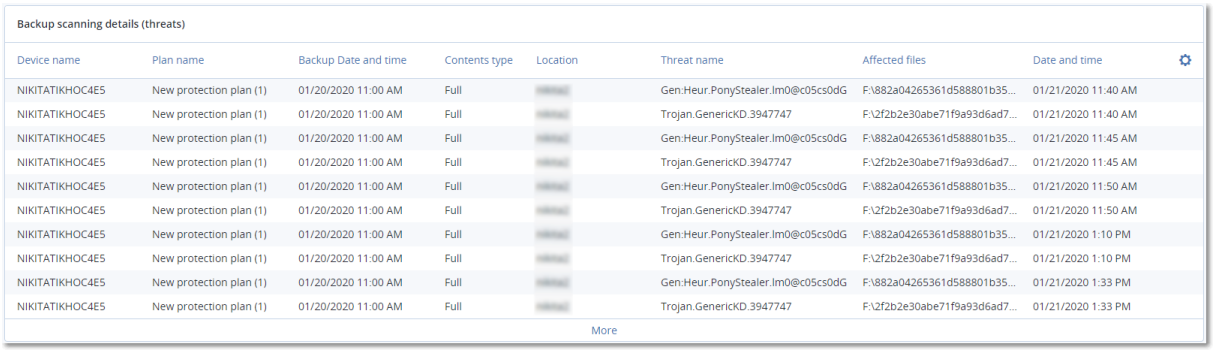
Este widget muestra el número de actualizaciones que faltan por categoría. Se muestran las siguientes categorías:

- Actualizaciones de seguridad
- Actualizaciones críticas
- Otros



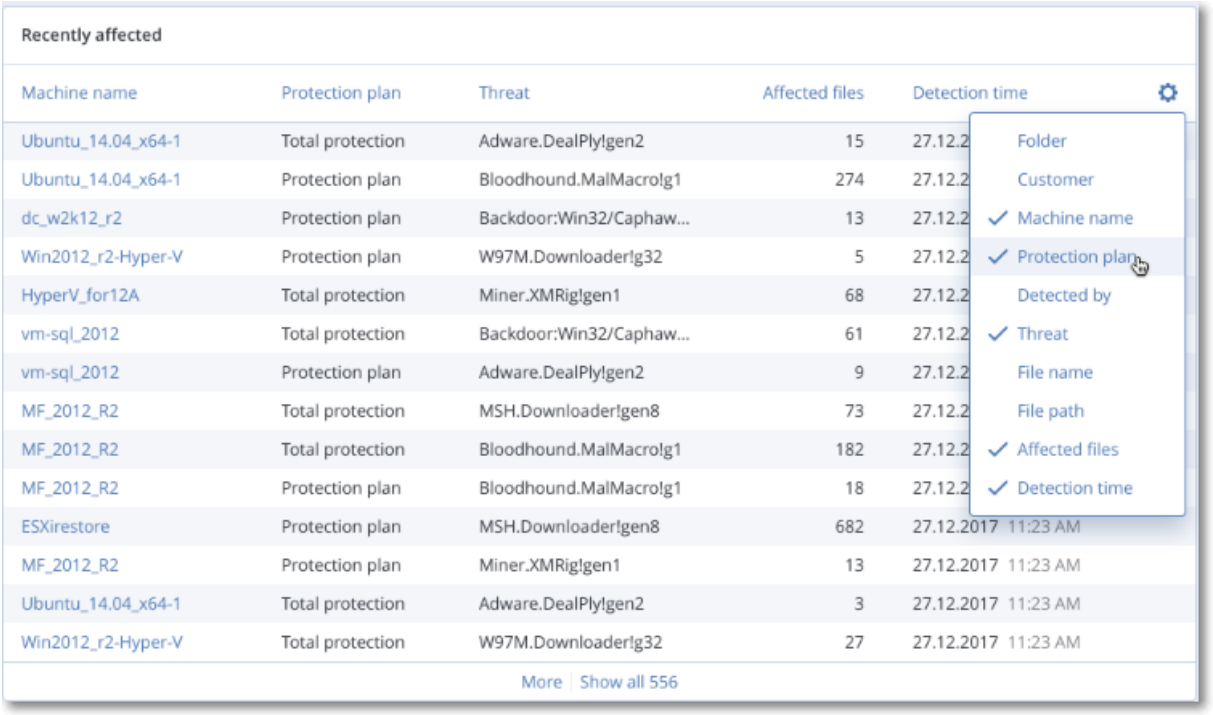
Detalles del análisis de copias de seguridad

Este widget muestra información detallada sobre las amenazas detectadas en las copias de seguridad.



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.



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:

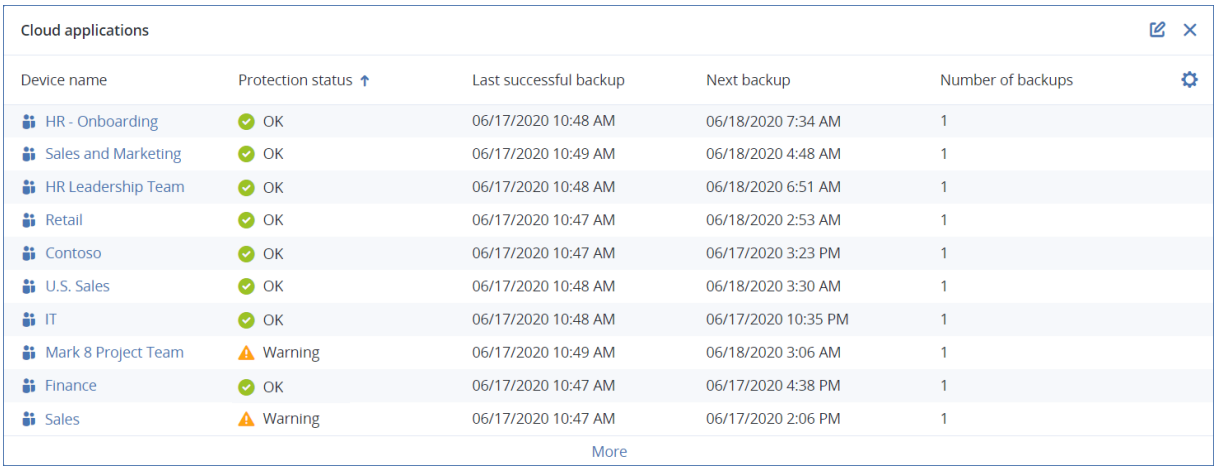
1. En el widget **Elementos afectados recientemente**, haga clic en **Descargar datos**.
2. En el campo **Período**, introduzca el número de días de los cuales desee descargar datos. Solo puede indicar 200 días como máximo.
3. En el campo **Destinatarios**, introduzca las direcciones de correo electrónico 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
- Colecciones de sitios de Microsoft 365
- Equipos de Microsoft 365
- Usuarios de Google Workspace (Gmail, Google Drive)
- Unidades compartidas de Google Workspace



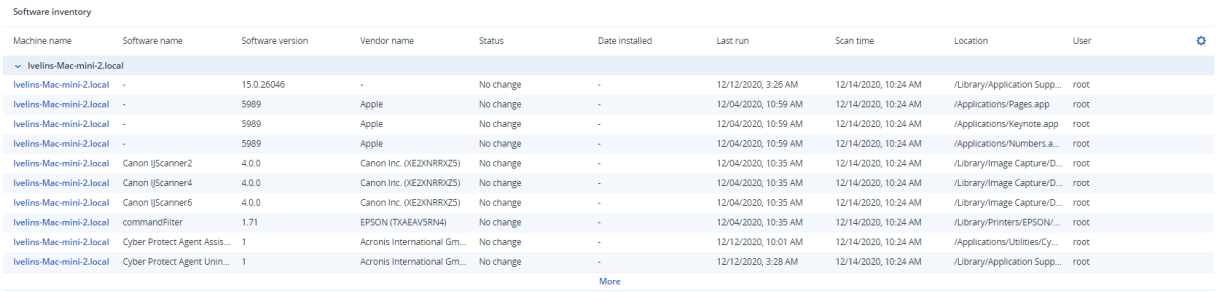
También hay información adicional acerca de los recursos nube a nube en los siguientes widgets:

- Actividades
- Lista de actividades
- 5 últimas alertas
- Historial de alertas
- Resumen de alertas activas

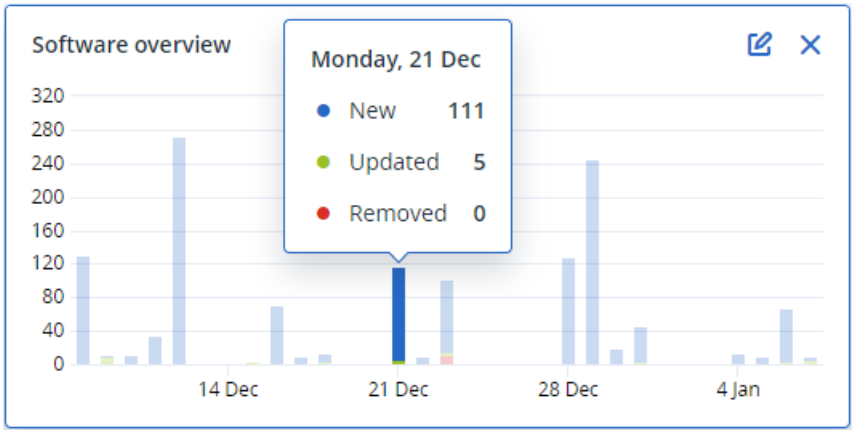
- Resumen del historial de alertas
- Detalles de las alertas activas
- Resumen de ubicaciones

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 en su organización.



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.

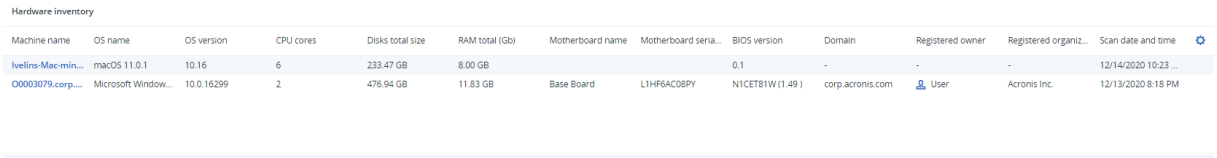
Actualizadas: el número de aplicaciones actualizadas.

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.

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.



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).

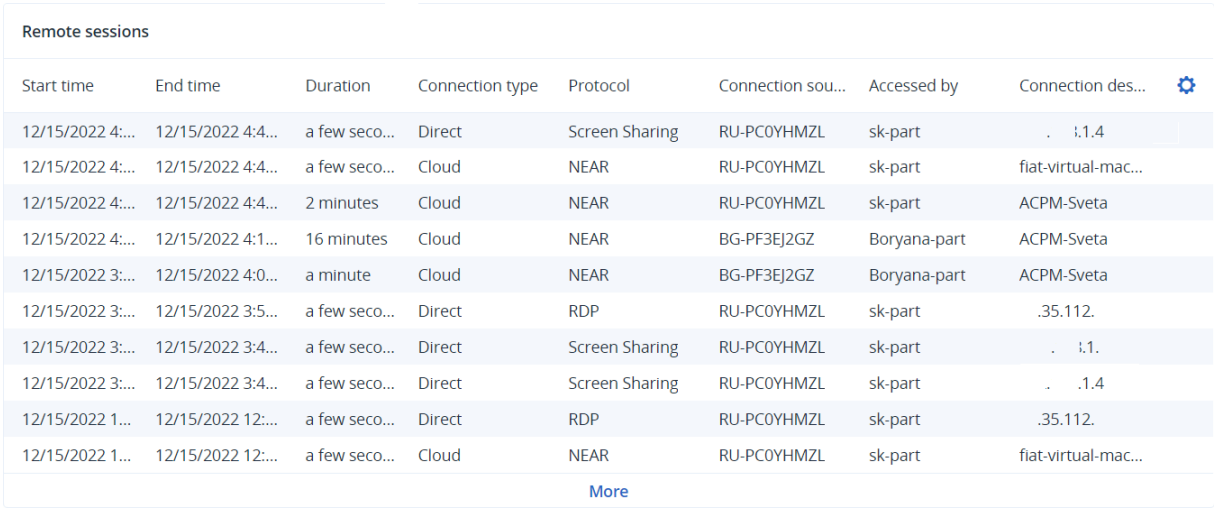
Hardware changes

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

Widget de sesiones remotas

Este widget muestra la información detallada sobre las sesiones de escritorio remoto y de transferencia de archivos.



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.

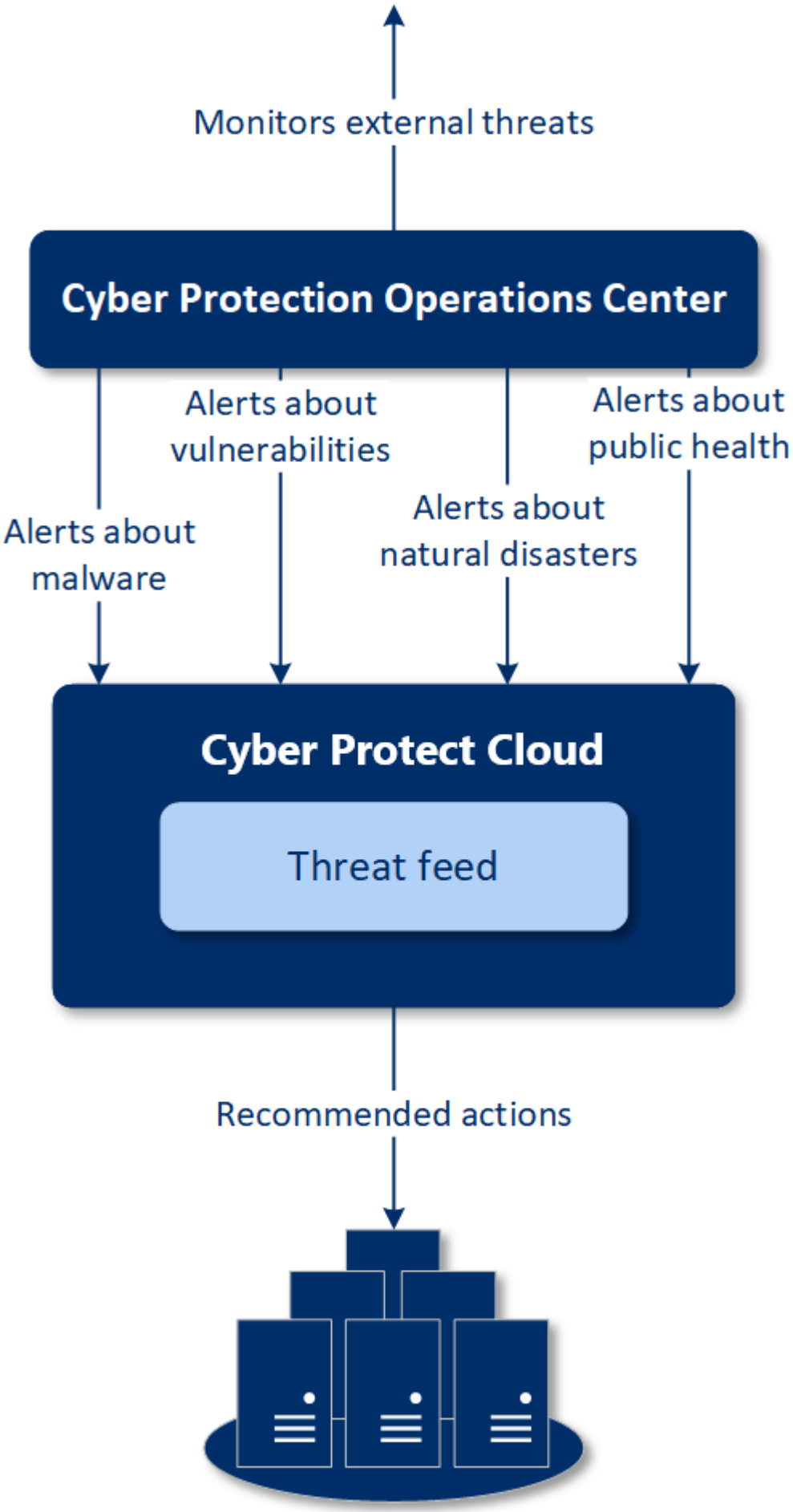
Algunas alertas de seguridad se pueden resolver con las acciones específicas que indican los expertos en seguridad. Otras alertas de seguridad solo le informan sobre las próximas amenazas, pero no hay acciones recomendadas disponibles.

Nota
Las alertas de malware se generan solo en los equipos que tienen instalado el agente para la protección antimalware.

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.

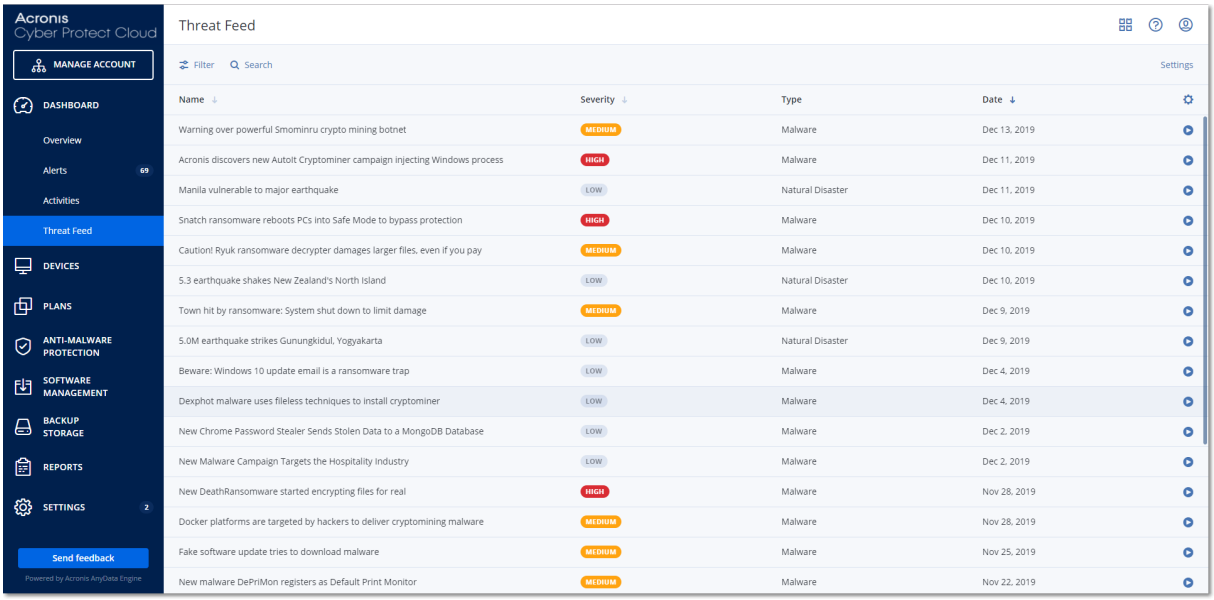


Para ejecutar las acciones de solución de amenazas recomendadas según las alertas recibidas del centro de operaciones de ciberprotección de Acronis, lleve a cabo las siguientes acciones:

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.



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 la funcionalidad Mapa de protección de datos podrá realizar las siguientes acciones:

- Obtener información detallada sobre los datos almacenados (clasificación, ubicaciones, estado de protección y otro tipo de información adicional) en sus equipos.
- Detectar si los datos están protegidos o no. Se considera que los datos están protegidos si lo están con una copia de seguridad (un plan de protección con el módulo de copia de seguridad habilitado).
- 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.

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

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.

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.

- **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

- 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

Cyber Protect Monitor muestra información sobre el estado de protección del equipo en el que está instalado el Agente para Windows o el Agente para Mac, y permite a los usuarios configurar el cifrado de la copia de seguridad y la configuración del servidor proxy.

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 incorporación obligatorio durante el cual los usuarios inician sesión en su propia cuenta de File Sync & Share y seleccionan una carpeta de sincronización personal. Para obtener más información sobre el Agente para File Sync & Share, consulte la Cyber Files Cloud guía del usuario.

Importante
El 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 a continuación 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	• Aplique planes de protección personalizados • Gestione planes de protección que ya están aplicados

Agentes instalados	Los usuarios pueden	Los usuarios no pueden
	• 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. 461). No es posible recuperar copias de seguridad cifradas si se pierde u olvida la contraseña.	
Agente para Windows y Agente para la sincronización y el uso compartido de archivos Agente para Mac y Agente la sincronización y el uso compartido de archivos	• 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	• Edite los tipos de archivos que no se pueden sincronizar

Configuración del servidor proxy en el monitor de Cyber Protect

Puede configurar el servidor proxy en el monitor de Cyber Protect. La configuración afectará a todos los agentes que están instalados en el equipo.

Pasos para configurar el servidor proxy

1. Abra el 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.
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.
5. Haga clic en **Guardar**.
   La configuración del servidor proxy se guarda en el archivo `http-proxy.yaml`.

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. 329).

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.

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.

Acciones con informes

Para ver un informe, haga clic en su nombre.

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.

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.

   Puede hacer lo siguiente:
   - Cambie el nombre al informe.
   - Cambie el intervalo de tiempo de todos los widgets del informe.
   - Especifique los destinatarios del informe y cuándo se les enviará. Los formatos disponibles son PDF y XLSX.

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. Haga clic en el icono de puntos suspensivos (...) y en **Eliminar**.
4. Haga clic en **Eliminar** para confirmar su elección.

Para programar un informe

1. En la consola de Cyber Protect, vaya a **Informes**.
2. En la lista de informes, seleccione el informe que desea programar y haga clic en **Configuración**.
3. Habilite el conmutador **Planificado**.
   - 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.
4. Haga clic en **Guardar**.

Pasos para descargar un informe

1. En la consola de Cyber Protect, vaya a **Informes**.
2. En la lista de informes, seleccione el informe y haga clic en **Descargar**.
3. Seleccione el formato del informe.

Pasos para enviar un informe

1. En la consola de Cyber Protect, vaya a **Informes**.
2. En la lista de informes, seleccione el informe y haga clic en **Enviar**.
3. Especifique las direcciones de correo electrónico de los destinatarios.

4. Seleccione el formato del informe.
5. Haga clic en **Enviar**.

Pasos para exportar la estructura del informe

1. En la consola de Cyber Protect, vaya a **Informes**.
2. En la lista de informes, seleccione el informe.
3. Haga clic en el icono de puntos suspensivos (...) y en **Exportar**.

Como resultado, la estructura del informe se guarda en su equipo como un archivo JSON.

Para volcar los datos del informe

Al utilizar esta opción, puede exportar todos los datos para un periodo personalizado, sin filtrarlos, a un archivo CSV y enviarlo a un destinatario de correo electrónico.

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. Haga clic en el icono de puntos suspensivos (...) y 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.

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
Equipos 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 del historial de alertas	Históricos
Historial de actividad del incidente	Históricos
Resumen de ubicaciones	Reales

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

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.

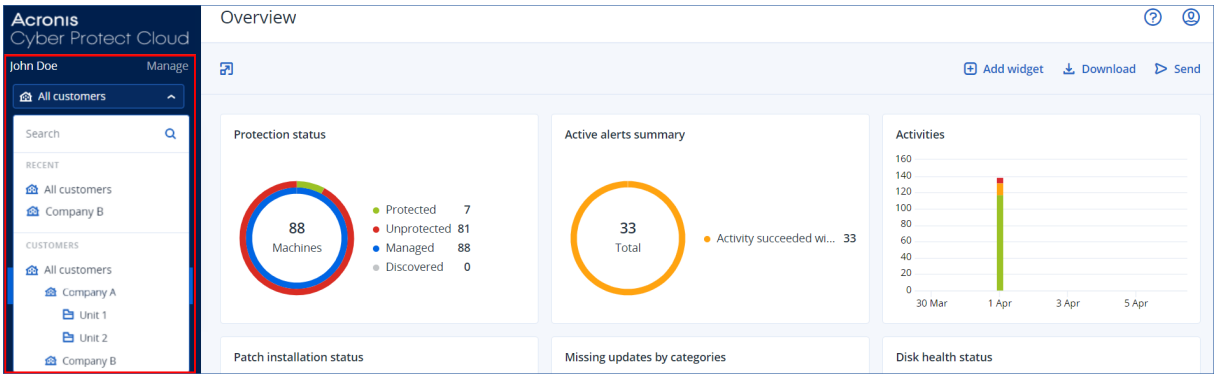
Consola de Cyber Protect

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 características adicionales, como File Sync & Share o protección antivirus y antimalware, 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.

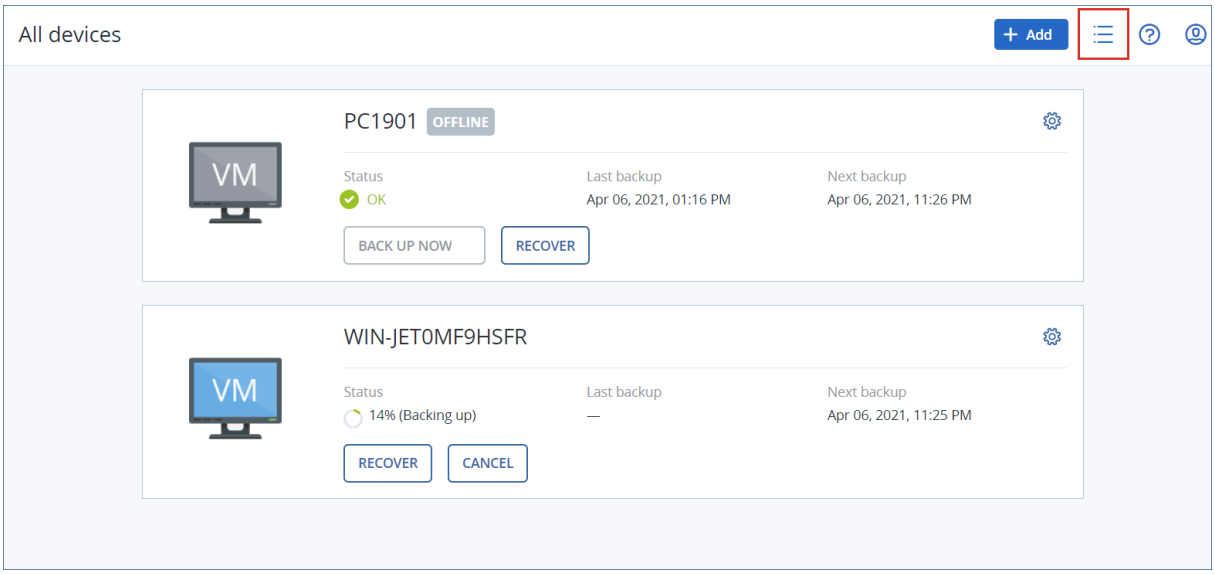
Para comprobar la información más importante acerca de su protección en el panel de control, vaya a **Supervisión** > **Información general**.

En función de sus permisos de acceso, puede gestionar la protección para uno o varios inquilinos cliente o unidades en un inquilino. Para cambiar el nivel de jerarquía, utilice la lista desplegable del menú de navegación. Solo aparecerán los niveles a los que tenga acceso. Para ir al portal de gestión, haga clic en **Gestionar**.

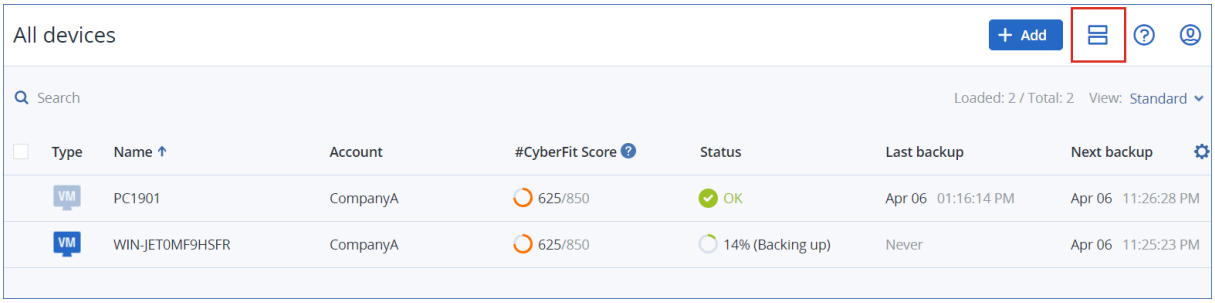


La sección **Dispositivos** está disponible en la vista sencilla y de tabla. Para cambiar entre ellas, haga clic en el icono correspondiente en la esquina superior derecha.

La vista sencilla muestra solo unas pocas cargas de trabajo.



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**.

Uso de la consola de Cyber Protect como administrador de partners

Como administrador de partners, puede utilizar la consola Cyber Protect en el nivel de inquilino partner (**Todos los clientes**) o en el nivel de inquilino del cliente.

Nivel de inquilino partner (**Todos los clientes**)

En el nivel de inquilino partner (**Todos los clientes**), puede realizar las siguientes acciones:

- Gestionar planes de scripts para cargas de trabajo de todos sus inquilinos de cliente gestionados. Puede aplicar el mismo plan de scripts a cargas de trabajo de diferentes clientes y crear grupos de dispositivos con cargas de trabajo de diferentes clientes. Para aprender cómo crear un grupo de dispositivos estático o dinámico en el nivel de partner, consulte "Crear un grupo de dispositivos estáticos en el nivel de partner" (p. 337) y "Crear un grupo dinámico de dispositivos en el nivel de partner" (p. 337). Para obtener más información sobre los scripts y los planes de scripts, consulte "Secuencia de comandos cibernética" (p. 244).
- Cree planes de supervisión para las cargas de trabajo de todos sus inquilinos de cliente gestionados.
- Cree planes de administración remota para las cargas de trabajo de todos sus inquilinos de cliente gestionados.
- Vea y gestione los incidentes de Endpoint Detection and Response (EDR) para todos los inquilinos de los clientes en una única interfaz de gestión de incidentes, en lugar de acceder a la pantalla de incidentes de cada cliente individualmente.
- Ejecute autodetección de máquinas para todos sus inquilinos de cliente gestionados.

Nivel de inquilino de cliente

En este nivel, tiene los mismos derechos que el administrador de la empresa en cuyo nombre actúa.

Seleccionar un nivel de inquilino

Puede seleccionar el nivel de inquilino en el que trabajar en la consola Cyber Protect.

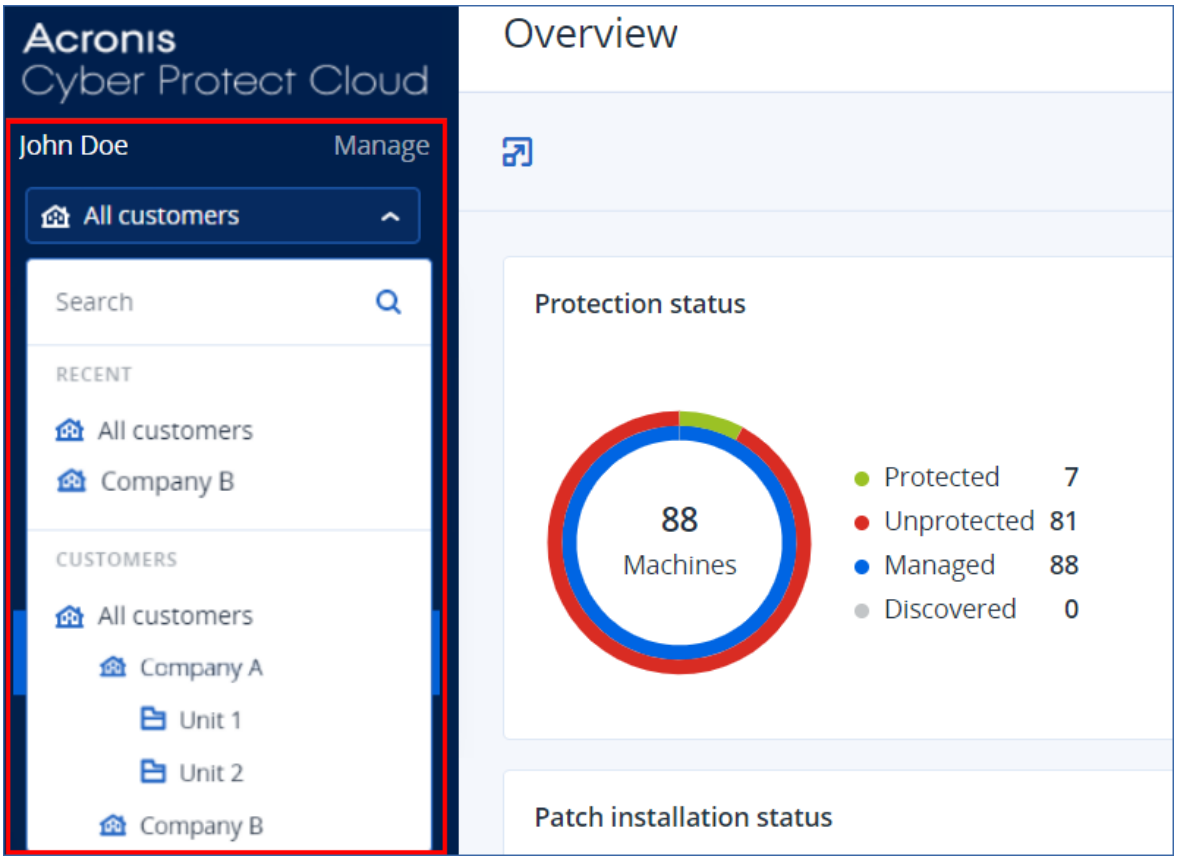
Requisitos previos

- Tiene derechos para acceder tanto a la consola Cyber Protect como al portal de administración.
- Puede gestionar más de un inquilino o unidad.

Para seleccionar un nivel de inquilino en la consola Cyber Protect

1. En el menú de navegación situado a la izquierda, haga clic en la flecha junto al nombre del inquilino de cliente.
2. Seleccione una de las siguientes opciones:
   - Para trabajar en el nivel de partner, seleccione **Todos los clientes**.

- Para trabajar en el nivel de cliente o unidad, seleccione el nombre de dicho cliente o unidad.



Nivel de inquilino partner en la consola Cyber Protect

Cuando utiliza la consola Cyber Protect en el nivel de inquilino partner (**Todos los clientes**), tiene una vista personalizada a su disposición.

Las pestañas **Alertas** y **Actividades** proporcionan otros filtros relacionados con los partner, mientras que las pestañas **Dispositivos** y **Gestión** ofrecen acceso solo a las funciones u objetos accesibles para los administradores partner.

Pestaña Alertas

Aquí puede ver las alertas de todos los clientes que gestiona, buscarlas y filtrarlas según los siguientes criterios:

- Dispositivo
- Cliente
- Plan

Puede seleccionar varios elementos para cada criterio.

Pestaña Actividades

Aquí puede ver las actividades de todos los inquilinos que gestiona o las de un inquilino de cliente específico.

Puede filtrar las actividades por cliente, estado, tiempo y tipo.

Los siguientes tipos de actividades se preseleccionan automáticamente en este nivel:

- Aplicando plan
- Creación del plan de protección
- Plan de protección
- Revocando plan
- Programación

Pestaña Dispositivos

En la pestaña **Equipos con agentes**, puede ver todas las cargas de trabajo de los inquilinos de cliente que gestiona y seleccionar las cargas de trabajo de uno o más inquilinos. También puede crear grupos de dispositivos que incluyan cargas de trabajo de diferentes inquilinos.

Importante
Cuando trabaja a nivel de partner (**Todos los clientes**), puede realizar un número limitado de operaciones con los dispositivos. Por ejemplo, no puede realizar ninguna de las siguientes operaciones:

- Ver y administrar los planes de protección existentes en los dispositivos de los clientes.
- Crear nuevos planes de protección.
- Recuperar copias de seguridad.
- Usar Disaster Recovery.
- Acceder a las funciones del escritorio Cyber Protection.

Para realizar cualquiera de estas operaciones, trabaje en el nivel de cliente.

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

Como administrador partner, puede ver las cargas de trabajo pertenecientes a los inquilinos de cliente que gestiona.

Para ver las cargas de trabajo de un cliente específico

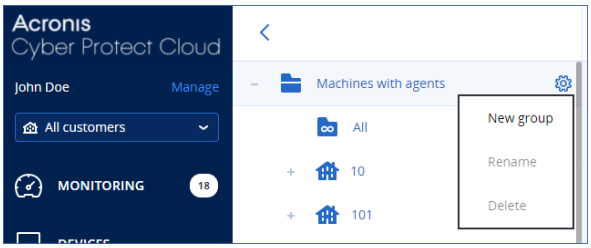
1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Equipos con agentes**.
2. En el árbol, haga clic en **Equipos con agentes** para ampliar la lista.
3. Haga clic en el nombre del cliente cuyas cargas de trabajo desea ver y gestionar.

Crear un grupo de dispositivos estáticos en el nivel de partner

Puede crear grupos de dispositivos estáticos en el nivel de partner (**Todos los dispositivos**).

Pasos para crear un grupo de dispositivos estático 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**.



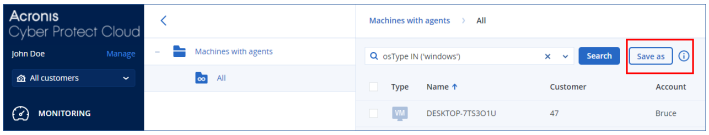
3. Especifique el nombre del grupo.
4. [Opcional] Agregue una descripción.
5. Haga clic en **Aceptar**.

Crear un grupo dinámico de dispositivos en el nivel de partner

Puede crear grupos de dispositivos dinámicos en el nivel de partner (**Todos los dispositivos**).

Pasos para crear un grupo de dispositivos dinámico 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. 361) y "Atributos de búsqueda para cargas de trabajo de la nube a la nube" (p. 360).
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 máquinas en el nivel de inquilino partner

Puede ejecutar la autodetección de máquinas en el nivel de inquilino partner (**Todos los clientes**).

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

1. En la consola Cyber Protect, seleccione **Todos los clientes**.
2. Vaya a **Dispositivos**> **Todos los dispositivos**.
3. Haga clic en **Agregar**.
4. En **Múltiples dispositivos**, haga clic en **Solo Windows**. Se abre el asistente de autodetección.
5. Seleccione un inquilino de cliente y, a continuación, seleccione el agente de detección que realizará el escaneo para detectar máquinas.
6. Seleccione el método de detección:
   - **Buscar en Active Directory**. Asegúrese de que el equipo con el agente de detección esté en el miembro del dominio de Active Directory.
   - **Analizar red local**. Si el agente de detección seleccionado no encuentra ningún equipo, seleccione otro agente de detección.
   - **Especificar manualmente o importar desde un archivo**. Defina manualmente los equipos que quiere añadir o impórtelos desde un archivo de texto.
7. [Si se ha seleccionado el método de detección Active Directory] Seleccione cómo buscar equipos:
   - **En lista de unidades organizativas**. Seleccione el grupo de equipos que se va a añadir.
   - **Mediante consulta en dialecto LDAP**. Utilice la consulta en Dialecto LDAP para seleccionar las máquinas. **Base de búsqueda** define dónde buscar, y en el **Filtro** puede especificar los criterios para la selección de máquinas.
8. Dependiendo del método de detección que haya seleccionado, realice una de las siguientes

acciones:

Método de detección	Acción
Buscar en Active Directory	En la lista de máquinas detectadas, seleccione las máquinas que desee añadir.
Analizar red local	En la lista de máquinas detectadas, seleccione las máquinas que desee añadir.

Especificar manualmente o importar desde un archivo	Especifique las direcciones IP o los nombres de host de las máquinas, o importe la lista de máquinas desde un archivo de texto. El archivo debe contener direcciones IP o nombres de host, uno por línea. Aquí le mostramos un ejemplo:
	`156.85.34.10`
	`156.85.53.32`
	`156.85.53.12`
	`EN-L00000100`
	`EN-L00000101`
	Cuando ya se han añadido las direcciones de los equipos manualmente o se han importado de un archivo, el agente intenta anclar los equipos añadidos y definir su disponibilidad.

9. Seleccione las acciones que deben realizarse después de la detección:

Opción	Descripción
Instalar agentes y registrar máquinas	Para seleccionar qué componentes desea instalar en las máquinas, haga clic en **Seleccionar componentes**. Para obtener más información, consulte "Selección de componentes para la instalación" (p. 136).
Cuenta de inicio de sesión para el servicio de agente	Esta configuración está disponible en la pantalla **Seleccionar componentes**. La configuración define la cuenta desde la que se ejecutarán los servicios. 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. Si elige la opción **Crear una cuenta nueva** o **Utilice la siguiente cuenta**, asegúrese de que las políticas de seguridad del dominio no afecten los derechos

Opción	Descripción
	de las cuentas relacionadas. Si a una cuenta se le priva de los derechos de usuario asignados durante la instalación, el componente podría funcionar incorrectamente o no funcionar en absoluto.
Registrar máquinas con agentes instalados	Utilice esta opción si el agente ya está instalado en las máquinas y solo necesita registrarlas en Cyber Protection. Si no se encuentra ningún agente en las máquinas, se añadirán como máquinas **No administradas**.
Añadir como máquinas no administradas	Si selecciona esta opción, el agente no se instalará en las máquinas. Podrás verlas en la consola e instalar o registrar el agente más tarde.
Reiniciar la máquina si es necesario	Esta opción aparece cuando se selecciona **Instalar agentes y registrar máquinas**. Si selecciona esta opción, la máquina se reiniciará tantas veces como sea necesario para completar la instalación. Se puede requerir que se reinicie el equipo en uno de los siguientes casos: • La instalación de los requisitos previos se ha completado, y es necesario reiniciar para continuar con la instalación. • La instalación se ha completado, pero es necesario reiniciar, ya que algunos archivos han quedado bloqueados durante la instalación. • La instalación se ha completado, pero es necesario reiniciar para el correcto funcionamiento de otro software previamente instalado.
No reiniciar si el usuario ha iniciado sesión	Esta opción aparece cuando se selecciona **Reiniciar la máquina si es necesario**. Al seleccionar esta opción, la máquina no se reiniciará automáticamente si el usuario ha iniciado sesión en el sistema. Por ejemplo, si un usuario está trabajando mientras la instalación requiere un reinicio, el sistema no se reiniciará. Si los requisitos previos se han instalado pero la máquina no se ha reiniciado porque un usuario había iniciado sesión, debe reiniciar la máquina y volver a iniciar la instalación para que esta pueda completarse. Si el agente se ha instalado pero no se ha reiniciado la máquina a continuación, debe reiniciar la máquina.
Usuario donde registrar las máquinas	[Si hay unidades en su organización] Seleccione la cuenta de usuario de la unidad o unidades subordinadas en las que desea registrar las máquinas. [Al ejecutar la autodetección en el nivel de inquilino partner] En la lista de inquilinos de cliente que administra, expanda la estructura de árbol y, a continuación, seleccione la cuenta de usuario en la que desea registrar las máquinas. [Al ejecutar la autodetección como administrador del cliente] Si ha seleccionado **Instalar agentes y registrar máquinas** o **Registrar máquinas con agentes instalados**, también existe la opción de aplicar el plan de protección a las máquinas. Si dispone de varios planes de protección, puede seleccionar cuál desea usar.

10. Especifique las credenciales del usuario con derechos de administrador para todos los equipos.

    Importante
    La instalación remota de agentes funciona sin ninguna preparación solo 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 como se describe en "Requisitos previos" (p. 338).

11. El sistema comprueba la conectividad a todos los equipos. Si la conexión a alguno de los equipos falla, puede cambiar las credenciales de esos equipos.

Después de iniciar la detección de máquinas, puede ver la tarea correspondiente en la actividad **Supervisión**> **Actividades** > **Detección de máquinas**.

Compatibilidad con varios inquilinos

El servicio de Cyber Protection admite varios inquilinos, lo que implica la administración en los siguientes niveles:

- [Para proveedores de servicios] Nivel de inquilino partner (**Todos los clientes**)
  Este nivel solo está disponible para los administradores de partners que gestionan inquilinos de cliente.
- Nivel de inquilino de cliente
  Este nivel lo gestionan los administradores de empresa.
  Los administradores de partners también pueden trabajar en este nivel en los inquilinos de cliente que gestionen. En este nivel, los administradores de partners tienen los mismos derechos que los administradores de clientes en cuyo nombre actúan.
- Nivel de unidad
  Este nivel lo gestionan los administradores de unidad y los administradores de empresa desde el inquilino de cliente principal.
  Los administradores de partners que gestionan el inquilino de cliente principal pueden acceder también al nivel de unidad. En este nivel, tienen los mismos derechos que los administradores de clientes en cuyo nombre actúan.

Los administradores pueden gestionar objetos en su propio inquilino y en los inquilinos secundarios correspondientes. No pueden ver objetos en un nivel de administración más alto, si los hay, ni acceder a ellos.

Por ejemplo, los administradores de empresa pueden gestionar planes de protección en el nivel de inquilino 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 ningún plan de protección en el nivel de inquilino de cliente ni los planes de protección creados por el administrador de clientes en el nivel de unidad.

Los administradores de partners también pueden crear y aplicar planes de programación en los inquilinos de cliente que gestionen. Los administradores de empresa de esos inquilinos tienen

acceso de solo lectura a los planes de programación que aplica un administrador de partners a sus cargas de trabajo. Sin embargo, los administradores de cliente pueden crear y aplicar sus propios planes de programación y protección.

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. 61).

Un dispositivo virtual es una máquina virtual disponible que incluye un agente de protección. Con un dispositivo virtual, puede hacer copias de seguridad de otras máquinas virtuales en el mismo entorno sin instalar un agente de protección (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. 32).

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

Tipo de carga de trabajo	Agente	Ejemplos (lista parcial)
		oVirt
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. 629). .	Buzón de correo de Microsoft 365 Microsoft 365 OneDrive Microsoft Teams Sitio de SharePoint 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. 64)

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. 348).

Pasos para añadir una carga de trabajo

1. Inicie sesión en la consola de Cyber Protect.
2. Vaya a **Dispositivos** > **Todos los dispositivos** y haga clic en **Añadir**.
   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.	"Ejecutar la autodetección y la detección manual" (p. 131)
Estaciones de trabajo de Windows Servidores de Windows	Instale el Agente para Windows.	"Instalación de agentes de protección en Windows" (p. 80) o "Instalación o desinstalación sin supervisión en Windows" (p. 90)
Estaciones de trabajo de macOS	Instale el Agente para macOS.	"Instalación de agentes de protección en macOS" (p. 85) o "Instalación sin supervisión e instalación en macOS" (p. 114)
Servidores de Linux	Instale el Agente para Linux.	"Instalación de agentes de protección en Linux" (p. 82)

Cargas de trabajo que se van a añadir	Acción necesaria	Procedimiento a seguir
		o "Instalación o desinstalación sin supervisión en Linux" (p. 108)
Dispositivos móviles (iOS y Android)	Instale la aplicación móvil.	"Protección de dispositivos móviles" (p. 621)
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 de la nube, consulte "Protección de los datos de Microsoft 365" (p. 629).	"Protección de los datos de Microsoft 365" (p. 629)
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. 676)
Equipos virtuales		
VMware ESXi	Despliegue el Agente para VMware (dispositivo virtual) en su entorno.	"Implementación de Agente para VMware (dispositivo virtual)" (p. 139)
	Instale el Agente para VMware (Windows).	"Instalación de agentes de protección en Windows" (p. 80) o "Instalación o desinstalación sin supervisión en Windows" (p. 90)
Virtuozzo Hybrid Infrastructure	Despliegue el Agente para Virtuozzo Hybrid Infrastructure	"Implementación del Agente para Virtuozzo Hybrid Infrastructure

Cargas de trabajo que se van a añadir	Acción necesaria	Procedimiento a seguir
	(dispositivo virtual) en su entorno.	(dispositivo virtual)" (p. 149)
Hyper-V	Instale el Agente para Hyper-V.	"Instalación de agentes de protección en Windows" (p. 80) o "Instalación o desinstalación sin supervisión en Windows" (p. 90)
Virtuozzo	Instale el Agente para Virtuozzo.	"Instalación de agentes de protección en Linux" (p. 82) o "Instalación o desinstalación sin supervisión en Linux" (p. 108)
KVM	Instale el Agente para Windows.	"Instalación de agentes de protección en Windows" (p. 80) o "Instalación o desinstalación sin supervisión en Windows" (p. 90)
	Instale el Agente para Linux.	"Instalación de agentes de protección en Linux" (p. 82) o "Instalación o desinstalación sin supervisión en Linux" (p. 108)
Red Hat Virtualization (oVirt)	Despliegue el Agente para oVirt (dispositivo virtual) en su entorno.	"Implementando Agent para oVirt (dispositivo virtual)" (p. 158)
Citrix XenServer	Instale el Agente para Windows.	"Instalación de agentes de protección en Windows" (p. 80) o "Instalación o desinstalación sin supervisión en Windows" (p. 90)
	Instale el Agente para Linux.	"Instalación de agentes de protección en Linux" (p. 82) o "Instalación o desinstalación sin supervisión en Linux" (p. 108)
Nutanix AHV	Instale el Agente para Windows.	"Instalación de agentes de

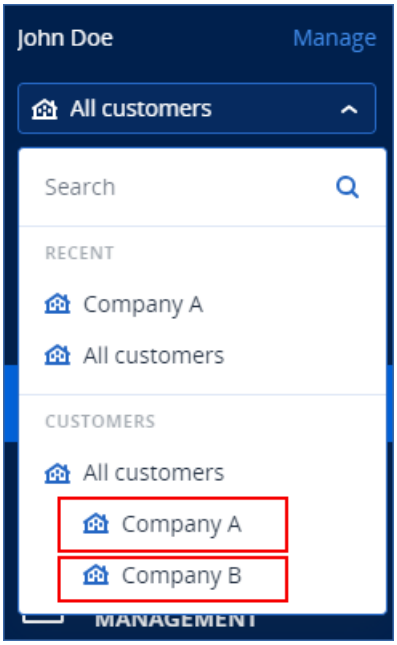
Cargas de trabajo que se van a añadir	Acción necesaria	Procedimiento a seguir
		protección en Windows" (p. 80) o "Instalación o desinstalación sin supervisión en Windows" (p. 90)
	Instale el Agente para Linux.	"Instalación de agentes de protección en Linux" (p. 82) o "Instalación o desinstalación sin supervisión en Linux" (p. 108)
MV Oracle	Instale el Agente para Windows.	"Instalación de agentes de protección en Windows" (p. 80) o "Instalación o desinstalación sin supervisión en Windows" (p. 90)
	Instale el Agente para Linux.	"Instalación de agentes de protección en Linux" (p. 82) o "Instalación o desinstalación sin supervisión en Linux" (p. 108)
Scale Computing HC3	Despliegue el Agente para Scale Computing HC3 (dispositivo virtual) en su entorno.	"Implementación de Agent para Scale Computing HC3 (dispositivo virtual)" (p. 144)
Almacenamiento conectado a red		
Synology	Despliegue el Agente para Synology (dispositivo virtual) en su entorno.	"Implementar Agente para Synology" (p. 164)
Aplicaciones		
Microsoft SQL Server	Instale el Agente para SQL.	"Instalación de agentes de protección en Windows" (p. 80) o "Instalación o desinstalación sin supervisión en Windows" (p. 90)
Microsoft Exchange Server	Instale el Agente para Exchange.	
Microsoft Active Directory	Instale el Agente para Active Directory.	
Oracle Database	Instale el Agente para Oracle.	"Protección de Oracle Database" (p. 705)

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. 712)

Para obtener más información sobre los agentes de protección disponibles y dónde instalarlos, consulte "¿Qué Agente necesito?" (p. 64)

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 artículos 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.

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. 351) (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. 351) (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. 351) (Carga de trabajo de la nube a la nube)

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. 351) (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. 351) (Carga de trabajo con un agente de protección)
Aplicaciones		
Microsoft SQL Server Microsoft Exchange Server Microsoft Active Directory Oracle Database	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. 351) (Carga de trabajo sin un agente de protección)

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. 351) (Sitio web)

Pasos para eliminar una carga de trabajo de la consola de Cyber Protect

Carga de trabajo con un agente de protección

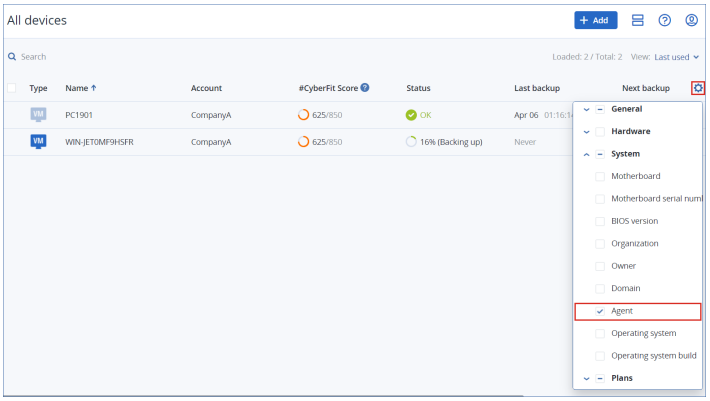
Puede eliminar este tipo de carga de trabajo directamente.

1. En la consola 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. 187).

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**.

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. 187).

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 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 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.

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.

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:

- 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.

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	**Administración** > **Copia de seguridad de aplicaciones en la nube**
Cargas de trabajo que no son de nube a nube	Plan de protección	**Administración** > **Planes de protección**
	Plan de administración remota	**Administración** > **Planes de administración remota**
	Plan de programación	**Administración** > **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.

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**.

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 **Añadir**.

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

trabajo que no son de nube a nube" (p. 361) y "Atributos de búsqueda para cargas de trabajo de la nube a la nube" (p. 360).

Los grupos dinámicos se crean en sus respectivos grupos raíz. No se admiten grupos dinámicos anidados.

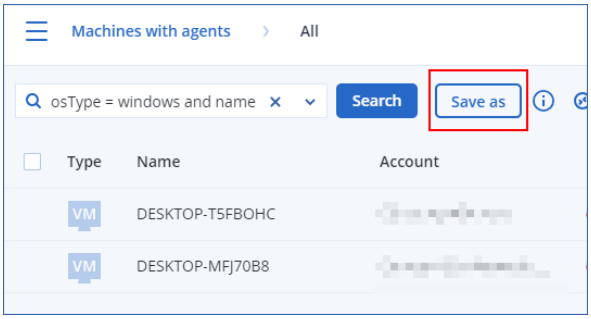
No se pueden crear grupos de dispositivos en ningún grupo de tipo **Todos**, como el grupo raíz **Todos los dispositivos** ni grupos integrados como **Equipos con agentes** > **Todos**, **Microsoft 365** > su organización > **Usuarios** > **Todos los usuarios**.

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. 361).
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**.

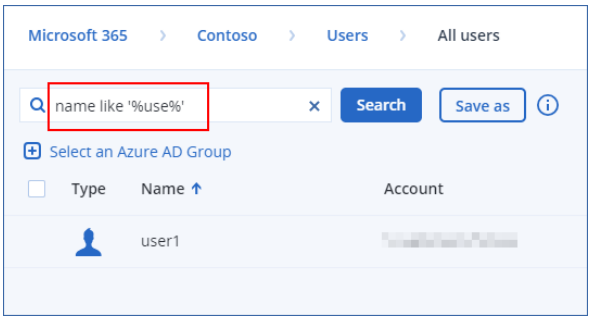
4. Especifique un nombre para el nuevo grupo.
5. [Opcional] En el campo **Comentario**, añada una descripción del nuevo grupo.
6. Haga clic en **Aceptar**.

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**.

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.

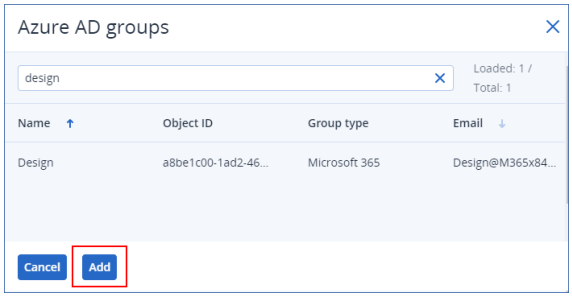
   Puede usar múltiples atributos y operadores en una sola consulta. Para obtener más información sobre los atributos admitidos, consulte "Atributos de búsqueda para cargas de trabajo de la nube a la nube" (p. 360).



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.

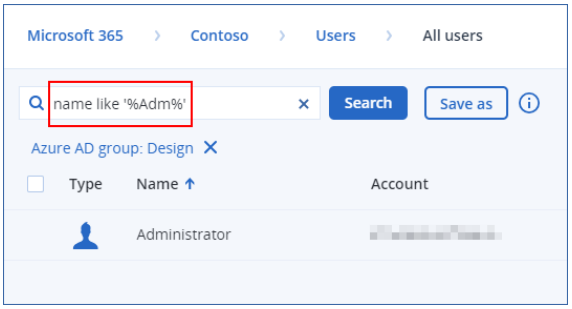
      En esta lista, puede buscar un grupo específico u ordenar los grupos por nombre o correo electrónico.
   c. Seleccione el grupo de Active Directory que desee y haga clic en **Añadir**.



   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

trabajo de la nube a la nube" (p. 360).



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**.

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. 361).

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
			`email = 'my_group_email@mycompany.com'`
			`email LIKE '*@company*'`
			`email NOT LIKE`
				Sí

Atributo	Significado	Se puede utilizar en	Ejemplos de consultas de búsqueda	Se admite para la creación de grupos
		Google Workspace > Usuarios	`'*enterprise.com'`	
`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. 360).

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 equipos físicos • Nombre para equipos virtuales • Nombre de la base de datos • Dirección de correo electrónico para buzones de correo	`name = 'en-00'`	Sí

Atributo	Significado	Ejemplos de consultas de búsqueda	Se admite para la creación de grupos
`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'` • `'virtual_cluster.vmwesx'` • `'virtual_appliance.vmwesx'` • `'virtual_application.vmwesx'` • `'virtual_resource_pool.vmwesx'`	`resourceType = 'machine'` `resourceType in ('mssql_aag_database', 'mssql_database')`	Sí

Atributo	Significado	Ejemplos de consultas de búsqueda	Se admite para la creación de grupos
	• '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_host.mshyperv' • 'virtual_network.mshyperv' • 'virtual_folder.mshyperv' • 'virtual_data_center.mshyperv' • 'datastore.mshyperv' • 'virtual_machine.msvs' • 'virtual_machine.parallelsw' • 'virtual_host.parallelsw' • 'virtual_cluster.parallelsw' • 'virtual_machine.rhev' • 'virtual_machine.kvm' • 'virtual_machine.xen' • 'bootable_media'		
chassis	Tipo de chasis. Valores posibles: • laptop • desktop • server	chassis = 'laptop' chassis IN ('laptop', 'desktop')	Sí

Atributo	Significado	Ejemplos de consultas de búsqueda	Se admite para la creación de grupos
	• `other` • unknown		
`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`	`comment = 'important machine'` `comment = ''` (todos los equipos sin ningún comentario)	Sí

Atributo	Significado	Ejemplos de consultas de búsqueda	Se admite para la creación de grupos
	`net start mms` 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.		

Atributo	Significado	Ejemplos de consultas de búsqueda	Se admite para la creación de grupos
	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 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		

Atributo	Significado	Ejemplos de consultas de búsqueda	Se admite para la creación de grupos
	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 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

Atributo	Significado	Ejemplos de consultas de búsqueda	Se admite para la creación de grupos
`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. Valores posibles: • `'windows'` • `'linux'` • `'macosx'`	`osType = 'windows'` `osType IN ('linux', 'macosx')`	Sí
`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.	`osProductType = 'server'`	Sí

Atributo	Significado	Ejemplos de consultas de búsqueda	Se admite para la creación de grupos
	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'`		
`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
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 `agente`.	`hostId = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	Sí
`virtualType`	Tipo de máquina virtual. Valores posibles: • `'vmwesx'` Máquinas virtuales	`virtualType = 'vmwesx'`	Sí

Atributo	Significado	Ejemplos de consultas de búsqueda	Se admite para la creación de grupos
	VMware. • `'mshyperv'` Máquinas virtuales Hyper-V. • `'pcs'` Máquinas virtuales Virtuozzo. • `'hci'` Máquinas virtuales de Virtuozzo Hybrid Infrastructure. • `'scale'` Máquinas virtuales de Scale Computing HC3. • `'ovirt'` Máquinas virtuales oVirt		
`insideVm`	Equipo virtual con un agente dentro. Valores posibles: • `true` • `false`	`insideVm = true`	Sí
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	`ou IN ('RnD', 'Computers')`	Sí

Atributo	Significado	Ejemplos de consultas de búsqueda	Se admite para la creación de grupos
	organizativa de Active Directory.		
Rango			
`state`	Estado del dispositivo. Valores posibles: • `'idle'` • `'interactionRequired'` • `'canceling'` • `'backup'` • `'recover'` • `'install'` • `'reboot'` • `'failback'` • `'testReplica'` • `'run_from_image'` • `'finalize'` • `'failover'` • `'replicate'` • `'createAsz'` • `'deleteAsz'` • `'resizeAsz'`	`state = 'backup'`	No
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 **Administración** > **Planes**	`protectedByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	No

Atributo	Significado	Ejemplos de consultas de búsqueda	Se admite para la creación de grupos
	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.		
`okByPlan`	Dispositivos que están protegidos por un plan de protección con un ID determinado y tienen el estado **Bueno**.	`okByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	No
`errorByPlan`	Dispositivos que están protegidos por un plan de protección con un ID determinado y tienen el estado **Error**.	`errorByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	No
`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

Atributo	Significado	Ejemplos de consultas de búsqueda	Se admite para la creación de grupos
`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.
	El formato es `'AAAA-MM-DD HH:MM'`.
		`lastVAScanTime > '2023-03-11'`
		`lastVAScanTime <= '2023-03-11 00:15'`
		`lastVAScanTime is null`
			Sí

`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`.

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')`
`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
			`name LIKE 'en-00'`
			`name LIKE '*en-00'`
			`name LIKE '*en-00*'`
			`name LIKE 'en-00_'`

Operador	Compatibilidad con	Significado	Ejemplos
		representa a ningún carácter, a uno o a varios • _ El guion bajo representa un solo carácter	

`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.
		Las solicitudes de búsqueda con cadenas alfanuméricas utilizan el orden de clasificación ASCII, pero no distinguen mayúsculas y minúsculas.
			`ip RANGE ('10.250.176.1','10.250.176.50')`
			`name RANGE('a','d')`
			Con esta consulta, puede filtrar todos 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'`

Operador	Compatibilidad con	Significado	Ejemplos
<	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'`

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

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**.

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 en **Eliminar**.
3. Haga clic en **Eliminar** para confirmar su elección.

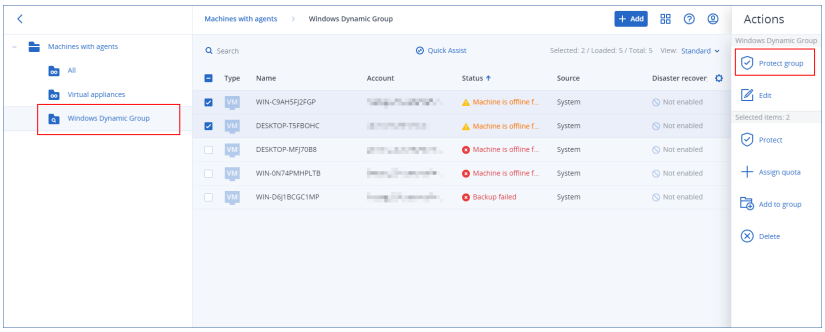
Aplicar un plan a un grupo

Puede aplicar un plan a un grupo mediante la selección del grupo primero y la asignación de un plan a este.

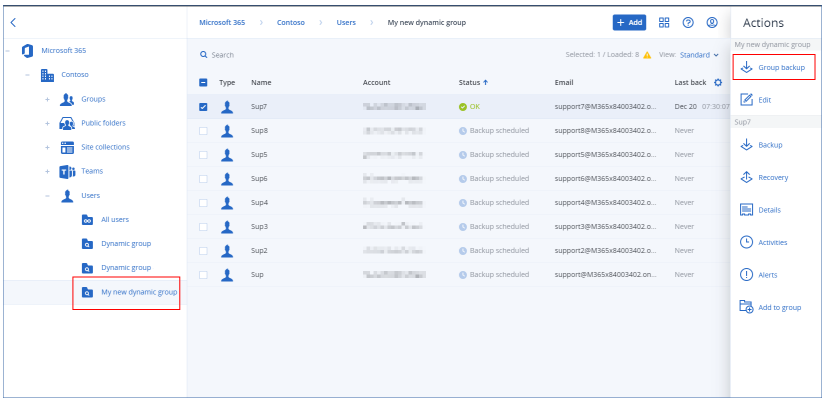
De manera alternativa, puede abrir el plan para editarlo y después añadir un grupo a este.

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. 355).

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 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[3] 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.

---

[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.

[3] 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.

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 y posterior
- macOS 10.15 (Catalina)
- macOS 11.2.3 (Big Sur)
- macOS 12 (Monterey)
- macOS 13 (Ventura)

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 y posterior

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 servidores Hyper-V de 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:

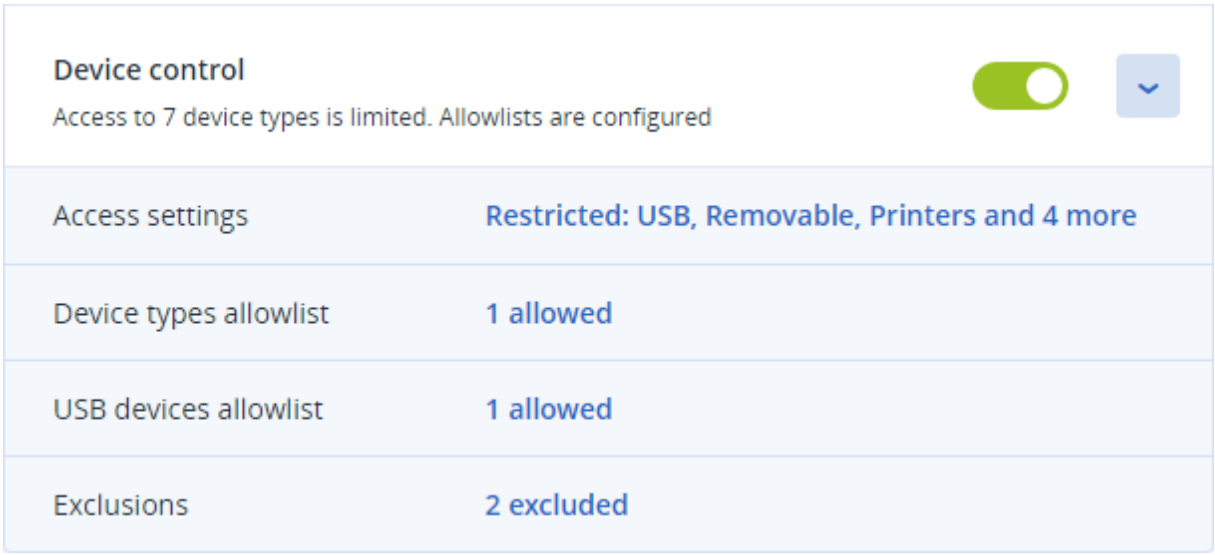
- 15.0.26473 (C21.02)
- 15.0.26570 (C21.02 HF1)
- 15.0.26653 (C21.03)
- 15.0.26692 (C21.03 HF1)
- 15.0.26822 (C21.04)

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
```

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 blanca de tipos de dispositivo: 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 blanca de dispositivos USB: 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

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

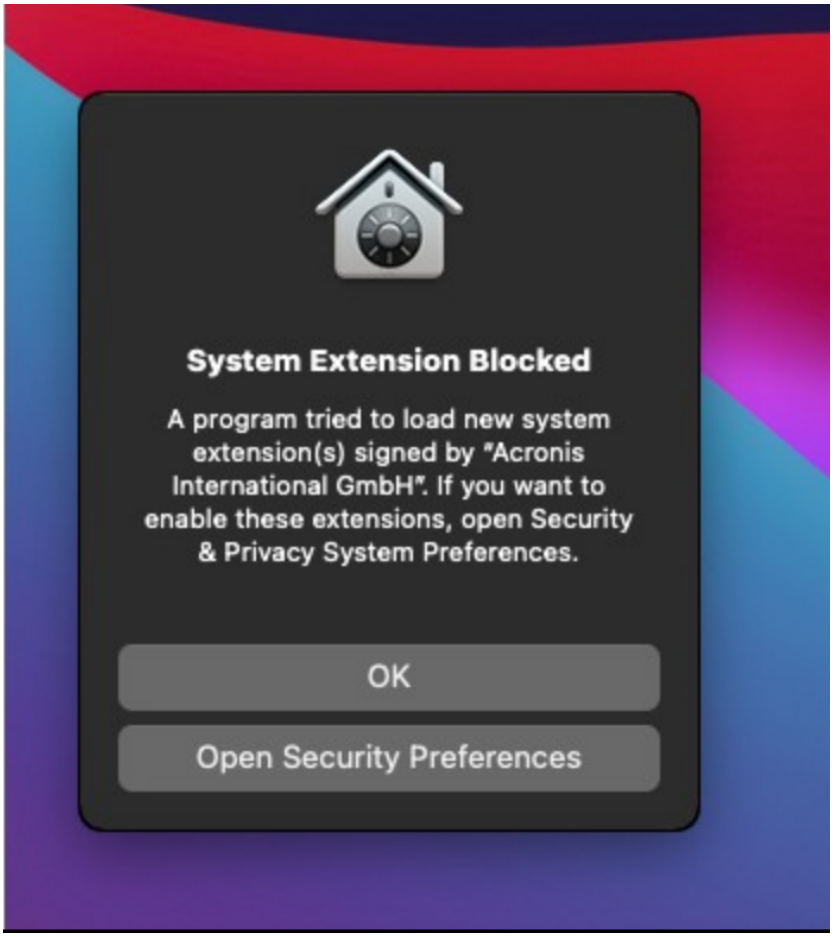
La configuración del control de dispositivos de un plan de protección es efectiva solo después de cargar el controlador del control de dispositivos en la carga de trabajo protegida. Esta sección describe cómo cargar el controlador del control de dispositivos para habilitar el uso del módulo de control de dispositivos en macOS. Es una operación única que requiere privilegios del administrador en el equipo de endpoint.

Versiones de macOS compatibles:

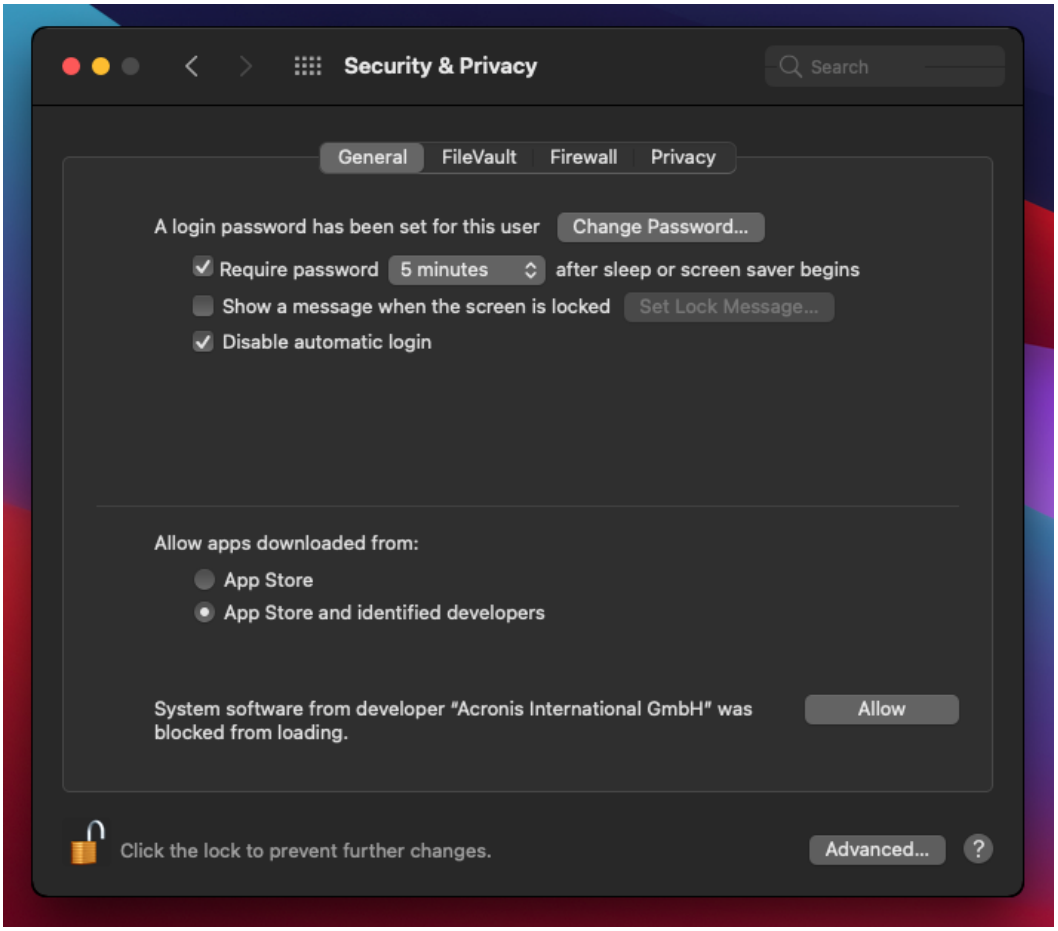
- macOS 10.15 (Catalina) y posterior
- macOS 11.2.3 (Big Sur) y posterior
- macOS 12.2 (Monterey) y posterior
- macOS 13.2 (Ventura) y posterior

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.
4. Aparecerá la advertencia "Extensión del sistema bloqueada" en la carga de trabajo protegida. Haga clic en **Abrir preferencias de seguridad**.



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**.

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. 929).

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 blanca de tipos de dispositivo**.
3. En la página para administrar la lista blanca, consulte o cambie la selección de subclases de dispositivos para excluirlas del control de acceso.

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 blanca de dispositivos USB**.
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, seleccione los dispositivos que desee de entre los registrados en la Base de datos de dispositivos USB.
5. Haga clic en el botón **Agregar a la lista blanca**.

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 blanca de dispositivos USB**.
3. En la página para administrar la lista blanca, 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**.

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 blanca de dispositivos USB**.
3. En la página **Lista blanca de dispositivos USB**, 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.

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. 399).

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 blanca de dispositivos USB**.
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".

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. 929).

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.

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.

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.

- **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.

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 blanca de tipos de dispositivo y Lista blanca de dispositivos USB).

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.

- 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 blanca de tipos de dispositivo

En la página **Lista blanca de tipos de dispositivo**, 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.

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 blanca de dispositivos USB.
- 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 blanca de dispositivos USB.
- 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 blanca de dispositivos USB).

Lista blanca de dispositivos USB

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 blanca de dispositivos USB**, 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 blanca de dispositivos USB**. 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.

- **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 blanca de dispositivos USB). 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).

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 blanca para dispositivos USB, 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 blanca, 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>.

- **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 blanca: Seleccione la casilla de verificación de cada dispositivo que desee añadir y haga clic en el botón **Agregar a la lista blanca**. 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 **Filtrar** 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 blanca de dispositivos USB**.
3. En la página Lista blanca de dispositivos USB, 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.

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 blanca de dispositivos USB**.
3. En la página Lista blanca de dispositivos USB, 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 **Importar**.
   Se abrirá el cuadro de diálogo Importar dispositivos USB desde archivo.
5. 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 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:\Carpeta\subcarpeta\proceso.exe`.
   Puede utilizar comodines:
   - * remplaza cualquier número de caracteres.
   - ? remplaza un carácter.

   Por ejemplo:

   ```
   C:\Carpeta\*
   *\Carpeta\Subcarpeta?\*
   *\proceso.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.

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 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 '<tipo de dispositivo o puerto>' en '<nombre del ordenador>' 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.
- **Fuente**: 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 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.
- **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.

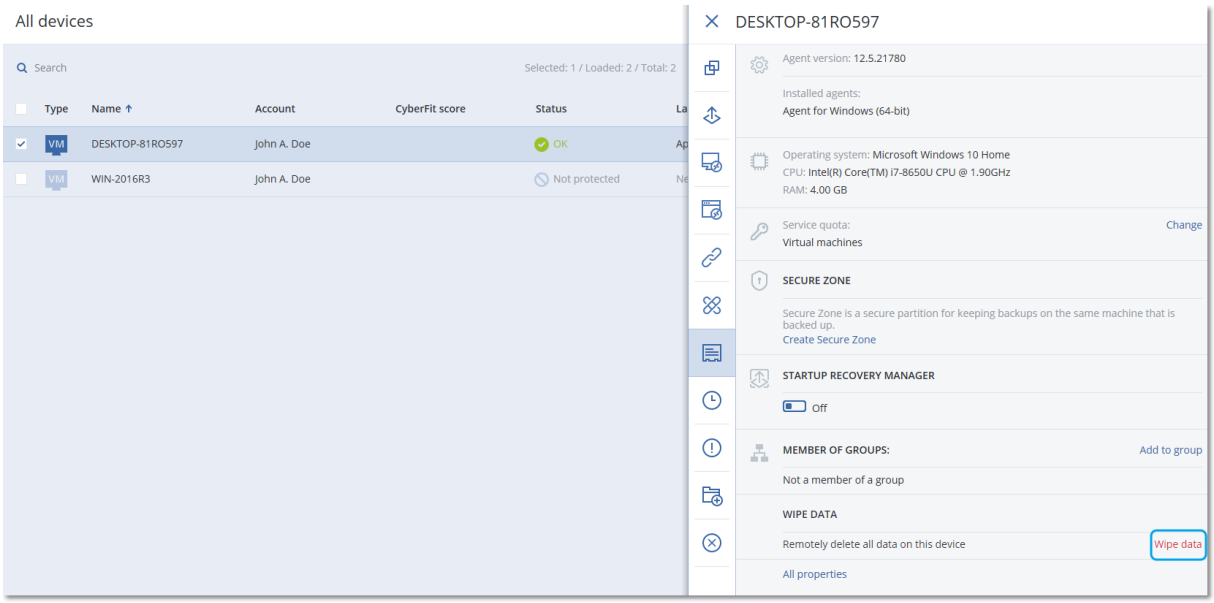
- **Datos RTF salientes (texto, archivo)**: Copiar/pegar texto y un archivo de la sesión alojada al equipo del cliente mediante el portapapeles redirigido utilizando el formato de texto enriquecido.
- **Datos RTF salientes (imagen, archivo)**: Copiar/pegar una imagen y un archivo de la sesión alojada 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 del servicio 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 con Windows 10 y posterior. 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.

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 de Advanced Automation.

Cuando integra una plataforma RMM como parte del servicio de Advanced Automation, 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. (Opcional) 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.

- 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.

Tenga en cuenta que, si 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.

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.

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.

Vinculación de cargas de trabajo a usuarios específicos

Nota
Esta característica solo está disponible si se ha habilitado el servicio de Advanced Automation.

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**.

Buscar el último usuario que ha iniciado sesión

Para que los administradores puedan gestionar los dispositivos, necesitan identificar qué usuario tiene o tenía la sesión iniciada en un dispositivo. Esta información se muestra en el panel de control o en los detalles de la carga de trabajo.

Puede habilitar o deshabilitar la visualización del último inicio de sesión en Planes de administración remota.

En el panel de control:

1. Haga clic en **Dispositivos**. Se muestra la ventana **Todos los dispositivos**.
2. En la columna **Último inicio de sesión**, se muestra el nombre del usuario que inició sesión por última vez en cada dispositivo.
3. En la columna **Hora del último inicio de sesión**, se muestra la hora a la que el usuario inició sesión por última vez en cada dispositivo.

En los detalles del dispositivo:

1. Haga clic en **Dispositivos**. Se muestra la ventana **Todos los dispositivos**.
2. Haga clic en el dispositivo cuyos detalles quiera comprobar.
3. Haga clic en el icono **Detalles**. El nombre del usuario, la fecha y la hora de los últimos inicios de sesión en el dispositivo seleccionado se muestran en la sección **Últimos usuarios que han iniciado sesión**.

Nota

En la sección **Últimos usuarios que han iniciado sesión**, se muestran hasta 5 usuarios diferentes que han iniciado sesión en el dispositivo.

Para mostrar u ocultar las columnas Último inicio de sesión y Hora del último inicio de sesión en el panel de control

1. Haga clic en **Dispositivos**. Se muestra la ventana **Todos los dispositivos**.
2. Haga clic en el icono de engranaje de la esquina superior derecha y, en la sección **General**, haga una de las siguientes opciones:
   - Habilite las columnas **Último inicio de sesión** y **Hora del último inicio de sesión** si quiere mostrarlas en el panel de control.
   - Deshabilite las columnas **Último inicio de sesión** y **Hora del último inicio de sesión** si quiere ocultarlas en el panel de control.

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.

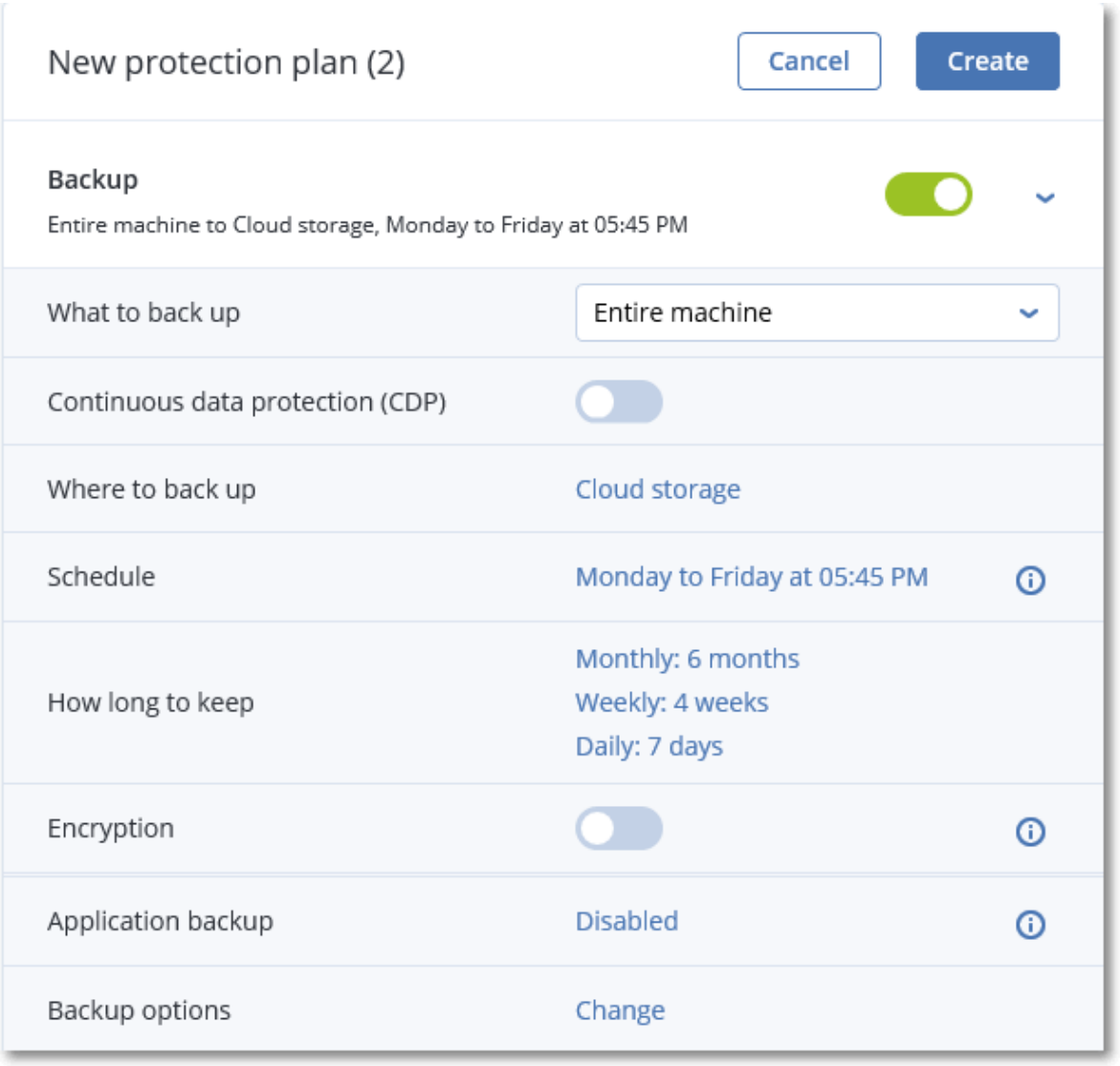
Copia de seguridad

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.

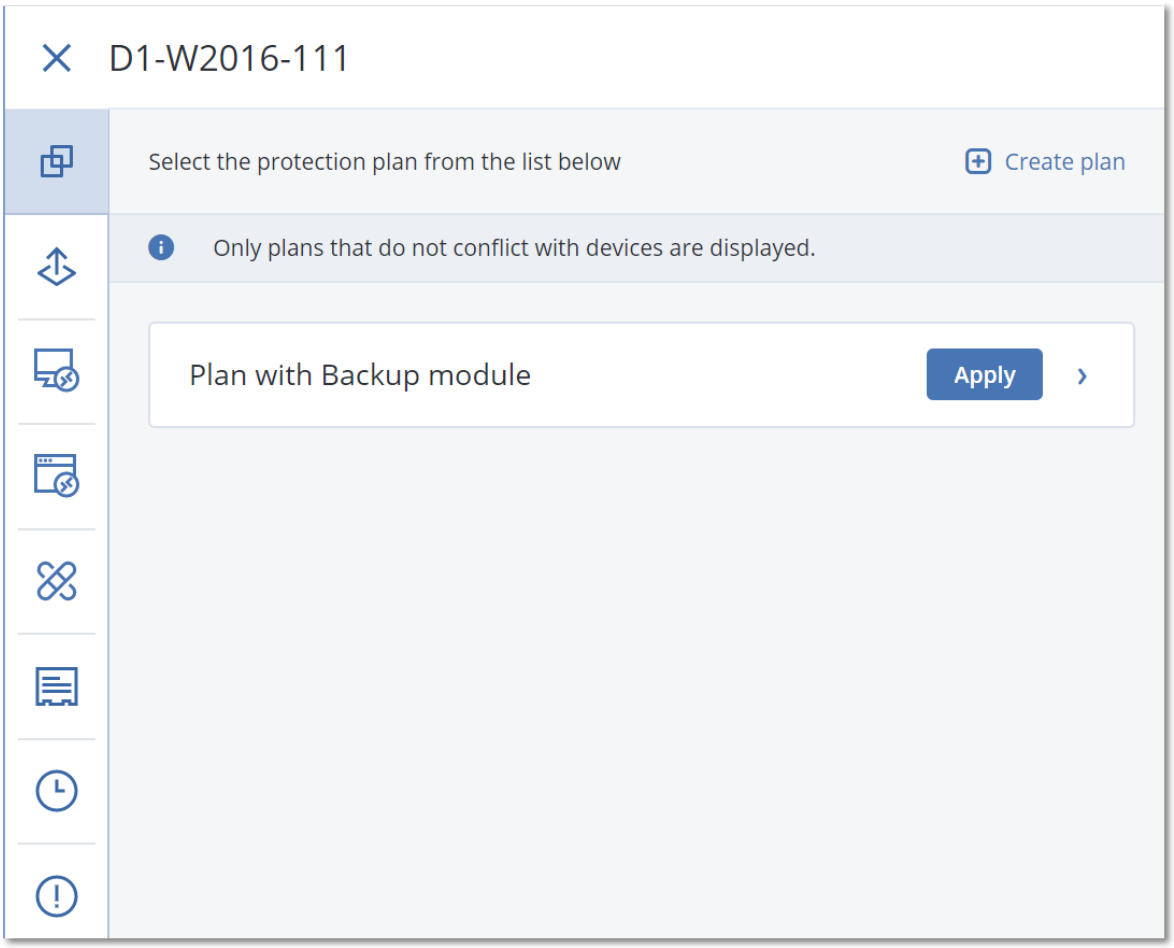


4. [Opcional] Para modificar el nombre del plan de protección, haga clic en el nombre predeterminado.
5. [Opcional] Para modificar los parámetros del módulo de copia de seguridad, haga clic en la configuración correspondiente del panel del plan de protección.
6. [Opcional] Para modificar las opciones de copia de seguridad, haga clic en **Cambiar**, 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.



3. Seleccione el plan de protección que desea aplicar.
4. Haga clic en **Aplicar**.

Apuntes del plan de protección

En la siguiente tabla se resumen los parámetros del plan de protección disponibles. Use la tabla para crear el plan de protección que mejor se ajuste a sus necesidades.

QUÉ INCORPORAR EN LA COPIA 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	CUÁNTO TIEMPO SE CONSERVARÁN
Discos/volúmenes (equipos físicos[1])	Selección directa	Nube	Siempre	Por antigüedad

[1]Un equipo que tiene una copia de seguridad realizada por un agente instalado en el sistema operativo.

	Normas de directiva Filtros de archivo	Carpeta local Carpeta de red NFS* Secure Zone**	incremental (archivo único) Siempre completa Completa semanal, incremental diaria Completa mensual, diferencial semanal, incremental diaria (GFS) Personalizadas (F-D-I)	de las copias de seguridad (norma única/por conjunto de copias de seguridad) Por número de copias de seguridad Por tamaño total de las copias de seguridad*** Guardar indefinidamente
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 (archivo único) 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	—	

[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.

<table>
<tr><td colspan="2">Estado del sistema</td><td rowspan="3">Selección directa</td><td rowspan="2">Nube
Carpeta local
Carpeta de red</td><td rowspan="3">Siempre completa
Completa semanal, incremental diaria
Siempre incremental (archivo único)
Personalizadas</td><td rowspan="10"></td></tr>
<tr><td colspan="2">Bases de datos SQL</td></tr>
<tr><td colspan="2">Bases de datos de Exchange</td></tr>
<tr><td rowspan="8">Microsoft 365</td><td rowspan="2">Buzones de correo
(Agente local para Microsoft 365)</td><td rowspan="2">Selección directa</td><td>Nube
Carpeta local
Carpeta de red</td></tr>
<tr><td>Buzones de correo
(Agente en la nube para Microsoft 365)</td><td rowspan="3">Selección directa</td><td rowspan="4">Nube</td><td>Siempre incremental (archivo único): solo para base de datos SQL</td></tr>
<tr><td>Carpetas públicas</td><td rowspan="3">Hasta 6 copias de seguridad al día</td></tr>
<tr><td>Teams</td></tr>
<tr><td>Archivos de OneDrive</td><td>Selección directa</td></tr>
<tr><td>Datos de SharePoint Online</td><td>Normas de directiva</td></tr>
<tr><td rowspan="3">Google Workspace</td><td>Buzones de correo de Gmail</td><td>Selección directa</td><td rowspan="3">Nube</td><td rowspan="3">Hasta 6 copias de seguridad al día</td></tr>
<tr><td>Archivos de Google Drive</td><td>Selección directa</td></tr>
<tr><td>Archivos de unidades compartidas</td><td>Normas de directiva</td></tr>
</table>

* En Windows no se pueden hacer copias de seguridad en NFS compartidos.

** Secure Zone no se puede crear en un Mac.

*** La regla de retención **Por tamaño total de las copias de seguridad** no está disponible con el esquema de copias de seguridad **Siempre incremental (archivo único)** o al guardar las copias de seguridad en el almacenamiento en la nube.

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. 418).

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.
- La carpeta raíz de OneDrive está excluida de las operaciones de copia de seguridad de forma predeterminada. Si selecciona realizar una copia de seguridad de determinados archivos y carpetas de OneDrive, dicha copia de seguridad se llevará a cabo. Los documentos que no estén disponibles en el dispositivo tendrán contenidos no válidos en el conjunto de la copia de seguridad.

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 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. 481).

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. 421).

   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.
- La carpeta raíz de OneDrive está excluida de las operaciones de copia de seguridad de forma predeterminada. Si selecciona realizar una copia de seguridad de determinados archivos y carpetas de OneDrive, dicha copia de seguridad se llevará a cabo. Los documentos que no estén disponibles en el dispositivo tendrán contenidos no válidos en el conjunto de la copia de seguridad.
- 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. 34).

¿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.
  - 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 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

- `[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. 481).

Pasos para seleccionar archivos o carpetas

Selección directa

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. En el árbol de carpetas, vaya a los archivos o carpetas requeridos.
      De manera alternativa, especifique la ruta hacia estos y haga clic en el botón de la flecha.
   d. [Para las carpetas compartidas] Cuando se le solicite, especifique las credenciales de acceso a la carpeta compartida.
      No se admite la copia de seguridad de carpetas con acceso anónimo.
   e. Seleccione los archivos y carpetas necesarios.
   f. 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. 423).

   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 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. 68).
- La carpeta raíz de OneDrive está excluida de las operaciones de copia de seguridad de forma predeterminada. Si selecciona realizar una copia de seguridad de determinados archivos y carpetas de OneDrive, dicha copia de seguridad se llevará a cabo. Los documentos que no estén disponibles en el dispositivo tendrán contenidos no válidos en el conjunto de la copia de seguridad.
- 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 `Archivos de programa`. 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

- 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 `/Usuarios/<nombre de usuario>/Escritorio/archivo.txt`.
  - Para realizar una copia de seguridad de las carpetas `Escritorio`, `Documentos` y `Descargas` de un usuario, especifique `/Usuarios/<nombre de usuario>/Escritorio`, `/Usuarios/<nombre de usuario>/Documentos` y `/Usuarios/<nombre de usuario>/Descargas`, respectivamente.
  - Para realizar una copia de las carpetas de inicio de todos los usuarios con una cuenta en este equipo, especifique `/Usuarios`.
  - Para hacer copias de seguridad de la carpeta donde están instaladas las aplicaciones, especifique `/Applications`.
- Reglas predefinidas

- `[All Profiles Folder]` selecciona `/Usuarios`. 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
- 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 el cloud 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.

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

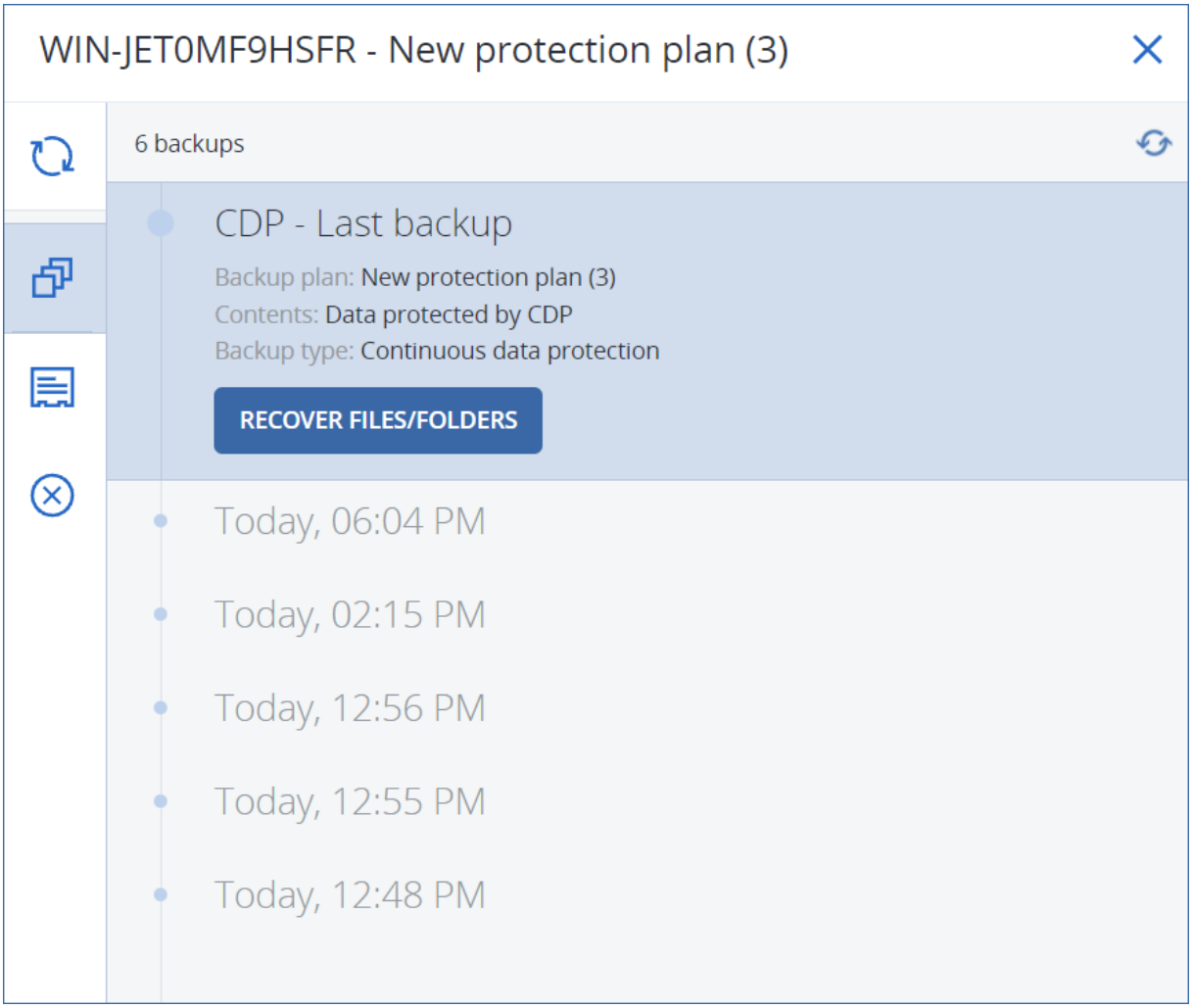
Solo son compatibles las carpetas locales. No pueden seleccionarse carpetas de red para la Protección continua de datos.

La Protección continua de datos no es compatible con la opción **Copia de seguridad de aplicación**.

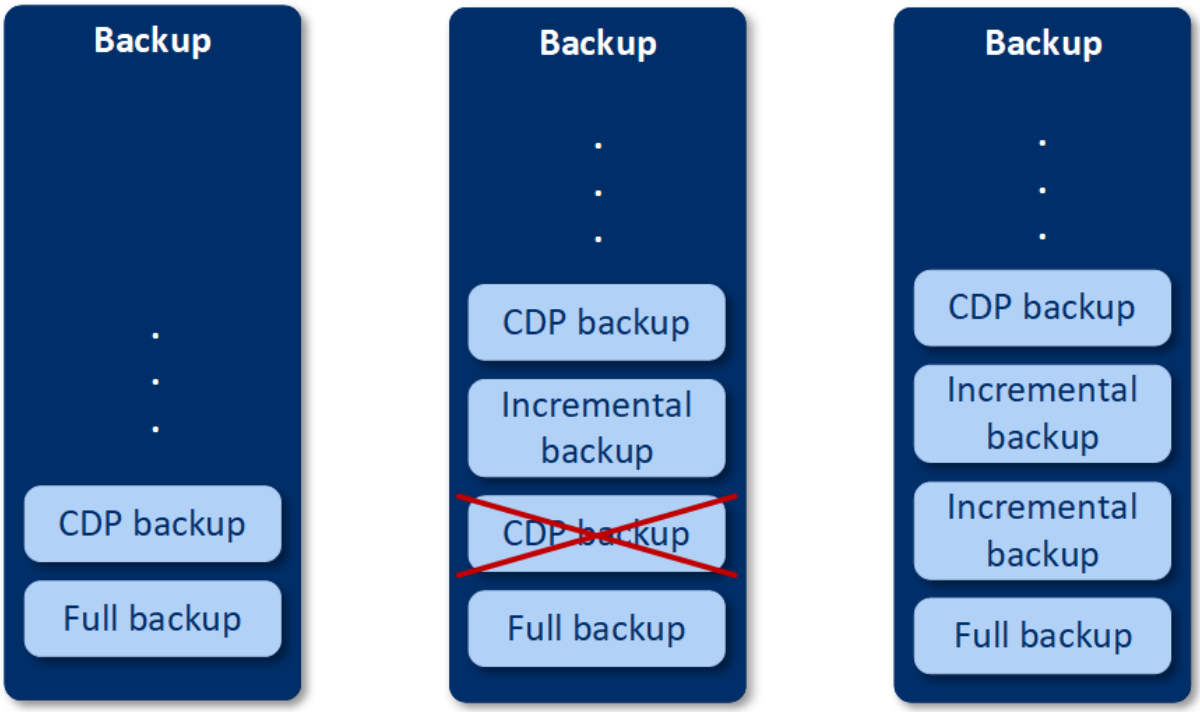
Cómo funciona

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.



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.



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:

- Todo el equipo
- Discos/volúmenes
- Archivos/carpetas

Después de seleccionar la fuente de datos en la sección **Qué incluir 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. 429).

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. 223).

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:

- `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:\Datos\*`

    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.

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.
- **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.

Busque la carpeta compartida requerida o escriba la ruta con el siguiente formato:

- Para recursos compartidos de SMB o CIFS: `\\<nombre de host>\<ruta>\` o `smb://<nombre de host>/<ruta>/`.
- Para recursos compartidos de DFS: `\\<nombre de dominio de DNS completo>\<raíz de DFS>\<ruta>`.

  Por ejemplo, `\\ejemplo.empresa.com\archivos\compartidos`.

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.

  Para obtener más información, consulte "Hacer copias de seguridad de cargas de trabajo en nubes públicas" (p. 566).

- **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.

  Busque la carpeta NFS requerida o introduzca la ruta con el siguiente formato:

  `nfs://<nombre de host >/<carpeta exportada>:/<subcarpeta>`

  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. 432).

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\<nombre del equipo>`:

  ```
  WScript.Echo("\\\\bkpsrv\\" + WScript.CreateObject("WScript.Network").ComputerName);
  ```

  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.

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.

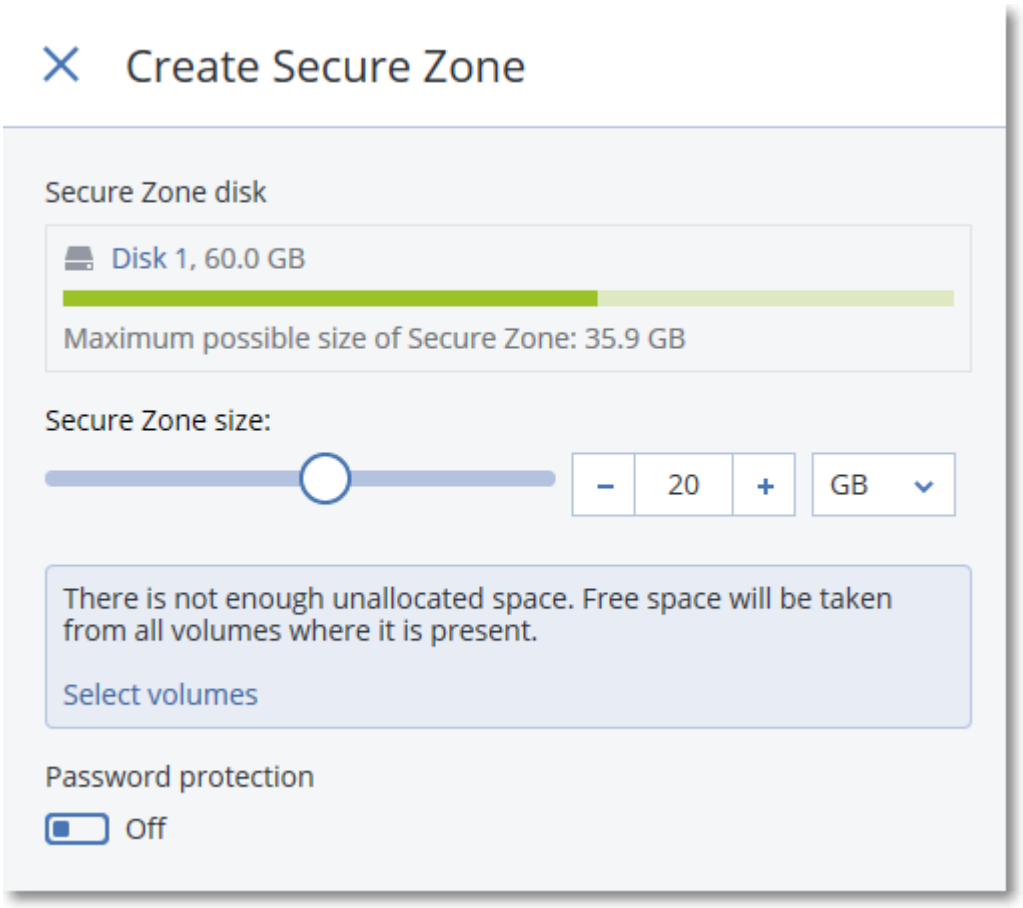
Cómo crear Secure Zone

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.



6. [Opcional] Habilite el conmutador **Protección con 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.
   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.

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

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. El esquema **Siempre incremental (archivo único)** no es compatible con los dispositivos de cintas.

Esquema de copias de seguridad	Descripción	Elementos configurables
Siempre incremental (archivo único)	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, incremental diaria	Se crea una copia de seguridad completa una vez a 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**.	• Iniciador de copia de seguridad: evento u hora • Hora de inicio • Condiciones de inicio • Otras opciones

[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.

Esquema de copias de seguridad	Descripción	Elementos configurables
	De forma predeterminada, las copias de seguridad se realizan a diario de lunes a viernes.	
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 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 (archivo único)** y el resto de esquemas de copia de seguridad, y viceversa. **Siempre incremental (archivo único)** 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.
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. 439) y "Planificación por eventos" (p. 441).
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. 435).

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 hora de inicio de la copia de seguridad.	Ejecutar una copia de seguridad de lunes 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	Ejecutar una copia de seguridad cada hora entre las 08:00 y las 18:00 de lunes

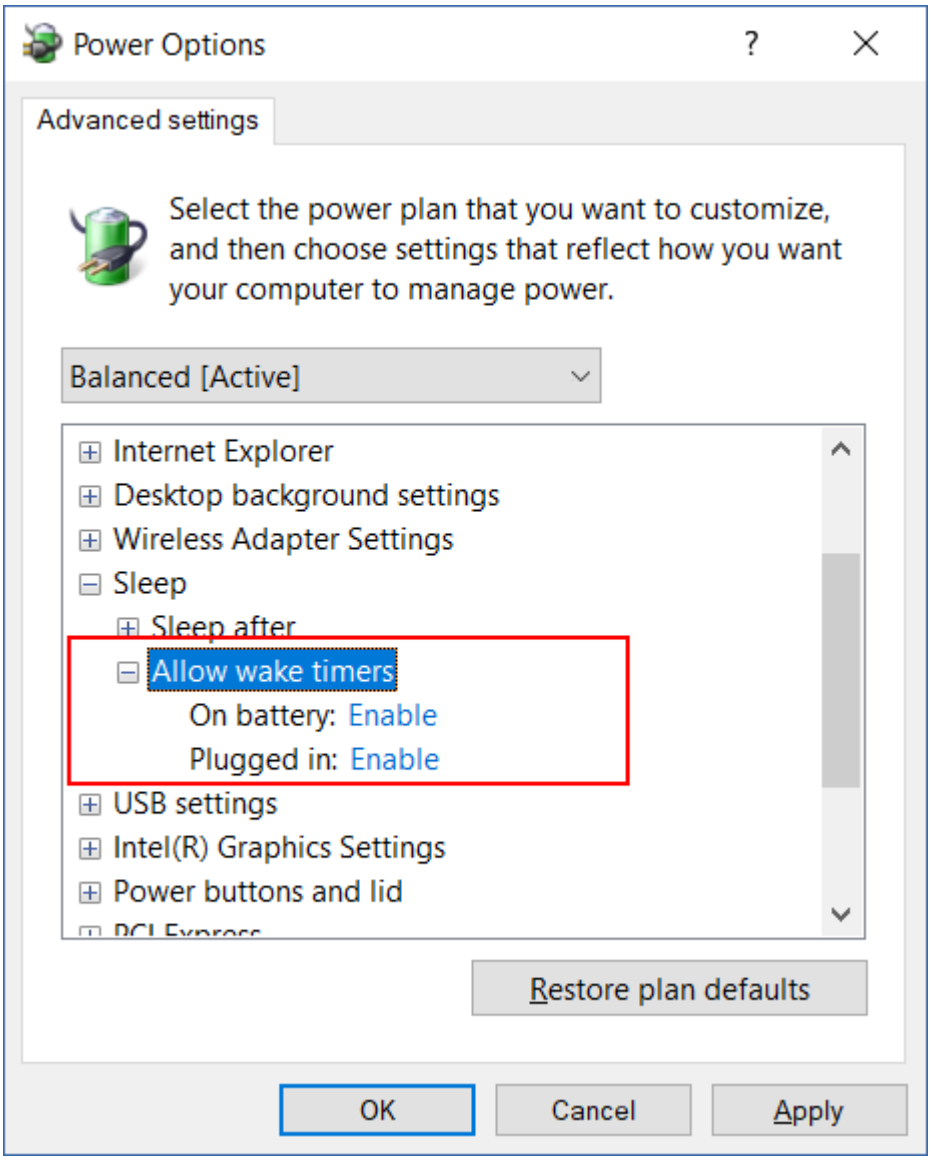
Opción	Descripción	Ejemplos
	seguridad consecutivas y el intervalo de tiempo en el que se ejecutan las copias de seguridad. Si configura el intervalo en minutos, puede seleccionar un intervalo sugerido entre 10 y 60 minutos o especificar uno personalizado, por ejemplo, 45 o 75 minutos.	a viernes. Ejecutar 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.



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

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.

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

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`,

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. 513).

Las condiciones de inicio no son aplicables cuando inicia una copia de seguridad manualmente.

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

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

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.

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.

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:

- 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 de la red del punto de conexión>`.
- 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.

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**: `<inicio del intervalo de direcciones IP de VPN>`, **A**: `<fin del intervalo de direcciones IP de VPN>`.
- 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**.

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. 445).
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. 511)
   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.

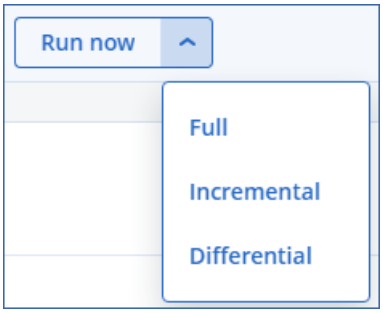
Si no se aplica ningún plan de protección a la carga de trabajo, aplique un plan existente o cree uno nuevo.

Para obtener más información sobre cómo crear un plan de protección, consulte "Creación de un plan de protección" (p. 223).

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 (archivo único)** 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

- 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. 455).

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. 559) para obtener más información sobre cómo eliminar copias de seguridad que ya no necesita.
- 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. 469).
- 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 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. 435).

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 (archivo único)	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, incremental diaria	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
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.
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 (archivo único)** 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.
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. 455).

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 (archivo único)**.
- **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.

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 "Replicación de copias de seguridad" (p. 206).

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	+	–
Nube pública	+	+

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. 500). Estos ajustes definen el rendimiento de la replicación.
   - **Eliminar ubicación**: elimine la ubicación de replicación seleccionada.
   - [Solo para el almacenamiento en la nube] **Servicio de envío físico**: 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. 504).

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. 454).
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.

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 "Replicación de copias de seguridad" (p. 206).

Cifrado

El algoritmo criptográfico Advanced Encryption Standard (AES) opera en modo Galois/Counter (GCM) y utiliza una clave de 256 bits generada aleatoriamente. La clave de cifrado se cifra luego con el algoritmo AES-256 utilizando el hash SHA-2 (256 bits) de la contraseña como clave. La contraseña en sí no se almacena en ningún lugar del disco ni en las copias de seguridad, y el hash de la contraseña se utiliza para la verificación.

Con esta seguridad de dos niveles, los datos de la copia de seguridad están protegidos contra el acceso no autorizado, pero no es posible recuperar una contraseña perdida.

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.

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. 462).

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:

- **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 propiedad de la máquina.

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)

Para configurar el cifrado

En la línea de comando

1. Inicie sesión como administrador (en Windows) o usuario root (en Linux).
2. En la línea de comando, ejecute el siguiente comando:
   - Para Windows:

     ```
     <installation_path>\PyShell\bin\acropsh.exe -m manage_creds --set-password
     <encryption_password>
     ```

     Por defecto, la ruta de instalación será `%ProgramFiles%\BackupClient`.
   - Para Linux:

     ```
     /usr/sbin/acropsh -m manage_creds --set-password <encryption_password>
     ```

   - Para un dispositivo virtual:

     ```
      /./sbin/acropsh -m manage_creds --set-password <encryption_password>
     ```

   Advertencia.
   No es posible recuperar copias de seguridad cifradas si se pierde u olvida la contraseña.

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. En la línea de comando, ejecute el siguiente comando:
   - Para Windows:

     ```
     <installation_path>\PyShell\bin\acropsh.exe -m manage_creds --reset
     ```

     Por defecto, la ruta de instalación será `%ProgramFiles%\BackupClient`.
   - Para Linux:

     ```
     /usr/sbin/acropsh -m manage_creds --reset
     ```

   - Para un dispositivo virtual:

     ```
     /./sbin/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

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

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 **Cambiar**.

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**	**Windows**
Alertas	+	+	+	+	+	+	+	+	+	+
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 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 horas de inicio en una ventana de tiempo	+	+	+	+	+	+	+	+	+	+
Limitar el número de copias de seguridad ejecutadas a la vez	-	-	-	-	-	-	+	+	+	-
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 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.

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 (archivo único)**.
- 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.

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 (archivo único)	**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.

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 copias 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`.

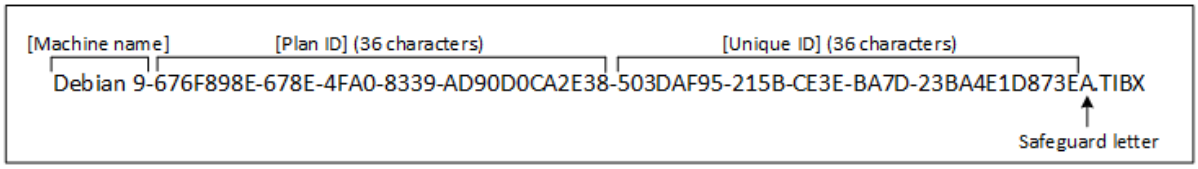
El nombre predeterminado de las copias de seguridad de Microsoft Azure incluye el prefijo `[Mailbox ID]_`. Este prefijo no se puede eliminar.

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`.

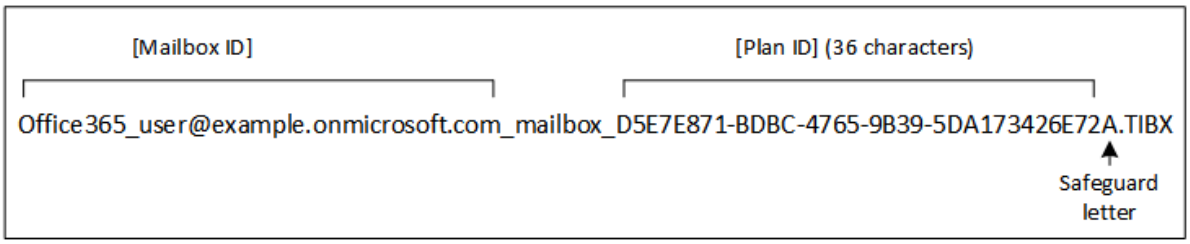
El nombre predeterminado consta de las siguientes variables:

- `[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 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 (archivo único)**:

```
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:

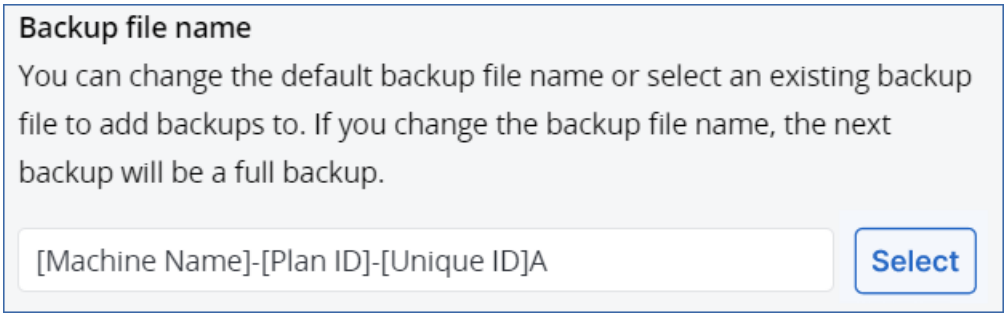
- La variable `[Plan name]`, que se sustituye por el nombre del plan de protección.
- La variable `[Virtualization Server Type]`, que se sustituye por "vmwesx" si Agent para VMware crea una copia de seguridad de los equipos virtuales o por "mshyperv" si Agente para Hyper-V crea una copia de seguridad 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.



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 **Cambiar**.
4. En la pestaña **Nombre de la copia de seguridad de archivos**, haga clic en **Seleccionar**.
   El botón **Seleccionar** muestra las copias de seguridad de la ubicación seleccionada en la sección **Dónde realizar 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 **Administración** > **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.

  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 (archivo único)	**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	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	

seguridad **Versión 12**	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 copias 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.

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 Compatibilidad del archivo de copia de seguridad en las diferentes versiones del producto (1689).

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. 213).

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
- 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 AlwaysOn 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 AlwaysOn (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 AlwaysOn, consulte "Protección de los grupos de disponibilidad AlwaysOn (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 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.

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: 10. 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 en cuanto la operación se lleve a cabo correctamente o se realice el número de intentos especificados (lo que suceda primero).

Por ejemplo, si no se tiene acceso o no está disponible el destino de la copia de seguridad en la red durante la ejecución de una copia de seguridad, el software intentará llegar al destino cada 30 segundos, pero solo 30 veces. Se detendrán los intentos en cuanto se reanude la operación o se realice el número de intentos especificados (lo que suceda primero).

Sin embargo, si el destino de la copia de seguridad no está disponible cuando se inicie la copia de seguridad, solo se llevarán a cabo 10 intentos.

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 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)

Utilice 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. 55).

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.

Para habilitar 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 **Cambiar**.
3. Seleccione **Filtros de archivo (inclusiones y exclusiones)**.
4. Use cualquiera de las opciones que se especifican a continuación.

Filtros de inclusión y exclusión

Hay dos filtros: filtro de inclusión y filtro de exclusión.

- **Incluir solo los archivos que cumplan los siguientes criterios**

  Si especifica `C:\File.exe` en el filtro de inclusión, solo se incluirá este archivo en la copia de seguridad, aunque seleccione "Copia de seguridad de todo el equipo".

  Nota

  Este filtro no es compatible con copias de seguridad a nivel de archivo cuando el formato de las copias de seguridad es la **Versión 11** y el destino de la copia de seguridad no es el almacenamiento en la nube.

- **Excluir 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".

Se pueden utilizar ambos filtros a la vez. El filtro de exclusión tiene prioridad sobre el filtro de inclusión; es decir, si especifica `C:\File.exe` en los dos campos, este archivo se omitirá durante el proceso de copia de seguridad.

Criterios de filtros

Como criterios de filtros, puede utilizar nombres de archivos y carpetas, rutas completas a archivos y carpetas y máscaras con símbolos comodín.

Los criterios de filtros no distinguen mayúsculas de minúsculas. Por ejemplo, si especifica `C:\Temp`, también seleccionará `C:\TEMP` y `C:\temp`.

- Nombre

  Especifique el nombre del archivo o carpeta, como por ejemplo `Document.txt`. Se seleccionarán todos los archivos y carpetas con ese nombre.
- Ruta completa

  Especifique la ruta completa hasta el archivo o carpeta, empezando por la letra de unidad de disco (al realizar copias de seguridad en Windows) o del directorio raíz (al hacer copias de seguridad 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 de directorio completo 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 sería `C:\Temp\File.tmp`. 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 del equipo del que se ha llevado a cabo una copia de seguridad no se detecta correctamente, los filtros no funcionarán de todos modos.

- Máscara

  Puede utilizar los siguientes caracteres comodín para los nombres y las rutas completas: asterisco (*), doble asterisco (**) y signo de interrogación (?).

  El asterisco (*) representa a cero o más caracteres. Por ejemplo, el criterio de filtro **Doc*.txt** coincide con los archivos `Doc.txt` y `Document.txt`.

  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 asterisco doble (**) para copias de seguridad en el formato de la versión 12.

  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`.

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 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 tenga lugar la actividad maliciosa dejará de estar disponible.

Las copias de seguridad con datos forenses permiten a los investigadores analizar áreas de disco que no suelen incluirse en una copia de seguridad del disco habitual. Con la opción de copias de seguridad llamada **Datos forenses** se pueden recopilar las siguientes pruebas digitales para utilizarlas en investigaciones forenses: capturas de espacio en disco no utilizado, volcados de memoria y capturas de procesos en ejecución.

Las copias de seguridad con datos forenses se certifican automáticamente.

La opción **Datos forenses** está disponible únicamente para equipos Windows con copias de seguridad completas con los siguientes sistemas operativos:

- Windows 8.1, Windows 10
- Windows Server 2012 R2 – Windows Server 2019

Las copias de seguridad con datos forenses no se encuentran disponibles para los siguientes equipos:

- Equipos conectados a su red mediante una VPN y sin acceso directo a Internet
- Equipos con discos cifrados por BitLocker

Nota

No puede modificar la configuración de los datos forenses después de aplicar un plan de protección con el módulo **Copia de seguridad** en un equipo. Para usar una configuración diferente de datos forenses, cree un nuevo plan de protección.

Puede almacenar copias de seguridad de datos forenses en las siguientes ubicaciones:

- Almacenamiento en la nube
- Carpeta local

  Nota
  La ubicación de la carpeta local solo se admite en discos duros externos conectados mediante USB.
  Los discos dinámicos locales no se admiten como ubicaciones para copias de seguridad de datos forenses.

- Carpeta de red

Proceso de copia de seguridad forense

El sistema realiza lo siguiente durante un proceso de copia de seguridad forense:

1. Recopila un volcado de memoria sin procesar y la lista de procesos en ejecución.
2. Reinicia un equipo automáticamente en el dispositivo de arranque.
3. Crea la copia de seguridad que incluye tanto el espacio ocupado como el que está sin asignar.
4. Certifica los discos de los que se ha realizado la copia de seguridad.
5. Reinicia en el sistema operativo en funcionamiento y sigue con la ejecución del plan (por ejemplo, replicación, retención, validación, entre otros).

Pasos para configurar la recopilación de datos forenses

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Todos los dispositivos**. Los planes de protección también se pueden crear desde la pestaña **Administración**.
2. Seleccione el dispositivo y haga clic en **Proteger**.
3. En el plan de protección, habilite el módulo **Copia de seguridad**.
4. En **Qué incorporar en la copia de seguridad**, seleccione **Todo el equipo**.
5. En **Opciones de copia de seguridad**, haga clic en **Cambiar**.
6. Busque la opción **Datos forenses**.
7. Habilite **Recopilar datos forenses**. El sistema recopilará automáticamente un volcado de memoria y creará una instantánea de los procesos en ejecución.

   Nota
   Un volcado de memoria completo puede incluir datos confidenciales, como contraseñas.

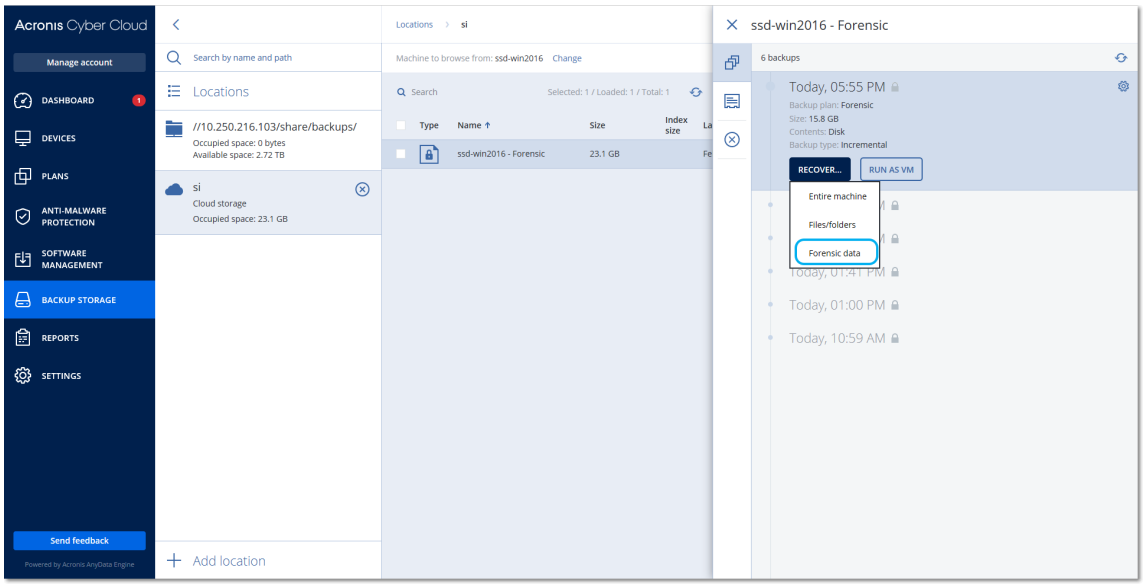
8. Especifique la ubicación.
9. Haga clic en **Ejecutar ahora** para llevar a cabo directamente una copia de seguridad con datos forenses o espere a que la copia de seguridad se cree según la planificación.

10. Vaya a **Supervisión** > **Actividades** y verifique que se haya creado correctamente la copia de seguridad con datos forenses.

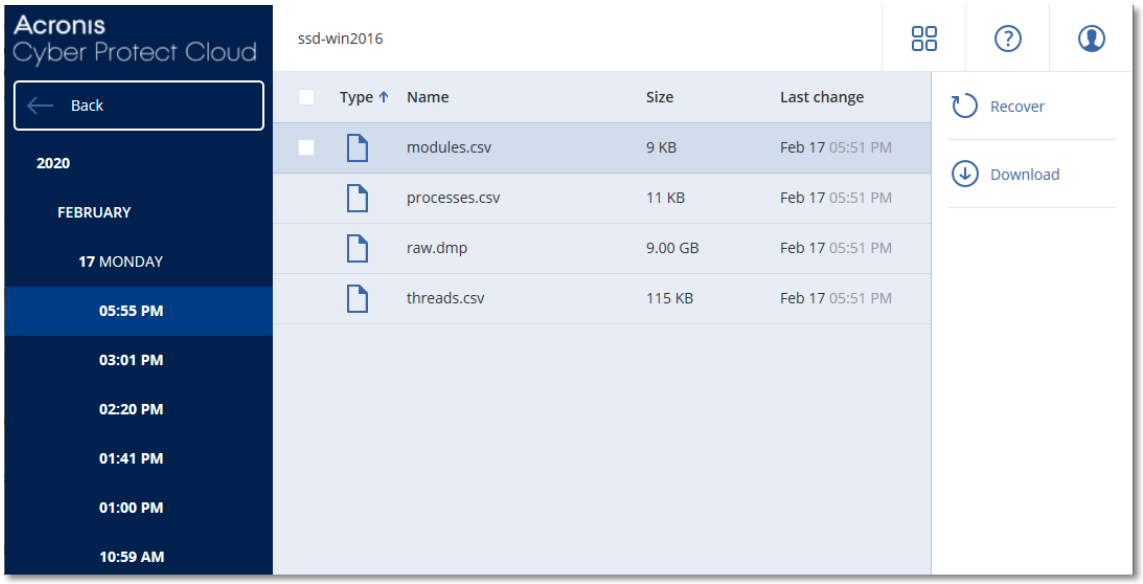
Como resultado, las copias de seguridad incluirán datos forenses, y podrá obtenerlas y analizarlas. Las copias de seguridad con datos forenses aparecen marcadas y se pueden filtrar de otras copias de seguridad en **Almacenamiento de la copia de seguridad** > **Ubicaciones** mediante la opción **Solo con datos forenses**.

¿Cómo se pueden obtener los datos forenses datos desde una copia de seguridad?

1. En la consola de Cyber Protect, vaya a **Almacenamiento de copias de seguridad** y seleccione la ubicación en la que se encuentran las copias de seguridad que contienen datos forenses.
2. Seleccione la copia de seguridad con datos forenses y haga clic en **Mostrar copias de seguridad**.
3. Haga clic en **Recuperar** para la copia de seguridad con datos forenses.
   - Para obtener únicamente los datos forenses, haga clic en **Datos forenses**.



El sistema mostrará una carpeta con los datos forenses. Seleccione un archivo de volcado de memoria o cualquier otro archivo de datos forenses y, a continuación, haga clic en **Descargar**.



- Para recuperar una copia de seguridad forense completa, haga clic en **Todo el equipo**. El sistema recuperará la copia de seguridad sin el modo de arranque. Por lo tanto, será posible comprobar que el disco no ha cambiado.

Puede usar el volcado de memoria proporcionado con varios softwares forenses de terceros, por ejemplo, use Volatility Framework en https://www.volatilityfoundation.org/ para obtener un mayor análisis de la memoria.

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.

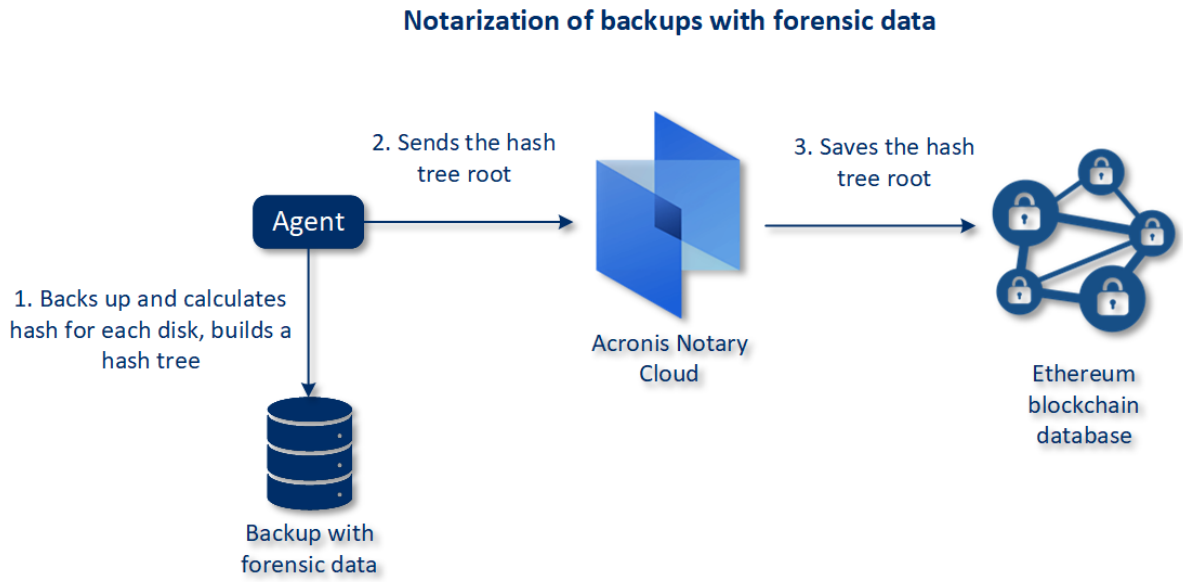
Durante una copia de seguridad, el agente calcula los códigos de cifrado de los discos de los que se ha realizado la copia de seguridad, crea un árbol de cifrado, guarda el árbol en la copia de seguridad y envía la raíz del árbol de cifrado al servicio de notarización. El servicio de notarización guarda 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 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.

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
  ```

  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   Fecha   Marca de fecha y hora
----   ------ --------------
<guid> <fecha> <marca de fecha y hora>
```

<guid>: GUID de copia de seguridad.

<fecha>: 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   Fecha   Marca de fecha y hora
----   ------ --------------
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.

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:

```
Disco     Tamaño   Estado de certificación
--------- ------ --------------------
<número> <tamaño> <estado de certificación>
```

<número>: identificador del disco.

<tamaño>: tamaño en bytes.

<estado_de_certificación>: se pueden dar los siguientes estados: Sin certificación, Certificada y Siguiente copia de seguridad.

Ejemplo de salida:

```
Disco     Tamaño   Estado de certificación
--------- ------ --------------
1         123123465798 Certificada
2         123123465798 Certificada
```

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
--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
	`--loc=<dirección IP>:443 --cert=<ruta_al_certificado> [--storage_path=/1]`
	`<dirección IP>`: puede encontrarla en la clave de registro en Windows: HKEY_LOCAL_

	MACHINE\SOFTWARE\Acronis\BackupAndRecovery\Settings\OnlineBackup\FesAddressCache\Default\<tenant_login>\FesUri `<ruta al certificado>`: 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 <nombre de usuario> 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 Fecha Marca de fecha y hora`
	`---- ------ --------------`
	`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 la copia de seguridad de bases de datos de Microsoft SQL Server y para la copia de seguridad a nivel de disco con la copia de seguridad de aplicaciones de Microsoft SQL Server habilitada.

Esta opción define si los registros de transacción de SQL Server se truncan tras una copia de seguridad correcta.

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 este software. 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. Podrá aplicar los registros de transacción después de una recuperación y, por lo tanto, recuperar una base de datos a cualquier momento específico.

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.

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 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. Esta copia de seguridad puede ser una copia de seguridad de todo el equipo, o una copia de seguridad de discos o volúmenes específicos de este equipo.

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 local
- Carpeta de red
- Almacenamiento en la nube

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

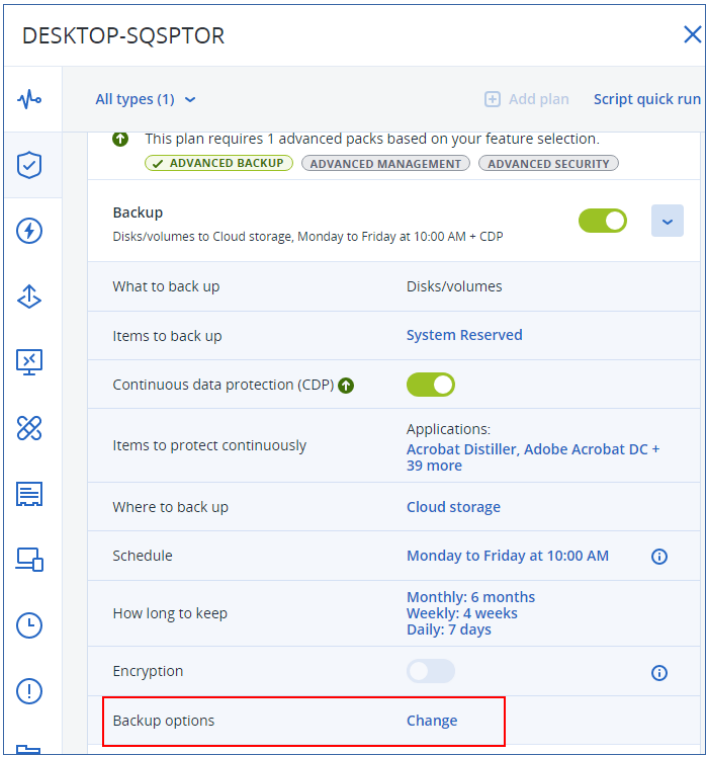
La recuperación con un clic es una opción de copia de seguridad en el plan de protección. Para obtener más información sobre cómo crear un plan, consulte "Creación de un plan de protección" (p. 223).

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. 772).

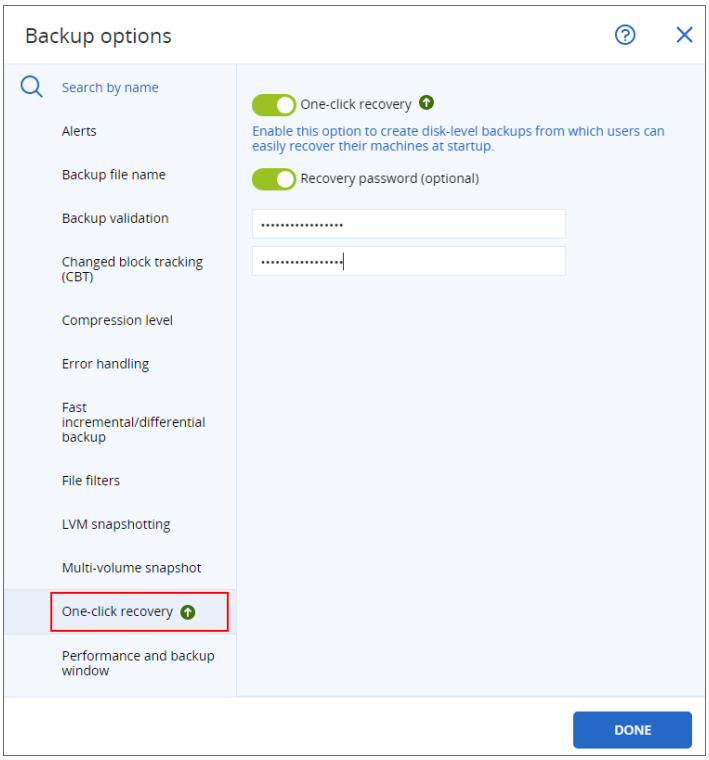
Para habilitar la recuperación con un clic

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 **Cambiar** y, a continuación, seleccione **Recuperación con un clic**.



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.



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.

Importante
La recuperación con un solo clic deja de estar disponible temporalmente cuando se actualiza el agente de protección. Para volver a activar la recuperación con un solo clic, ejecute una copia de seguridad. Cuando finalice la copia de seguridad, podrá volver a realizar la recuperación con un solo clic.

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

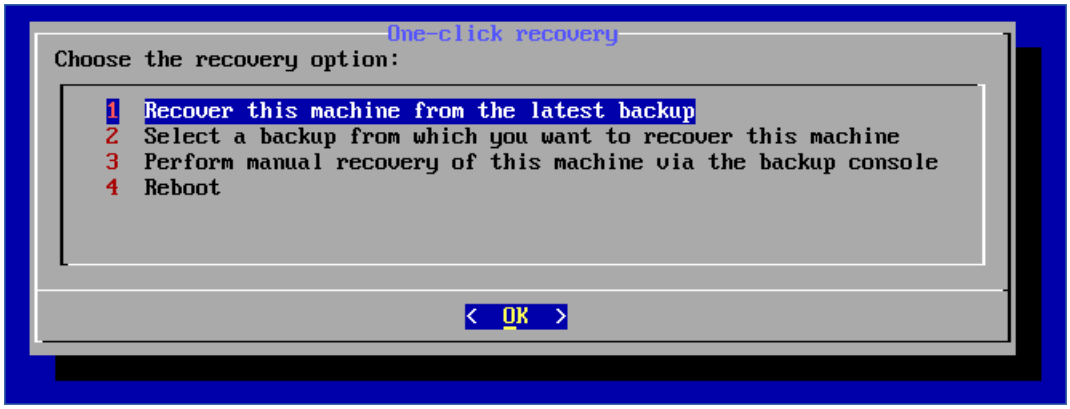
Requisitos previos

- 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

1. Reinicie el equipo que desea recuperar.
2. Durante el reinicio, pulse F11 para entrar en Startup Recovery Manager.

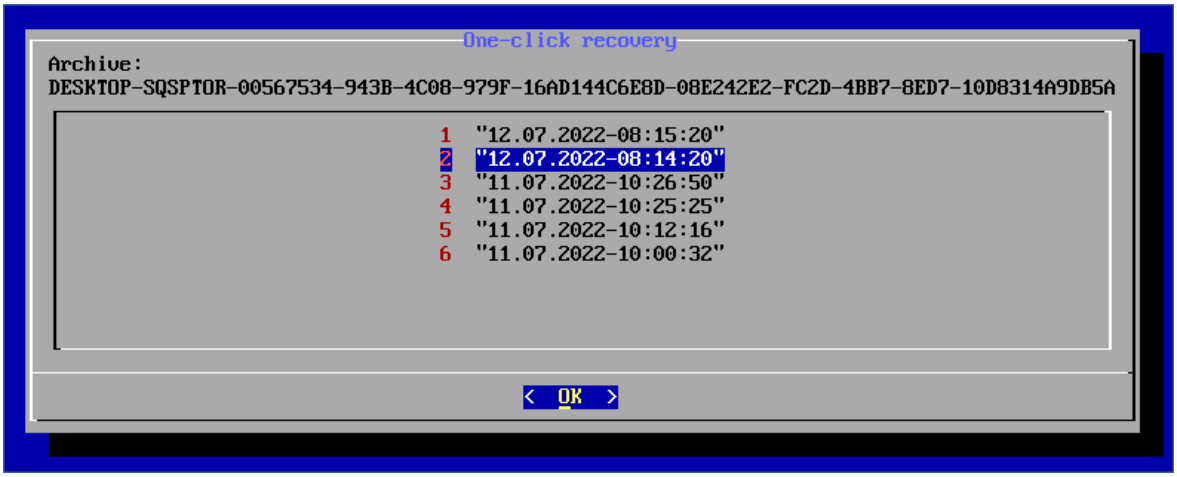
   Se abre la ventana del dispositivo de rescate.
3. Seleccione **Acronis Cyber Protect**.
4. [Si se ha especificado una contraseña de recuperación en el plan de protección] Introduzca la contraseña de recuperación y, a continuación, haga clic en **Aceptar**.
5. Seleccione la opción de Recuperación con 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**.



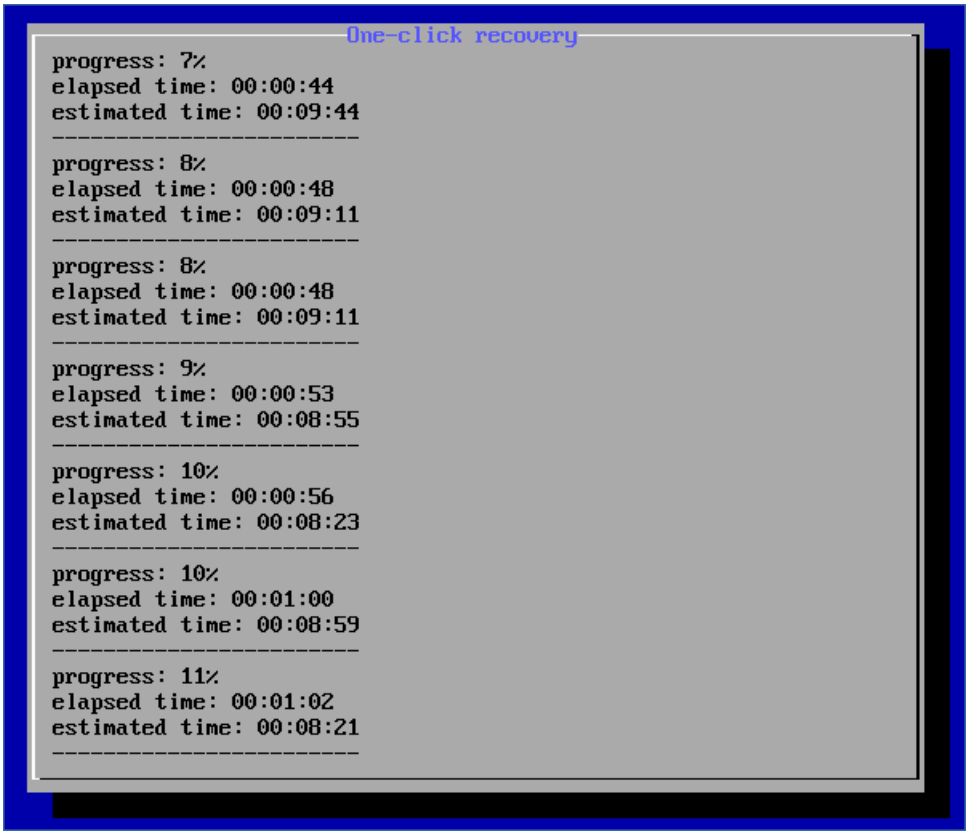
6. Haga clic en **Sí** para confirmar su elección.

   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.



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**

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.

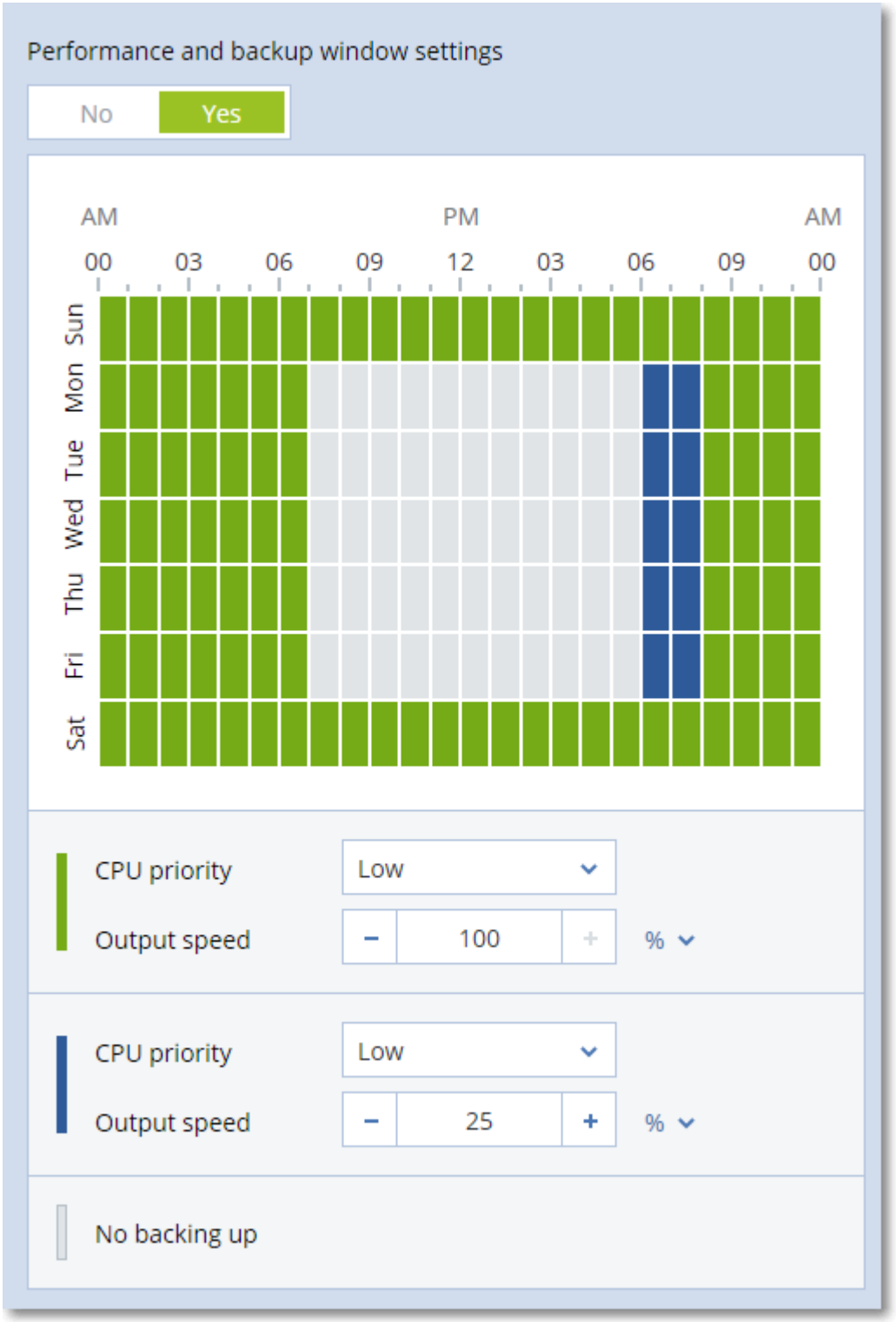
Nota
Puede configurar la realización y el período de copia de seguridad para cada ubicación de replicación de manera individual. Para acceder a la configuración de la ubicación de replicación, en el plan de protección, haga clic en el ícono de engranaje junto al nombre de la ubicación, y luego haga clic 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.



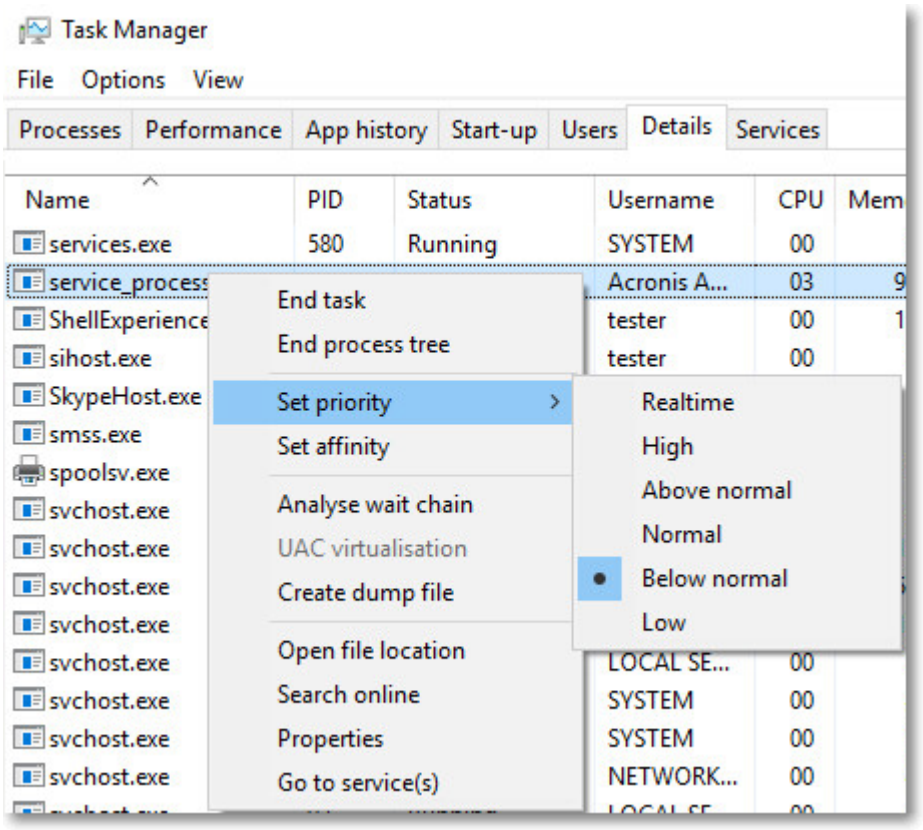
Prioridad de la CPU

Este parámetro define la prioridad del proceso de copia de seguridad en el sistema operativo.

Los ajustes disponibles son: **Baja**, **Normal**, **Alta**.

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

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.

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 **Especificar 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.

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 por lotes para que se ejecute antes de que comience el proceso de copia de seguridad

1. Habilite el conmutador **Ejecutar un comando antes de la copia de seguridad**.
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 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.

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 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...**, 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 copia de seguridad 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 copia de seguridad será **Error**.

   Cuando no se marca la casilla de verificación, los resultados de la ejecución del comando no afectarán al éxito o fallo de la copia de seguridad. Puede realizar un seguimiento de la ejecución de comandos desde la pestaña **Actividades**.
6. Haga clic en **Listo**.

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...**, 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 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	N/D	Realizar la captura de

	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.	captura de datos después de que se ejecute el comando a pesar del éxito o fallo de la ejecución		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.

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 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...**, 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 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 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. 438).

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**

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. 743).

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

Esta opción permite seleccionar el método de división de las copias de seguridad de gran tamaño en archivos más pequeños.

Nota
No se puede dividir en planes de protección que usen el almacenamiento en la nube como ubicación de la copia de seguridad.

El valor predeterminado es el siguiente:

- Si la ubicación de la copia de seguridad es una carpeta local o de red (SMB) y la copia de seguridad tiene el formato Versión 12: **Tamaño fijo: 200 GB**

Esta configuración permite que el software de copia de seguridad funcione con amplios volúmenes de datos en el sistema 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 de la lista desplegable.

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. 445).

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.

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, los proveedores de instantáneas de software y Microsoft Software Shadow Copy Provider.
- **Usar Microsoft Software Shadow Copy Provider**
  Se recomienda seleccionar esta opción cuando se realice una copia de seguridad de los servidores de la aplicación (Microsoft Exchange Server, Microsoft SQL Server, Microsoft SharePoint o Active Directory).

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 señala si se van a realizar instantáneas inactivas de los equipos virtuales.

El valor predeterminado es el siguiente: **Habilitado**.

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.

Cuando esta opción está habilita, se completan las transacciones de todas las aplicaciones compatibles con VSS que se ejecutan en la máquina virtual y, a continuación, se toma una instantánea en modo inactivo.

Si no se puede tomar ninguna instantánea en modo inactivo tras el número de reintentos especificado en la opción "Control de errores" y la copia de seguridad de la aplicación está habilitada, se producirá un error en la copia de seguridad.

Si no se puede tomar ninguna instantánea en modo inactivo tras el número de reintentos especificado en la opción "Control de errores" y la copia de seguridad de la aplicación está deshabilitada, se creará una copia de seguridad coherente con un bloqueo. Para que se produzca

un error en la copia de seguridad en lugar de crear una copia de seguridad coherente con un bloqueo, seleccione la casilla **Error en la copia de seguridad si no es posible tomar una instantánea en modo de inactividad**.

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 una instantánea en modo de inactividad** 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.	Error al realizar la copia de seguridad.
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 máquinas 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 comandos, consulte "Ejecución de comandos anteriores y posteriores a la instantánea automáticamente" (p. 735).

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**.

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

No puede recuperar copias de seguridad en la consola de Cyber Protect para inquilinos en el modo de Cumplimiento. Para obtener más información sobre cómo recuperar dichas copias de seguridad, consulte "Recuperación de copias de seguridad para inquilinos en el modo de Cumplimiento" (p. 1151).

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 (VMware, Hyper-V, Red Hat Virtualization (oVirt) o Scale Computing HC3)	Uso de la consola de Cyber Protect Uso de dispositivos de arranque
Máquina virtual o contenedor (Virtuozzo, Virtuozzo Hybrid Server, o Virtuozzo Hybrid Infrastructure)	Uso de la consola de Cyber Protect
Configuración de ESXi	Uso de dispositivos de arranque
Archivos/Carpetas	Uso de la consola de Cyber Protect 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.
- 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.

En la tabla siguiente se muestran algunos ejemplos de recuperación multiplataforma.

Recuperación multiplataforma	
Copia de seguridad sin agente	Recuperación basada en agente
Copia de seguridad basada en agente	Recuperación sin agente
Copia de seguridad del Agente para Windows	Recuperación del Agente para VMware
Copia de seguridad del Agente para VMware	Recuperación del Agente para Hyper-V
Copia de seguridad del Agente para Windows instalado en una máquina virtual de VMware ESXi (basada en agente)	Recuperación del Agente para VMware (sin agente) en el mismo servidor de VMware ESXi

Recuperación multiplataforma	
Copia de seguridad del Agente para Windows	Recuperación del Agente para Windows instalado en un equipo con hardware diferente
Copia de seguridad de un equipo físico	Recuperación como una máquina virtual

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 segura

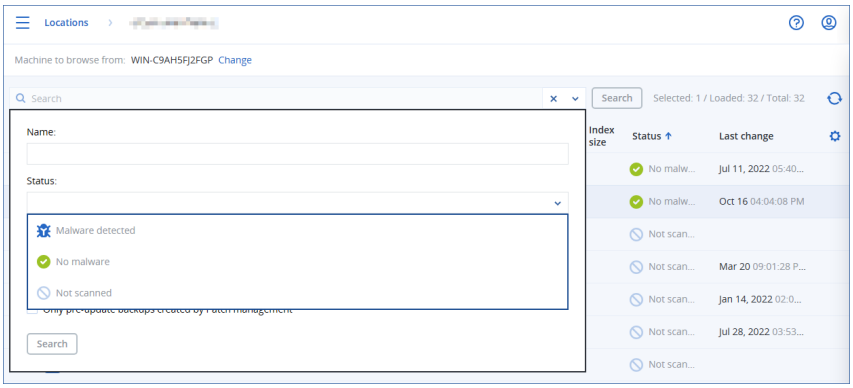
Utilice la recuperación segura con copias de seguridad de **Todo el equipo** o **Discos/volúmenes** de cargas de trabajo de Windows para garantizar que solo recupera datos libres de malware, incluso si la copia de seguridad contiene archivos infectados.

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.



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 **Equipo entero** 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. 426).

Recuperar un equipo

Recuperación de equipos físicos

En esta sección se describe la recuperación de equipos físicos mediante la interfaz web.

Use dispositivos de inicio en vez de interfaz web si necesita recuperar:

- Una máquina que ejecute macOS
- Un equipo de un inquilino en el modo de Cumplimiento
- Cualquier sistema operativo desde cero o en un equipo sin conexión
- La estructura de los volúmenes lógicos (volúmenes creados por Logical Volume Manager en Linux). El dispositivo le permite recrear automáticamente la estructura del volumen lógico.

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.

Recuperación con reinicio

La recuperación de un sistema operativo y de los volúmenes cifrados con BitLocker requiere un reinicio. Puede elegir si reiniciar el equipo automáticamente o asignarle el estado **Interacción necesaria**. El sistema operativo recuperado se conecta a Internet automáticamente.

Importante
Los volúmenes no cifrados de los que se haya hecho una copia de seguridad se recuperan como no cifrados.

La recuperación de los volúmenes cifrados con BitLocker requiere que haya un volumen no cifrado en el mismo equipo y que dicho volumen tenga al menos 1 GB de espacio libre. Si no se cumple alguna de estas condiciones, la recuperación fallará.

La recuperación de un volumen del sistema cifrado no requiere ninguna acción adicional. Para recuperar un volumen cifrado que no es del sistema, primero debe bloquearlo, por ejemplo, abriendo un archivo que resida en ese volumen. De lo contrario, la recuperación continuará sin reiniciarse y Windows podría no reconocer el volumen recuperado.

Nota
Si la recuperación falla y su equipo se reinicia con el error `No puede obtenerse el archivo de la partición`, pruebe a deshabilitar el arranque seguro. Para obtener más información sobre cómo hacerlo, consulte Deshabilitación del arranque seguro en la documentación de Microsoft.

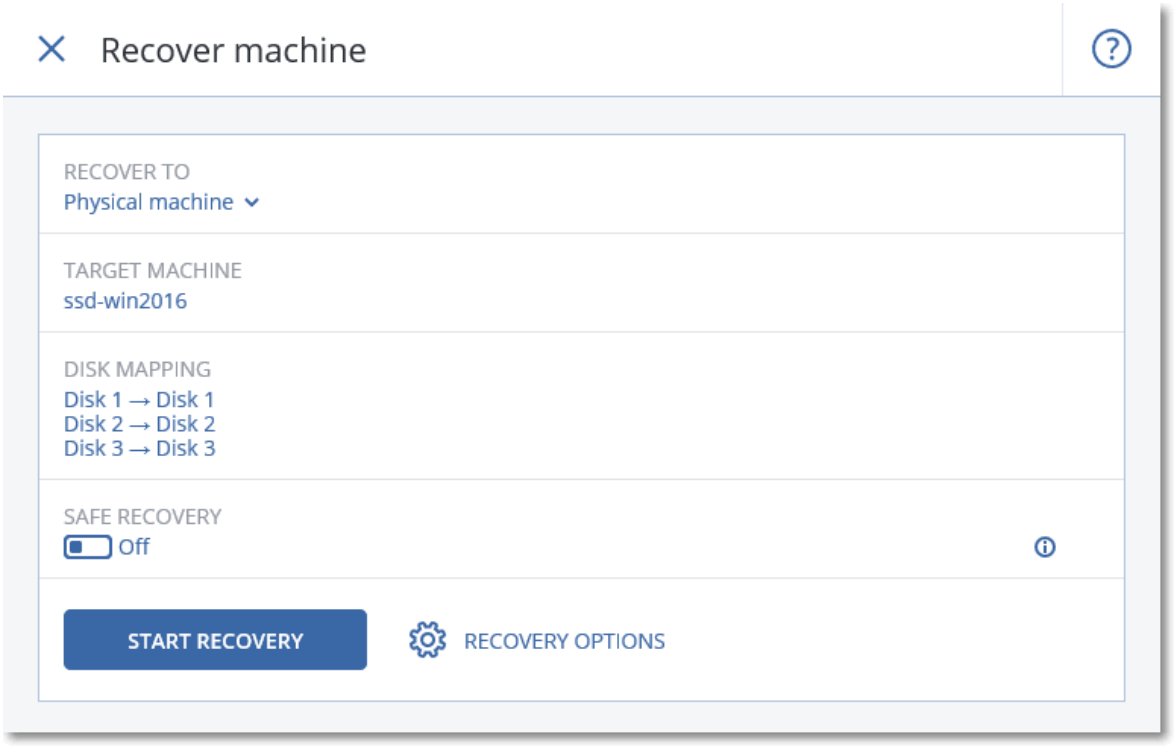
Para recuperar un equipo físico

1. Seleccione el equipo del que se ha realizado la 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 el equipo no está conectado a Internet, no se muestran los puntos de recuperación. Realice una de las siguientes operaciones:
   - 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.
   - Recupere el equipo como se describe en "Recuperar discos usando dispositivos de inicio".
4. Haga clic en **Recuperar** > **Todo el equipo**.

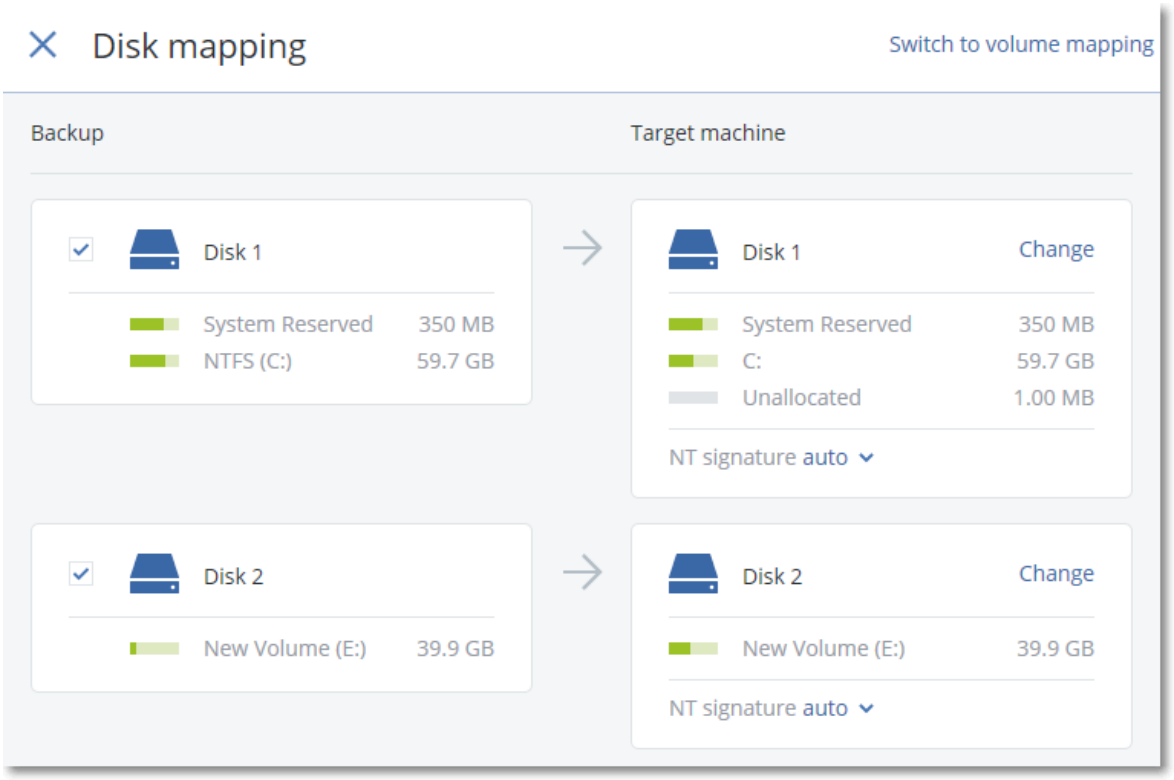
   El software asigna automáticamente los discos de las copias de seguridad a los discos del equipo de destino.

Para recuperar en otro equipo físico, haga clic en **Equipo de destino** y, a continuación, seleccione un equipo de destino que esté conectado.



5. Si no está satisfecho con el resultado de la asignación o si la asignación de discos falla, haga clic en **Asignación de volúmenes** puede volver a asignar los discos manualmente.

   La sección de asignación también permite elegir los discos individuales o volúmenes para la recuperación. Podrá cambiar entre recuperar discos y volúmenes utilizando el enlace **Cambiar a...** ubicado en la esquina superior derecha.



6. [Solo disponible para equipos Windows en los que hay instalado un agente de protección] Habilite el conmutador **Recuperación segura** para garantizar que los datos recuperados están libres de malware. Para obtener más información sobre cómo funciona la recuperación segura, consulte "Recuperación segura" (p. 521).
7. Haga clic en **Iniciar recuperación**.
8. Confirme si desea sobrescribir los discos con sus respectivas copias de seguridad. Elija si desea reiniciar el equipo automáticamente.

El proceso de recuperación se muestra en la pestaña **Actividades**.

De equipo físico a virtual

Puede recuperar una máquina física en una máquina virtual en uno de los hipervisores compatibles. También hay un mecanismo para migrar de una máquina física a una máquina virtual. Para obtener más información sobre las rutas de migración P2V compatibles, consulte "Migración de máquinas".

En esta sección se describe la recuperación de un equipo físico como equipo virtual mediante la interfaz web. Esta operación se puede realizar si hay instalado y registrado por lo menos un Agente para el correspondiente hipervisor en el Servidor de gestión de Acronis. Por ejemplo, para la recuperación en VMware ESXi se necesita al menos un agente para VMware y para la recuperación en Hyper-V debe haber al menos un agente para Hyper-V instalado y registrado en el entorno.

La recuperación a través de la interfaz web no está disponible para los inquilinos en el modo de Cumplimiento.

Nota
No puede recuperar equipos 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.

Además, no puede recuperar copias de seguridad de máquinas físicas macOS como si fuesen máquinas virtuales.

Para recuperar un equipo físico como un equipo virtual

1. Seleccione el equipo del que se ha realizado la 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.

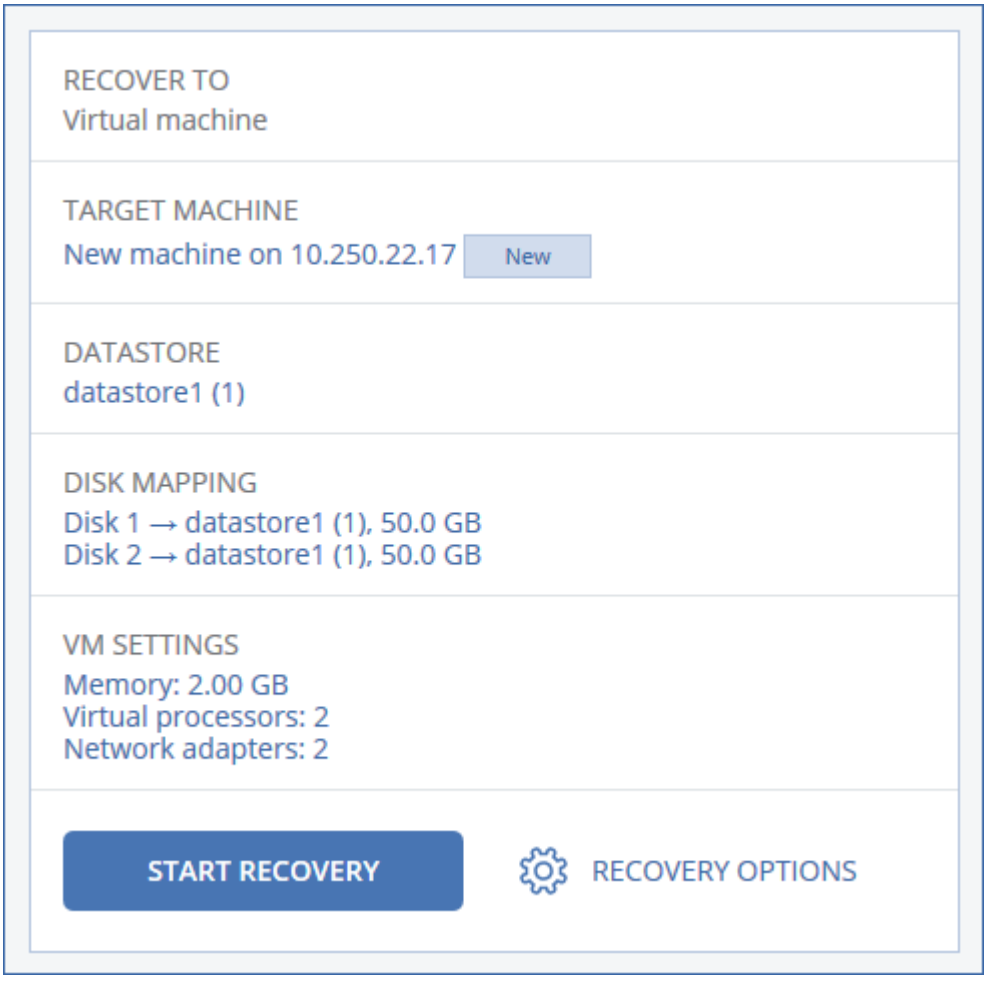
   Si el equipo no está conectado a Internet, no se muestran los puntos de recuperación. Realice una de las siguientes operaciones:
   - Si la copia de seguridad se encuentra en el almacenamiento compartido o en la cloud (es decir, otros agentes pueden acceder a ella), haga clic en **Seleccionar equipo**, seleccione un equipo 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.
   - Recupere el equipo como se describe en "Recuperar discos usando dispositivos de inicio".
4. Haga clic en **Recuperar** > **Todo el equipo**.
5. En **Recuperar en**, seleccione **Equipo virtual**.
6. Haga clic en **Equipo de destino**.
   a. Seleccione el hipervisor.

      Nota
      Debe haber al menos un agente para el hipervisor instalado y registrado en el Servidor de gestión de Acronis.

   b. Seleccione si desea realizar la recuperación en un equipo nuevo o en otro ya existente. Es preferible usar la opción de nuevo equipo porque no requiere que la configuración de disco del equipo de destino coincida exactamente con la configuración de disco de la copia de seguridad.
   c. Seleccione el servidor y especifique el nuevo nombre de equipo, o bien seleccione un equipo de destino existente.
   d. Haga clic en **Aceptar**.
7. [Para Virtuozzo Hybrid Infrastructure] Haga clic en **Configuración de VM** para seleccionar **Variante**. De manera opcional, puede cambiar el tamaño de la memoria, el número de procesadores y las conexiones de red de la máquina virtual.

Nota
Para Virtuozzo Hybrid Infrastructure, la selección de variante es un paso obligatorio.

8. [Opcional] Configure las opciones de recuperación adicionales:
   - [No disponible para Virtuozzo Hybrid Infrastructure] 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.
   - Haga clic en **Asignación de discos** para seleccionar el almacén de datos (almacenamiento), interfaz y modo de aprovisionamiento para cada unidad de disco virtual. La sección de asignación también permite elegir discos individuales para la recuperación.
     Para la Virtuozzo Hybrid Infrastructure, solo puede seleccionar la directiva de almacenamiento de los discos de destino. Para hacerlo, seleccione el disco de destino deseado y, a continuación, haga clic en Cambiar. En la ficha que se abre, haga clic en el icono de engranaje, seleccione la directiva de almacenamiento y, a continuación, haga clic en Listo.
   - [Para VMware ESXi, Hyper-V y Red Hat Virtualization/oVirt] 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.



9. [Solo disponible para equipos Windows en los que hay instalado un agente de protección] Habilite el conmutador **Recuperación segura** para garantizar que los datos recuperados están libres de malware. Para obtener más información sobre cómo funciona la recuperación segura, consulte "Recuperación segura" (p. 521).
10. Haga clic en **Iniciar recuperación**.
11. Al realizar la recuperación en un equipo virtual existente, confirme que desea sobrescribir los discos.

El proceso de recuperación se muestra en la pestaña **Actividades**.

Recuperación de una máquina virtual

Puede recuperar equipos virtuales gracias a sus copias de seguridad.

Nota
No puede recuperar copias de seguridad en la consola de Cyber Protect para inquilinos en el modo de Cumplimiento. Para obtener más información sobre cómo recuperar dichas copias de seguridad, consulte "Recuperación de copias de seguridad para inquilinos en el modo de Cumplimiento" (p. 1151).

Requisitos previos

- Durante la recuperación en un equipo virtual, éste debe permanecer detenido. De forma predeterminada, el software detiene el equipo sin previo aviso. Cuando se complete la recuperación, debe iniciar el equipo manualmente. Puede modificar este comportamiento mediante la opción de recuperación de gestión de energía del equipo virtual (haga clic en **Opciones de recuperación** > **Gestión de energía del equipo virtual**).

Procedimiento

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 **Recuperar** > **Todo el equipo**.
3. Si desea recuperar el equipo virtual en un equipo físico, seleccione **Equipo físico** en **Recuperar en**. De lo contrario, omita este paso.

   La recuperación en un equipo físico solo es posible si la configuración de disco del equipo de destino coincide exactamente con la configuración de disco de la copia de seguridad.

   En caso afirmativo, siga con el paso 4 de la sección "Equipo físico". En caso contrario, le recomendamos que realice la migración V2P mediante un dispositivo de arranque.
4. [Opcional] De forma predeterminada, el software selecciona automáticamente el equipo original como equipo de destino. Para recuperar el equipo virtual en otro equipo virtual, haga clic en **Equipo de destino** y, a continuación, haga lo siguiente:

a. Seleccione el hipervisor (**VMware ESXi**, **Hyper-V**, **Virtuozzo**, **Virtuozzo Hybrid Infrastructure**, **Scale Computing HC3** o **oVirt**).

   Solo los equipos virtuales Virtuozzo pueden recuperarse en Virtuozzo. Para obtener más información sobre la migración del entorno virtual al virtual, consulte "Migración de equipos".

b. Seleccione si desea realizar la recuperación en un equipo nuevo o en otro ya existente.

c. Seleccione el servidor y especifique el nuevo nombre de equipo, o bien seleccione un equipo de destino existente.

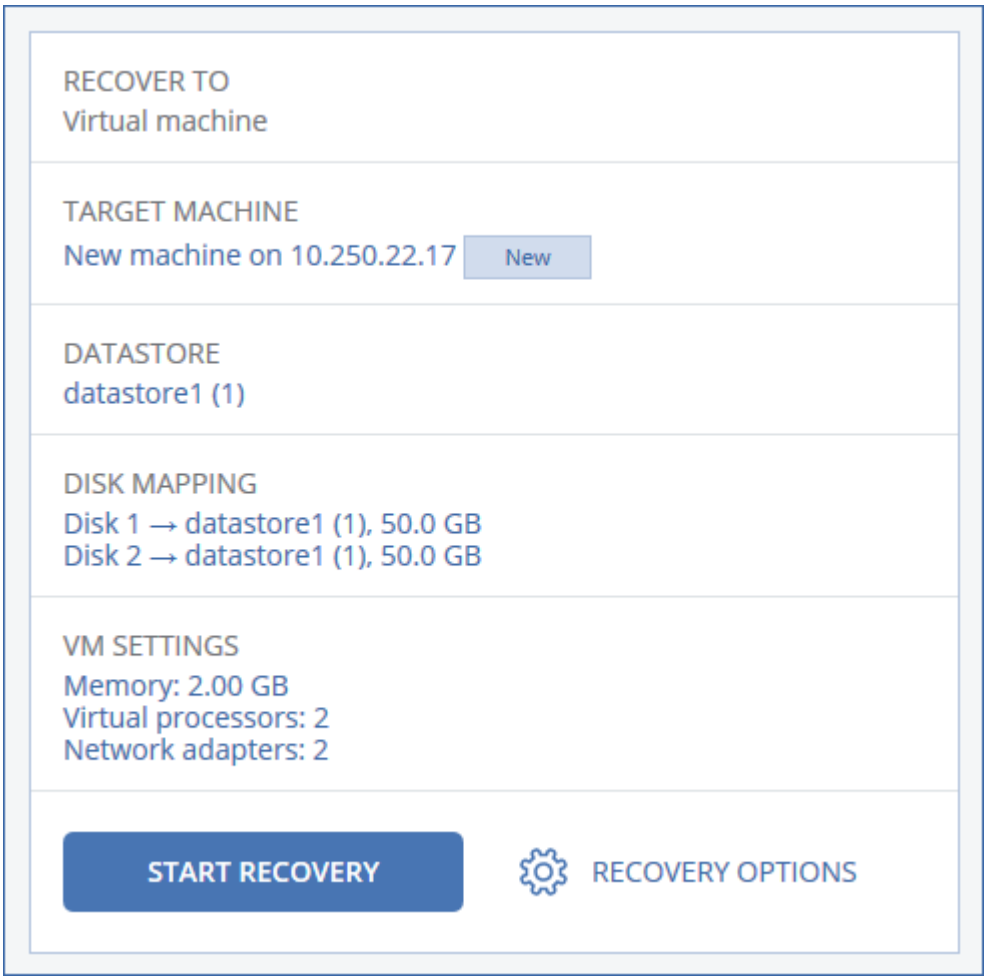
d. Haga clic en **Aceptar**.

5. Configure las opciones de recuperación adicionales que necesite.

   - [Opcional] [No disponible para Virtuozzo Hybrid Infrastructure ni para Scale Computing HC3] Haga clic en **Almacén de datos** para ESXi, **Ruta** para Hyper-V y Virtuozzo o **Dominio de almacenamiento** para Red Hat Virtualization (oVirt). A continuación, seleccione el almacén de datos (almacenamiento) para la máquina virtual.
   - [Opcional] Para ver el almacén de datos (almacenamiento), la interfaz y el modo de aprovisionamiento para cada unidad de disco virtual, haga clic en **Asignación de discos**. Puede modificar esta configuración a menos que esté recuperando un contenedor de Virtuozzo o un equipo virtual de la Virtuozzo Hybrid Infrastructure.

     Para la Virtuozzo Hybrid Infrastructure, solo puede seleccionar la directiva de almacenamiento de los discos de destino. Para hacerlo, seleccione el disco de destino deseado y, a continuación, haga clic en **Cambiar**. En la ficha que se abre, haga clic en el icono de engranaje, seleccione la directiva de almacenamiento y, a continuación, haga clic en **Listo**.

     La sección de asignación también permite elegir discos individuales para la recuperación.
   - [Opcional] [Disponible para VMware ESXi, Hyper-V y Virtuozzo] Haga clic en **Configuración de VM** para cambiar el tamaño de la memoria, el número de procesadores y las conexiones de red de la máquina virtual.
   - [Para Virtuozzo Hybrid Infrastructure] Seleccione **Variante** para cambiar el tamaño de la memoria y el número de procesadores de la máquina virtual.



6. [Solo disponible para equipos Windows en los que hay instalado un agente de protección] Habilite el conmutador **Recuperación segura** para garantizar que los datos recuperados están libres de malware. Para obtener más información sobre cómo funciona la recuperación segura, consulte "Recuperación segura" (p. 521).
7. Haga clic en **Iniciar recuperación**.
8. Al realizar la recuperación en un equipo virtual existente, confirme que desea sobrescribir los discos.

El proceso de recuperación se muestra 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. 750).

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:
   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. 768).

   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.
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.

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**.

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

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.

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.

Recuperación de archivos

Recuperación de archivos en la consola de Cyber Protect

Nota
No puede recuperar copias de seguridad en la consola de Cyber Protect para inquilinos en el modo de Cumplimiento. Para obtener más información sobre cómo recuperar dichas copias de seguridad, consulte "Recuperación de copias de seguridad para inquilinos en el modo de Cumplimiento" (p. 1151).

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.
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 "Máscara" (p. 483).

   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 "Descargar archivos del almacenamiento en la cloud" (p. 537).
8. Haga clic en **Recuperar**.

   En **Recuperar en**, 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. 542).

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.

     Nota
     No se pueden usar vínculos simbólicos.

   - Una carpeta de red accesible desde el equipo de destino
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**

El proceso de recuperación se muestra en la pestaña **Actividades**.

Descargar archivos del almacenamiento en la cloud

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.

Nota
Solo puede acceder a la consola de Web Restore si es un administrador de cliente Cyber Protection o un usuario de inquilino de cliente. No se permiten los roles de usuario en el nivel de partner.

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.

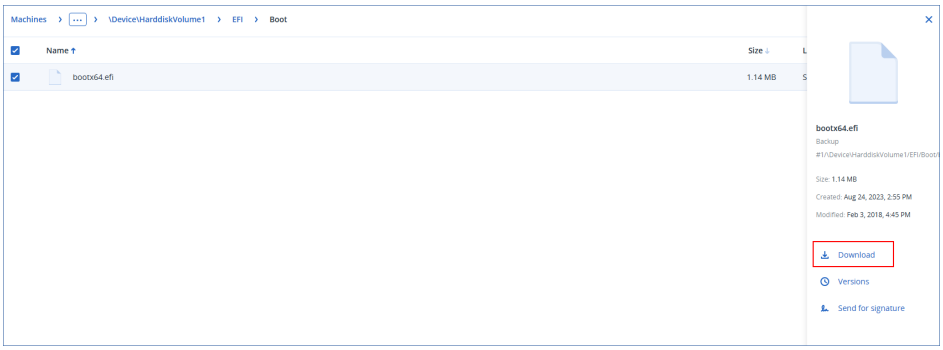
Para descargar archivos y carpetas del almacenamiento en la nube

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**.
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.

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.
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 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. 768).

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:
   `<nombre del equipo> - <GUID del plan de protección>`
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

No puede recuperar copias de seguridad en la consola de Cyber Protect para inquilinos en el modo de Cumplimiento. Para obtener más información sobre cómo recuperar dichas copias de seguridad, consulte "Recuperación de copias de seguridad para inquilinos en el modo de Cumplimiento" (p. 1151).

Recuperación en 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 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. 548), 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
```

Recuperación del estado del sistema

Nota
No puede recuperar copias de seguridad en la consola de Cyber Protect para inquilinos en el modo de Cumplimiento. Para obtener más información sobre cómo recuperar dichas copias de seguridad, consulte "Recuperación de copias de seguridad para inquilinos en el modo de Cumplimiento" (p. 1151).

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.

El proceso de recuperación se muestra 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. 750).

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**.
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.

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.

	Discos			**Archivos**				**Equipos virtuales**	**SQL y Exchange**
	Windows	**Linux**	**Dispositivo de arranqu**	**Windows**	**Linux**	**macOS**	**Dispositivo de arranqu**	**ESXi, Hyper-V y**	**Windows**

			e				e	Virtuozzo	
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 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. 213).

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 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
- La transferencia entre UEFI y BIOS no es compatible si la copia de seguridad está almacenada en un dispositivo de cintas.

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**.

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.

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.

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**.

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.

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.

* 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 Agente para VMware, Agente para Hyper-V, Agente para Virtuozzo, Agente para Scale Computing HC3 o Agente para oVirt realizan la recuperación en una máquina virtual.

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**.

Operaciones con copias de seguridad

Pestaña Almacenamiento de la copia de seguridad

La pestaña **Almacenamiento de la copia de seguridad** le permite acceder a todas las copias de seguridad, incluidas las de los equipos no conectados, las de equipos que ya no estén registrados en el servicio Cyber Protection, las de nubes públicas como Microsoft Azure y las copias de seguridad huérfanas[1].

Las copias de seguridad creadas a través de `acrocmd` se marcan como huérfanas. Las copias de seguridad creadas en la versión 12.5 del producto también se identifican como huérfanas.

Nota
Tenga en cuenta que también se cobran las copias de seguridad huérfanas.

Las copias de seguridad almacenadas en una ubicación compartida (como un recurso compartido de SMB o NFS) son visibles para todos los usuarios que dispongan del permiso de lectura para dicha ubicación.

En Windows, los archivos de copia de seguridad heredan los permisos de acceso de su carpeta principal. Por lo tanto, le recomendamos restringir los permisos de lectura para esta carpeta.

En el caso del almacenamiento en la cloud, los usuarios solo tienen acceso a sus propias copias de seguridad.

Un administrador puede visualizar las copias de seguridad en la nube en nombre de cualquier cuenta que pertenezca a dicha unidad o compañía y a sus grupos secundarios mediante la selección del almacenamiento en la nube para la cuenta. Para seleccionar el dispositivo que desea utilizar para obtener datos de la nube, haga clic en **Cambiar** en la fila **Equipo desde el cual examinar**. La pestaña **Almacenamiento de la copia de seguridad** muestra las copias de seguridad de todos los equipos que se han registrado a lo largo de la historia de la cuenta seleccionada.

Las copias de seguridad creadas por Agente para Microsoft 365 en la *nube* y las de los datos de Google Workspace no se muestran en la ubicación **Almacenamiento en la nube**, sino en una sección separada llamada **Copias de seguridad de aplicaciones en la nube**.

Las ubicaciones de copia de seguridad que se usan en los planes de protección se añaden automáticamente a la pestaña **Almacenamiento de la copia de seguridad**. Para añadir una carpeta personalizada (por ejemplo, un dispositivo USB extraíble) a la lista de ubicaciones de copia de seguridad, haga clic en **Examinar** y especifique la ruta de la carpeta.

Si ha usado el administrador de archivos para añadir o eliminar alguna copia de seguridad, haga clic en el icono de engranaje que se encuentra junto al nombre del ubicación y haga clic en **Actualizar**.

[1]Una copia de seguridad huérfana es una copia de seguridad que ya no está asociada a un plan de protección.

Advertencia.
No intente editar los archivos de copia de seguridad de forma manual porque el archivo podría dañarse y hacer que las copias de seguridad no se puedan utilizar. Además, le recomendamos que utilice la replicación de copia de seguridad en lugar de mover los archivos de copia de seguridad de forma manual.

La ubicación de una copia de seguridad (excepto en el caso del almacenamiento en la nube) desaparece de la pestaña **Almacenamiento de la copia de seguridad** al eliminar del servicio Cyber Protection los equipos que hayan realizado copias de seguridad a dicha ubicación. De este modo, no deberá pagar por las copias de seguridad almacenadas en esta ubicación. Cuando se realice una copia de seguridad en la ubicación, esta se volverá a añadir junto a todas las copias de seguridad que contenga.

En la pestaña **Almacenamiento de la copia de seguridad**, puede filtrar las copias de seguridad de la lista utilizando los siguientes criterios:

- **Solo con datos forenses**: solo se mostrarán las copias de seguridad que tengan datos forenses.
- **Solo copias de seguridad anteriores a la actualización creadas con Gestión de parches**: solo se mostrarán las copias de seguridad que se crearon durante la gestión de parches ejecutada antes de la instalación de parches.

Pasos para seleccionar un punto de recuperación desde la pestaña Almacenamiento de la copia de seguridad

1. En la pestaña **Almacenamiento de la copia de seguridad**, seleccione la ubicación en la que se almacenan las copias de seguridad.
   El software muestra todas las copias de seguridad que su cuenta tiene permiso para visualizar en la ubicación seleccionada. Las copias de seguridad se combinan en grupos. Los nombres de los grupos se basan en la siguiente plantilla:
   `<nombre del equipo> - <nombre del plan de protección>`
2. Seleccione un grupo del que desee recuperar los datos.
3. [Opcional] Haga clic en **Cambiar** junto a **Equipo desde el cual examinar** y, a continuación, seleccione otro equipo. Algunas copias de seguridad solo pueden examinarse mediante agentes específicos. Por ejemplo, debe seleccionar un equipo que ejecute el Agente para SQL para examinar las copias de seguridad de las bases de datos de Microsoft SQL Server.

   Importante
   Tenga en cuenta que **Equipo desde el cual examinar** es un destino predeterminado para realizar una recuperación desde una copia de seguridad de un equipo físico. Después de seleccionar un punto de recuperación y hacer clic en **Recuperar**, compruebe la configuración de **Equipo de destino** para asegurarse de que desea recuperar en este equipo determinado. Para cambiar el destino de recuperación, especifique otro equipo en **Equipo desde el cual examinar**.

4. Haga clic en **Mostrar copias de seguridad**.
5. Seleccione el punto de recuperación.

Pasos para agregar una ubicación a una copia de seguridad

Nota
Esta operación solo está disponible si tiene un agente en línea.

En la pestaña **Almacenamiento de la copia de seguridad**, haga clic en **Agregar ubicación**.

Seleccione una ubicación de uno de los siguientes tipos y haga clic en **Listo**:

- Carpeta local
- Carpeta de red
- Secure Zone
- Carpeta NFS
- Nube pública

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.
- 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:

   `<nombre del equipo> - <GUID del plan de protección>`
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**.
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

Al validar una copia de seguridad, verifica que puede recuperar los datos con su ayuda. Para obtener más información sobre esta operación, consulte "Validación" (p. 209).

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 "Pestaña Almacenamiento de la copia de seguridad" (p. 553).
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.

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 "Replicación de copias de seguridad" (p. 206).

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 "Pestaña Almacenamiento de la copia de seguridad" (p. 553).
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**.

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.

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.

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: <nombre de la carga de trabajo> - <nombre del plan de protección>
   - Archivos de copia de seguridad de nube a nube: <nombre del usuario> o <nombre de la unidad> o <nombre del equipo> - <servicio en la nube> - <nombre del plan de protección>
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.

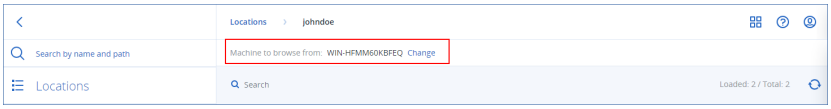
Eliminación de copias de seguridad fuera de la consola de Cyber Protect

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

actualizar la ubicación de la copia de seguridad para sincronizar los cambios con la consola de Cyber Protect.

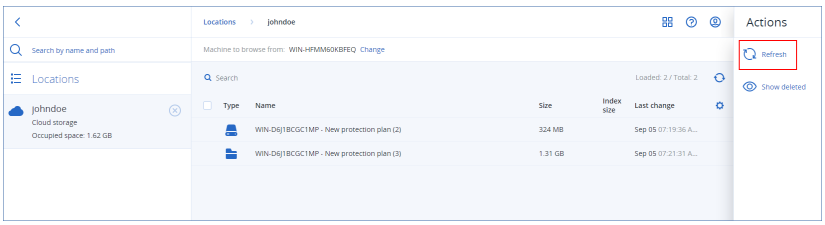
Prerrequisito

- 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. 563) y "¿Se muestran los atascos en las cargas de trabajo, los agentes y las ubicaciones de copia de seguridad?" (p. 565).

¿Qué es un atasco?

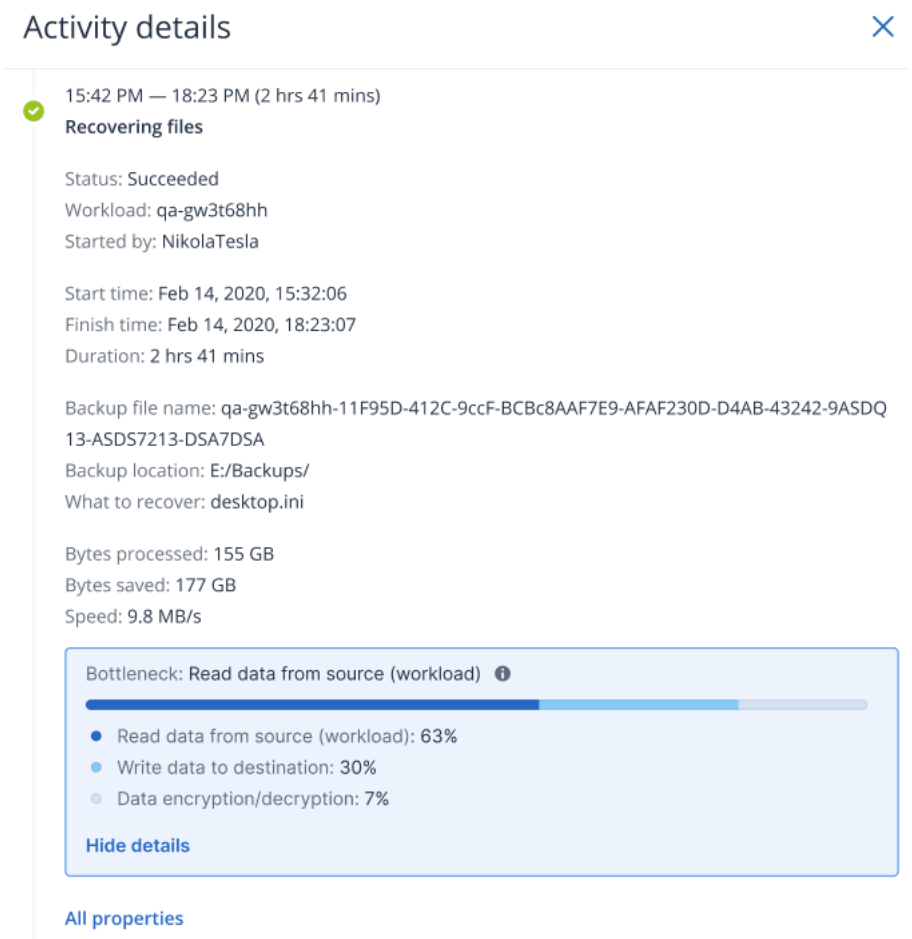
Los atascos suelen estar causados por un componente lento de la cadena de procesamiento, es decir, un componente al que tienen que esperar el resto de componentes.

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 %**).



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.

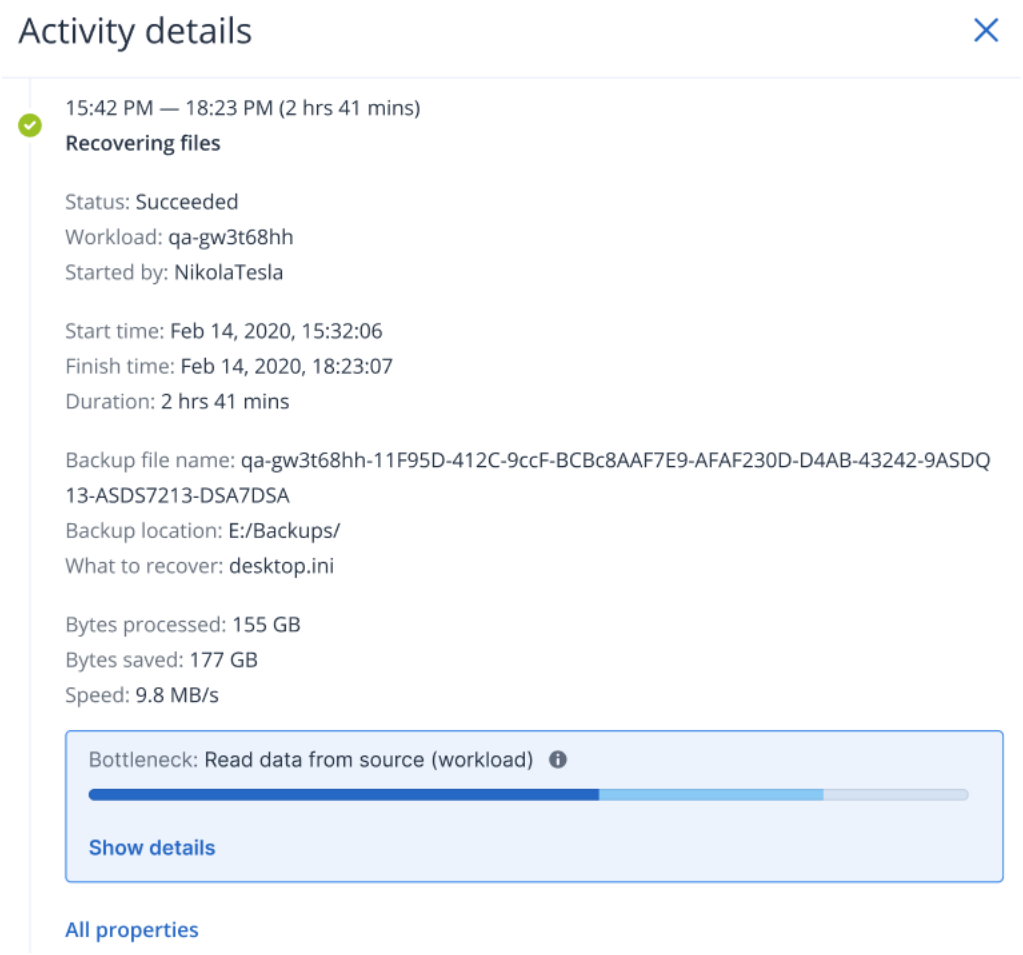
Visualización de detalles de atasco

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.

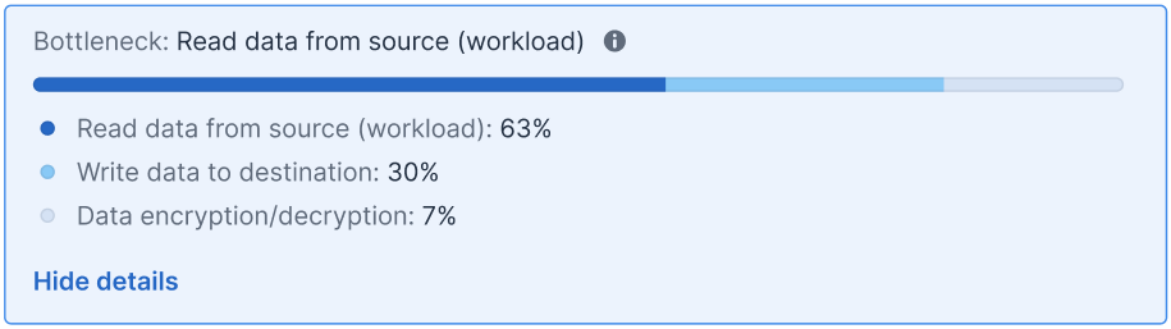
Para obtener más información sobre la definición y los conceptos básicos de los tipos de atascos, consulte "Descripción de la detección de atascos" (p. 561).

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.



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.

¿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
  - Agente para Scale Computing
  - 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

- 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.

Puede seleccionar servicios de nube pública, como Microsoft Azure y Amazon S3 (Simple Storage Service), como destinos de copia de seguridad en la consola de Cyber Protect.

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.

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. 578)), 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 realizar copias de seguridad**.

     Para obtener más información sobre cómo trabajar con los planes de protección, consulte "Planes de protección y módulos" (p. 223).
   - 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**.

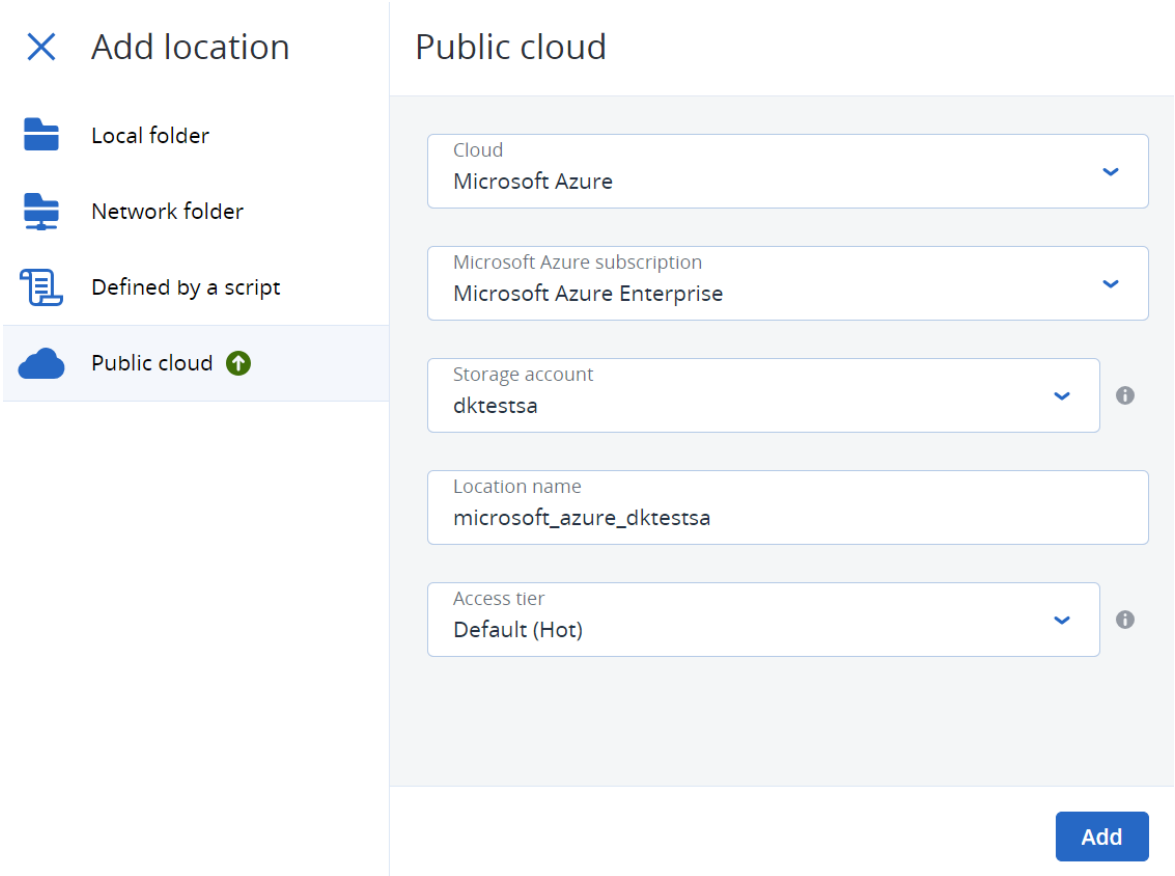
     Para obtener más información sobre cómo gestionar las ubicaciones de almacenamiento de copia de seguridad, consulte "Pestaña Almacenamiento de la copia de seguridad" (p. 553).
2. Haga clic en **Añadir ubicación**.
3. Desde la lista desplegable de **Nubes públicas**, seleccione **Microsoft Azure**.
4. 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 **Añadir** 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 a una suscripción de Microsoft Azure, consulte "Añadir el acceso a una suscripción de Microsoft Azure" (p. 579).
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`. Además, la cuenta de almacenamiento seleccionada debe ser del tipo Almacenamiento V2.

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_[cuenta de almacenamiento]` y el nivel de acceso seleccionado es **Predeterminado (frecuente)**. Se pueden modificar ambos campos si es necesario.

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**.



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 realizar 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. 573).

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. 582)), 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

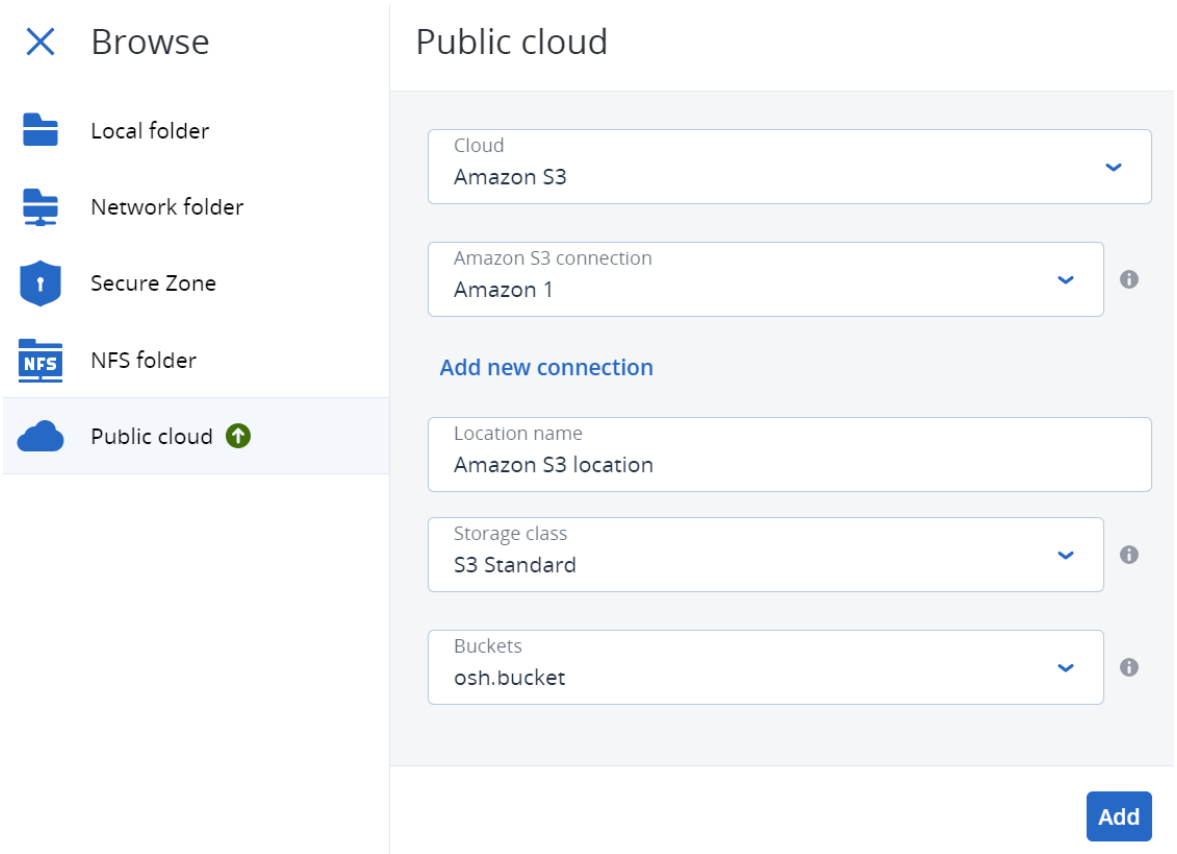
1. En la consola de Cyber Protect, realice uno de los siguientes procedimientos:
   - Si está creando o editando un plan de protección, vaya a **Dispositivos** y seleccione la carga de trabajo de la que quiera hacer una copia de seguridad en Amazon S3. En la sección de **Copia de seguridad** del plan de protección de la carga de trabajo seleccionada, haga clic en el enlace en la fila **Dónde hacer la copia de seguridad**.
     Para obtener más información sobre cómo trabajar con los planes de protección, consulte "Planes de protección y módulos" (p. 223).

- Si está gestionando sus ubicaciones de almacenamiento de copia de seguridad y quiere añadir Amazon S3 como una nueva ubicación, vaya a **Almacenamiento de copia de seguridad**.

  Para obtener más información sobre cómo gestionar las ubicaciones de almacenamiento de copia de seguridad, consulte "Pestaña Almacenamiento de la copia de seguridad" (p. 553).

2. Haga clic en **Añadir ubicación**.
3. Desde la lista desplegable de **Nubes públicas**, seleccione **Amazon S3**.
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 nueva conexión**. 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. 582). Cuando se añada la conexión, continúe al siguiente paso.



5. Defina lo siguiente:
   - En el campo **Nombre de 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
- En el campo **Bucket**, selecciona el bucket relevante de 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 hacer la copia 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 obtener más información, consulte "Visualización y actualización de ubicaciones de copia de seguridad en la nube pública" (p. 573).

Definición de una ubicación de copia de seguridad en Wasabi

Nota
Para configurar ubicaciones de copia de seguridad en Wasabi, 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 Wasabi , debe definir la ubicación de la copia de seguridad de Wasabi en la consola de Cyber Protect, y luego conectarse a la conexión relevante de Wasabi. Puede hacer esto de las siguientes maneras:

- Al crear o editar un plan de protección.
- Al definir y gestionar ubicaciones de almacenamiento de copia de seguridad.

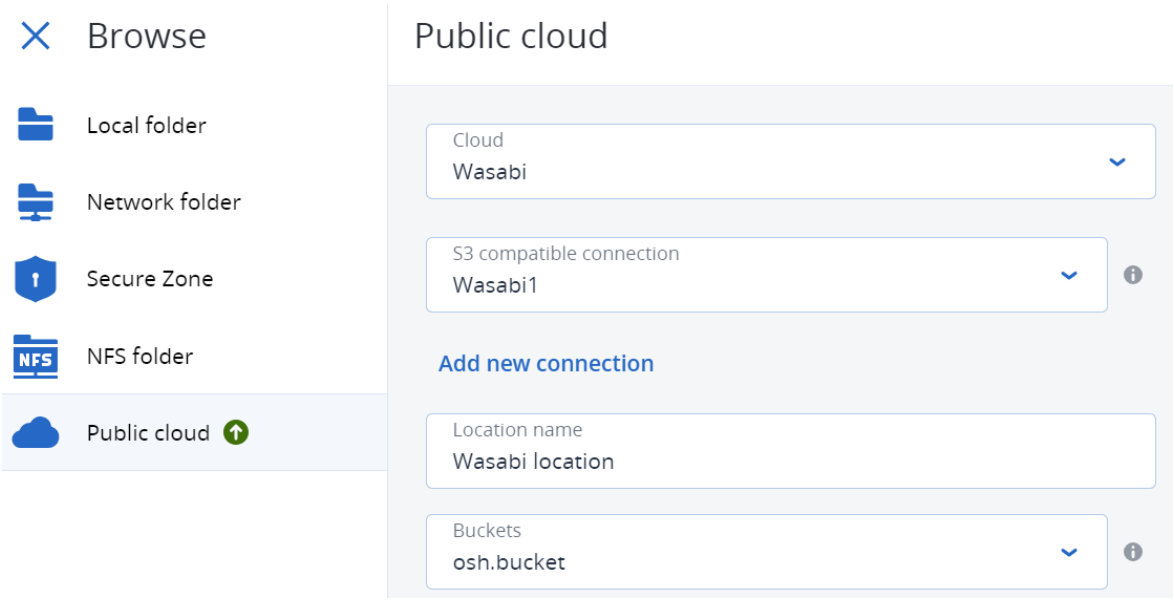
Importante
Tanto los administradores como los usuarios no administradores pueden hacer copias de seguridad de las cargas de trabajo en Wasabi.

Los usuarios no administradores pueden añadir acceso a una conexión de Wasabi (ver "Gestión del acceso a otros servicios de almacenamiento en la nube pública" (p. 582)), pero solo pueden aplicar planes de protección donde la ubicación de la copia de seguridad está conectada a la conexión de Wasabi 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 Wasabi 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 copia de seguridad en Wasabi

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 luego seleccione la carga de trabajo de la que quiera hacer una copia de seguridad en Wasabi. 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 hacer la copia de seguridad**.
     Para obtener más información sobre cómo trabajar con los planes de protección, consulte "Planes de protección y módulos" (p. 223).
   - Si está gestionando sus ubicaciones de almacenamiento de copia de seguridad y quiere añadir Wasabi como una nueva ubicación, vaya a **Almacenamiento de copia de seguridad**.
     Para obtener más información sobre cómo gestionar las ubicaciones de almacenamiento de copia de seguridad, consulte "Pestaña Almacenamiento de la copia de seguridad" (p. 553).
2. Haga clic en **Añadir ubicación**.
3. Desde la lista desplegable de **Nubes públicas**, seleccione **Wasabi**.
4. Si la conexión relevante de Wasabi ya está registrada en la consola de Cyber Protect, selecciónela de la lista de conexiones.
   Si la conexión relevante no está registrada en la consola de Cyber Protect, haga clic en **Añadir nueva conexión**. Para obtener más información sobre cómo añadir y definir el acceso a una conexión Wasabi, consulte "Añadir acceso a una conexión de nube pública" (p. 582). Cuando se añada la conexión, continúe al siguiente paso.



5. Defina lo siguiente:
   - En el campo **Nombre de 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 Wasabi** ya existe, el nombre se actualizará automáticamente a **almacenamiento de Wasabi 1**.

   - En el campo **Bucket**, seleccione el bucket de Wasabi relevante.
6. Haga clic en **Agregar**.

   Si está creando o editando un plan de protección, la ubicación de la copia de seguridad de Wasabi se establece como la ubicación en la fila **Dónde hacer la copia 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 gestiona sus ubicaciones de almacenamiento de copia de seguridad, puede ver y actualizar los detalles de la ubicación cuando sea necesario. La ubicación de Wasabi 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. 573).

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 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. 581). 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. 582).

Nota
No puede actualizar manualmente ni eliminar una ubicación de copia de seguridad en la nube pública en el módulo de **Almacenamiento de copias 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 "Pestaña Almacenamiento de la copia de seguridad" (p. 553).
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 realizar copias de seguridad**.
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. 579)). 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 la nube pública 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,

cuando se trabaja con 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.

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 fue previamente eliminada. Para obtener más información, contacte con el equipo de Soporte.

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
- Wasabi

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).

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 Acronis 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.

Ejemplos

El siguiente ejemplo de política muestra el conjunto mínimo de permisos para un amplio alcance de recursos. Tenga en cuenta que `*` indica todos los recursos.

```
{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action":
"s3:ListAllMyBuckets", "Resource": "*" }, { "Effect": "Allow", "Action": [
"s3:GetBucketLocation", "s3:GetBucketObjectLockConfiguration" ], "Resource": "*" },
{ "Effect": "Allow", "Action": "sts:GetFederationToken", "Resource": "*" }, {
"Effect": "Allow", "Action": [ "s3:GetBucketLocation", "s3:PutObject",
"s3:GetObject", "s3:DeleteObject" ], "Resource": "*" }, { "Effect": "Allow",
"Action": [ "s3:ListBucket" ], "Resource": "*" } ] }
```

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", "Resource": "*" }, { "Effect": "Allow", "Action": [
"s3:GetBucketLocation", "s3:GetBucketObjectLockConfiguration" ], "Resource":
"arn:aws:s3:::[BUCKETNAME]" }, { "Effect": "Allow", "Action":
"sts:GetFederationToken", "Resource": "*" }, { "Effect": "Allow", "Action": [
"s3:GetBucketLocation", "s3:PutObject", "s3:GetObject", "s3:DeleteObject" ],
"Resource": "arn:aws:s3:::[BUCKETNAME]/*" }, { "Effect": "Allow", "Action": [
"s3:ListBucket" ], "Resource": "arn:aws:s3:::[BUCKETNAME]" } ] }
```

Claves de acceso

Acronis requiere para cada conexión de Amazon S3 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
Acronis actualmente no admite la versión del bucket y el bloqueo de objetos en Amazon S3, incluso cuando está habilitado en el bucket.

Copia de seguridad en Wasabi

Cuando hace una copia de seguridad en Wasabi, 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 Wasabi, asegúrese de que las políticas relevantes se apliquen a los grupos y usuarios pertinentes en Wasabi.

Ejemplos

La siguiente política de ejemplo muestra el conjunto mínimo de permisos con un amplio alcance de recursos. Tenga en cuenta que * indica cualquier recurso.

```
{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action":
"s3:ListAllMyBuckets", "Resource": "*" }, { "Effect": "Allow", "Action":
"s3:GetBucketLocation", "Resource": "*" }, { "Effect": "Allow", "Action": [
"iam:CreateRole", "iam:AttachRolePolicy", "sts:GetCallerIdentity", "sts:AssumeRole"
], "Resource": "*" }, { "Effect": "Allow", "Action": [ "s3:PutObject",
"s3:GetObject", "s3:DeleteObject" ], "Resource": "*" }, { "Effect": "Allow",
"Action": "s3:ListBucket", "Resource": "*" } ] }
```

La siguiente política de ejemplo muestra permisos limitados con un alcance limitado de recursos. Tenga en cuenta que `[BUCKETNAME]` debe reemplazarse con el nombre del bucket, y `[ACCOUNTID]` con el ID de la cuenta de Wasabi.

```
{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action":
"s3:ListAllMyBuckets", "Resource": "*" }, { "Effect": "Allow", "Action":
"s3:GetBucketLocation", "Resource": "arn:aws:s3:::[BUCKETNAME]" }, { "Effect":
"Allow", "Action": [ "iam:CreateRole", "iam:AttachRolePolicy",
"sts:GetCallerIdentity", "sts:AssumeRole" ], "Resource": "arn:aws:iam::
[ACCOUNTID]:*" }, { "Effect": "Allow", "Action": [ "s3:PutObject", "s3:GetObject",
"s3:DeleteObject" ], "Resource": "arn:aws:s3:::[BUCKETNAME]/*" }, { "Effect":
"Allow", "Action": "s3:ListBucket", "Resource": "arn:aws:s3:::[BUCKETNAME]" } ] }
```

Claves de acceso

Acronis requiere claves de acceso para cada conexión de Wasabi, y se utilizan al definir la conexión de Wasabi. Para obtener más información sobre cómo generar claves de acceso e ID de claves de acceso, consulte la documentación de Wasabi.

Configuración del bucket

Al usar los buckets de Wasabi como ubicación de copia de seguridad, asegúrese de que el cubo esté configurado con los ajustes predeterminados. Para obtener más información sobre cómo trabajar con buckets, consulte la documentación de Wasabi.

Nota
Acronis actualmente no admite la versión del bucket y el bloqueo de objetos en Wasabi, incluso cuando está habilitado en el bucket.

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. 566).

Estas suscripciones de Microsoft Azure también se pueden configurar en la pantalla **Nubes públicas** (vaya a **Infraestructura > Nubes públicas**). Aquí podrá gestionar sus suscripciones, lo que incluye renovar el acceso, ver las propiedades y actividades de las mismas y eliminarlas.

Según su rol de usuario asignado, puede ser capaz de 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, puede ver y gestionar las suscripciones de Microsoft Azure añadidas por otros administradores y las añadidas por usuarios no administradores. Los usuarios no 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.

Importante
Acronis requiere los permisos mínimos para conectarse a una suscripción de Microsoft Azure. Para obtener más información sobre los permisos necesarios, consulte el artículo Auditoría y seguridad de conexión de Microsoft Azure (72684).

Añadir el acceso a una suscripción de Microsoft Azure

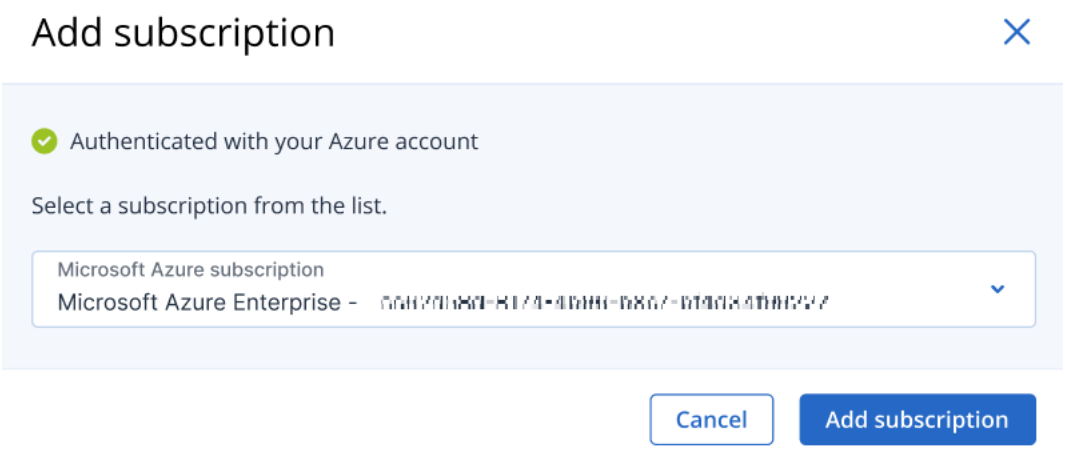
Al añadir una suscripción de Microsoft Azure en la consola de Cyber Protect, Acronis puede acceder de forma segura a su suscripción y hacer copias de seguridad directamente de las cargas de trabajo correspondientes en Microsoft Azure.

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 **Añadir**, 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 se complete la conexión, seleccione la suscripción correspondiente en la lista desplegable del diálogo que se muestra y haga clic en **Añadir 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. 580).

Para eliminar el acceso a la suscripción, consulte "Eliminar el acceso a una suscripción de Microsoft Azure" (p. 581).

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

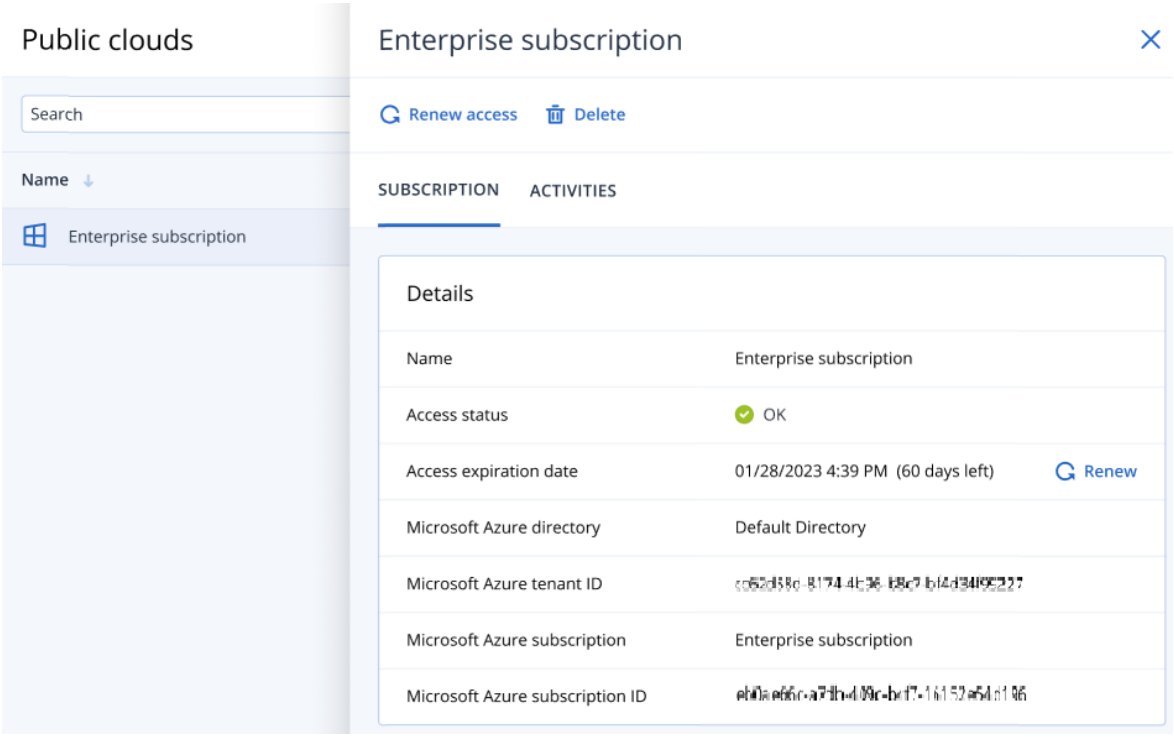
1. En la consola de Cyber Protect, vaya a **Infraestructura > Nubes públicas**.
2. Seleccione la suscripción correspondiente en la lista que se muestra.

   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**.



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.

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 de acceso para todos los servicios de almacenamiento en la nube pública, a excepción de Microsoft Azure, que se describe en "Gestionar el acceso a las suscripciones de Microsoft Azure" (p. 578).

Al conectarse a la cuenta de la nube pública 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 copias 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. 575).

Añadir acceso a una conexión de nube pública

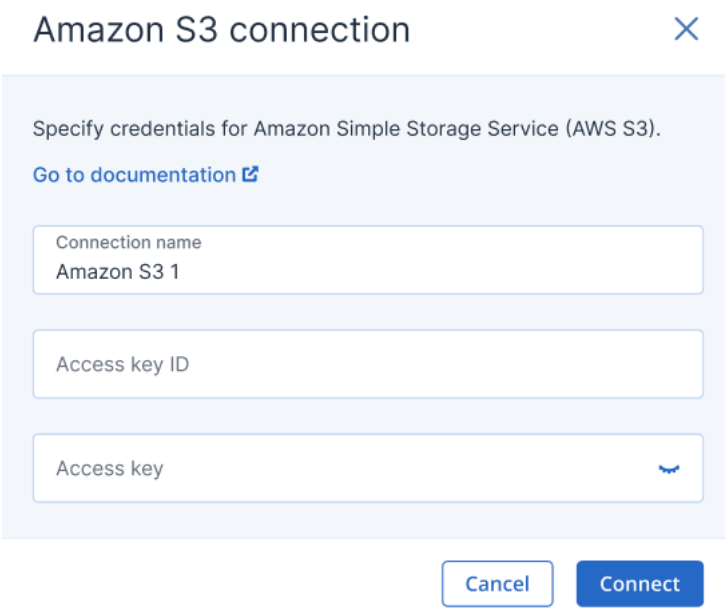
Después de añadir una conexión a la nube pública (como Amazon S3 o Wasabi) en la consola de Cyber Protect, Acronis puede acceder de manera segura a sus recursos en la nube y hacer copias de seguridad de las cargas de trabajo directamente en el almacenamiento en la nube pública correspondiente.

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 **Añadir** 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 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 a Acronis Access 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 requeridos por Acronis Access, consulte "Requisitos de acceso necesarios para hacer una copia de seguridad en el almacenamiento en la nube pública" (p. 575).

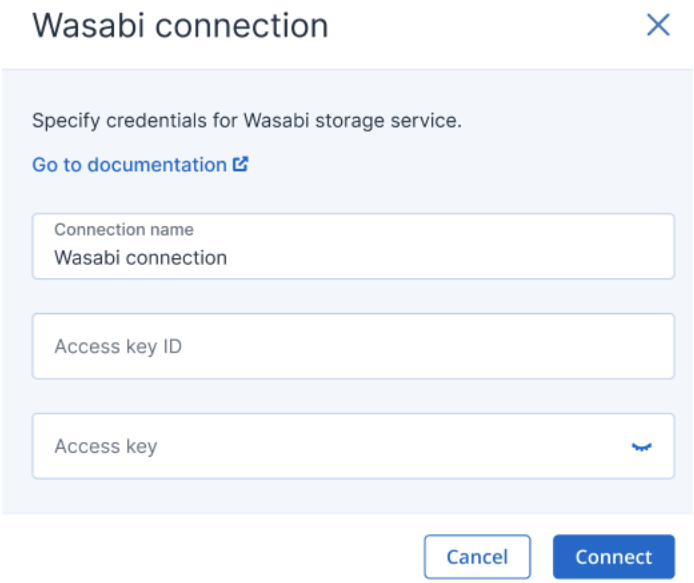
     

   - **Wasabi**

     En el diálogo que se muestra, defina lo siguiente:
     - **Nombre de la conexión**: El nombre para la conexión de Wasabi.
     - **ID de 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 a Acronis Access 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 requeridos por Acronis Access, consulte "Requisitos de acceso necesarios para hacer una copia de seguridad en el

almacenamiento en la nube pública" (p. 575).



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. 584).

   Para eliminar el acceso a la conexión, consulte "Eliminando el acceso a una conexión a la nube pública" (p. 585).

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.

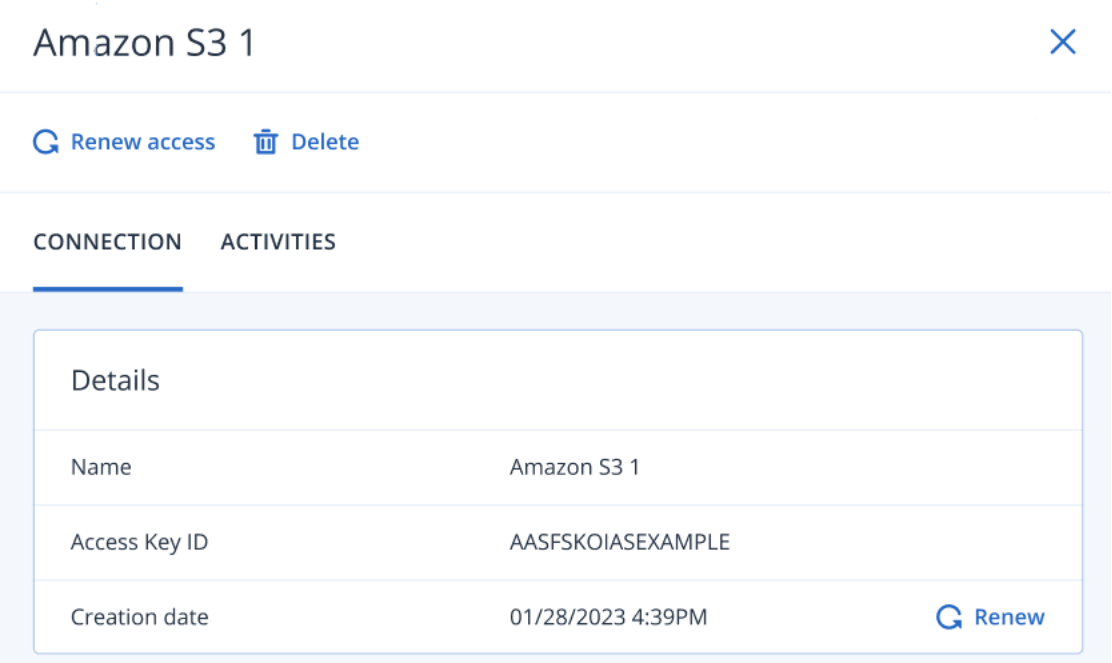
Pasos para renovar el certificado de acceso a su conexión a la nube pública

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**.

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.

Eliminando el acceso a una conexión a la nube pública

Debería eliminar el acceso a las conexiones de nube pública si no está respaldando cargas de trabajo en nubes públicas.

Pasos para eliminar el acceso a una conexión a la nube pública

Importante
No puede eliminar una conexión si actualmente se utiliza para copias de seguridad en una nube pública.

1. En la consola de Cyber Protect, vaya a **Infraestructura > Nubes públicas**.
2. Seleccione la conexión de la lista.
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.

4. Haga clic en **Eliminar** en el mensaje de confirmación que se muestra.

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 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 Bases de datos como archivos	Todo el equipo
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 previos

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:

- 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 o, de lo contrario, será imposible realizar una 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:

- El equipo virtual del que se va a realizar una copia de seguridad cumple los requisitos de copia de seguridad y restauración consistentes con la aplicación que aparecen en el artículo "Implementaciones de la copia de seguridad de Windows" de la documentación de VMware: https://code.vmware.com/docs/1674/virtual-disk-programming-guide/doc/vddkBkupVadp.9.6.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.
  - 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 AlwaysOn (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 AlwaysOn (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.

   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. 599), 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.
   - 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. 594).
   - 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. 599), 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 AlwaysOn (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.

Configuraciones de clúster compatibles

Este software de copia de seguridad es compatible *solo* con el grupo de disponibilidad AlwaysOn (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 `<nombre del AAG> - <nombre del plan de protección>` 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.

   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 AlwaysOn 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.

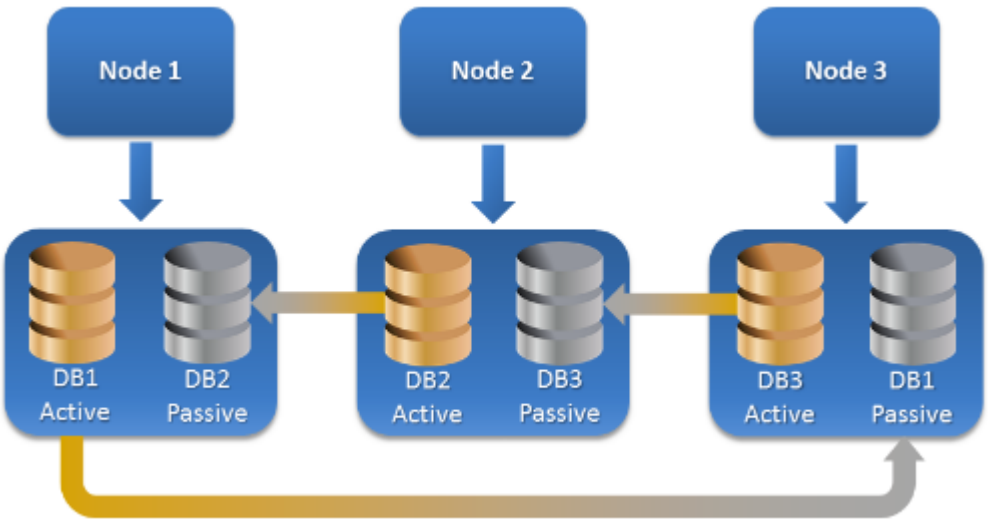
Copia de seguridad compatible con el clúster

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.

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. 591).
2. Configure la opción de copia de seguridad de "Modo de copia de seguridad de clústeres" (p. 477).
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**.

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** > `<nombre de clúster>` > `<nombre de nodo>` 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. 610), 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 a nivel de disco compatible con la aplicación está disponible para equipos físicos, equipos virtuales ESXi y equipos virtuales Hyper-V.

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.
- 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 un equipo virtual no es necesario instalar ningún agente; se presupone que Agent para VMware (Windows) o Agent para Hyper-V hacen una copia de seguridad del equipo.

Nota
Para las máquinas virtuales de Hyper-V y VMware ESXi que ejecutan Windows Server 2022, la copia de seguridad con información de aplicaciones no se admite en el modo sin agente, es decir, cuando la copia de seguridad la lleva a cabo el Agente para Hyper-V o el Agente para VMware, respectivamente. Para proteger las aplicaciones de Microsoft en estos equipos, instale el Agente para Windows dentro del sistema operativo invitado.

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 copias de seguridad** y, a continuación, seleccione este equipo en **Equipo desde el cual examinar**.

En las secciones "Requisitos previos" y "Derechos de usuario necesarios" se recogen otros requisitos.

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.

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:

  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`
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. 613). 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** > **Añadir**.
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.
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.

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. 586).

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. 609).

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. 604).
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.
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. 604).
3. Seleccione un punto de recuperación.

   Los puntos de recuperación se filtran por ubicación.
4. Haga clic en **Recuperar** > **Bases de datos SQL**.
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.

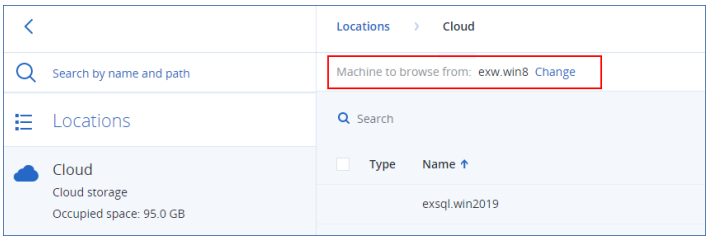
La versión de SQL Server en el equipo de destino debe ser la misma que la versión del equipo de origen o una más nueva.

Pasos para recuperar las bases de datos de SQL en un equipo que no sea original

Desde el almacenamiento de copias de seguridad

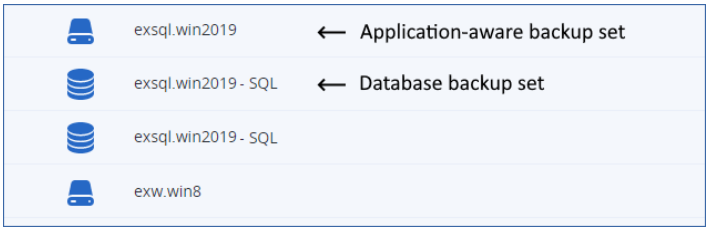
Este procedimiento se aplica a copias de seguridad con información de aplicaciones y copias de seguridad de bases de datos.

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:

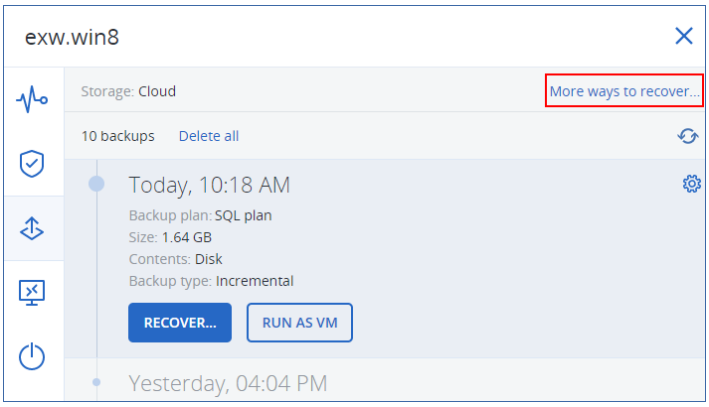
    ```
    C:\Program Files\Microsoft SQL Server\MSSQL16.MSSQLSERVER\MSSQL\DATA\
    ```

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**.

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. 610).

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.

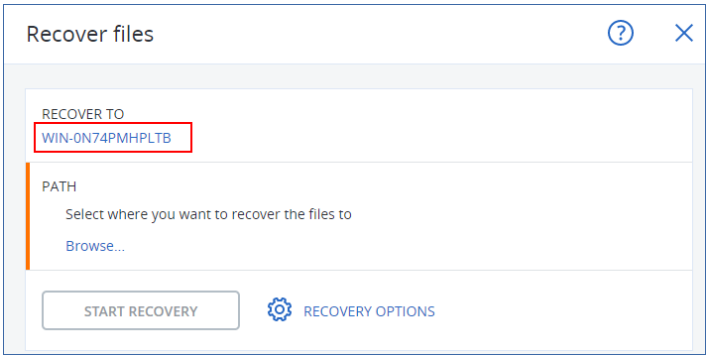
Nota
Si utiliza Agente para VMware (Windows), el único método de recuperación disponible será la recuperación de bases de datos como archivos. No se puede usar Agente para VMware (dispositivo virtual) para recuperar bases de datos.

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 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

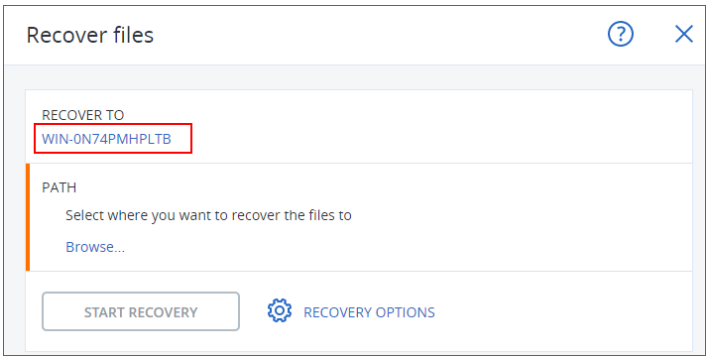
Este procedimiento se aplica a los equipos de origen en línea.

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**.



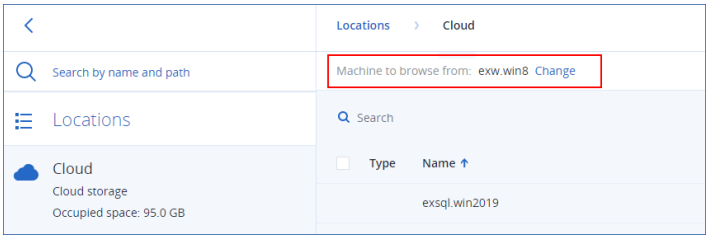
6. En **Ruta**, haga clic en **Examinar**, seleccione una carpeta local o de red en que guardar los archivos y, a continuación, haga clic en **Listo**.
7. Haga clic en **Iniciar recuperación**.

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.

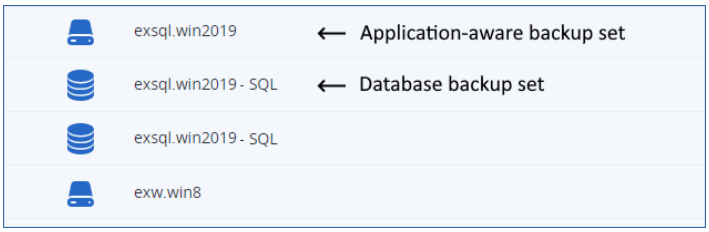
1. En la consola de Cyber Protect, vaya a **Almacenamiento de la copia de seguridad**.
2. Seleccione la ubicación del conjunto de copias de seguridad desde donde desea recuperar los datos.
3. En **Equipo desde el cual examinar**, seleccione el equipo de destino.

   Este es el equipo en el que se recuperarán los datos. El equipo de destino deben estar conectado.



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 **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.

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 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 en**.

   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.
   - 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

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 una base de datos
- 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. 591).

- 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.

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. 629).

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:
   - 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.
   - 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.

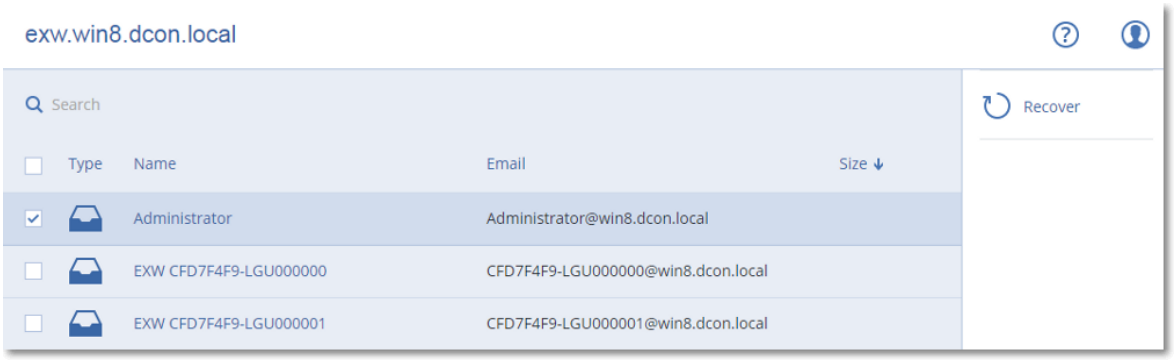
3. Haga clic en **Recuperación**.
4. Seleccione un punto de recuperación. Tenga en cuenta que los puntos de recuperación se filtran por ubicación.

   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.

   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.
9. Si se le pide, proporcione las credenciales de la cuenta que se utilizará para acceder al equipo.

Los requisitos de esta cuenta aparecen en la sección Derechos de usuario necesarios.

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**.

El proceso de recuperación se muestra 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.
   - 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.

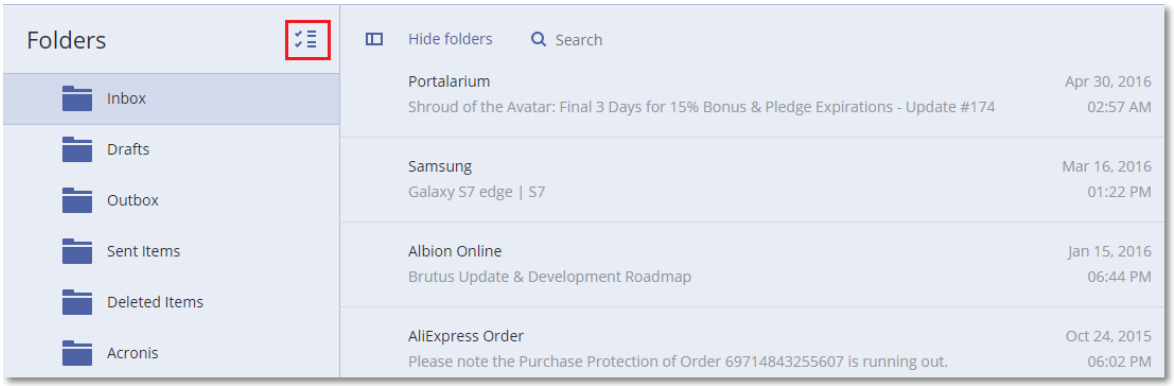
   Tiene a su disposición las siguientes opciones de búsqueda. No se pueden usar caracteres comodín.

   - 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.



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**.

[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.

10. Si se le pide, proporcione las credenciales de la cuenta que se utilizará para acceder al equipo. Los requisitos de esta cuenta aparecen en la sección Derechos de usuario necesarios.
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**.

El proceso de recuperación se muestra 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.

   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`
	`store.exe`
		`%ProgramFiles%\Microsoft\Exchange Server\V14\bin`

Microsoft Exchange Server 2013	`ese.dll`	`%ProgramFiles%\Microsoft\Exchange Server\V15\bin`
	`msvcr110.dll`	`%WINDIR%\system32`
Microsoft Exchange Server 2016 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 AlwaysOn, 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 de Cyber Protect le permite realizar una copia de seguridad de los datos de un dispositivo móvil en el Almacenamiento en la nube para que pueda recuperarlos en caso de pérdida o daños. Tenga en cuenta que el uso del almacenamiento en la nube requiere una cuenta y una suscripción a la nube.

Dispositivos móviles compatibles

Puede instalar la aplicación de Cyber Protect en cualquier dispositivo móvil que ejecute uno de los siguientes sistemas operativos:

- De iOS 14 a iOS 16 (iPhone, iPod y iPad)
- De Android 9 a Android 13

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)

- 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 **Copia de seguridad continua** se encuentra habilitada de forma predeterminada. Si se habilita esta configuración, la aplicación de Cyber Protect detectará de forma automática nuevos datos sobre la marca y los cargará a la nube.
- La opción **Usar Wi-Fi solamente** está habilitada de forma predeterminada en la configuración de la aplicación. Si se activa esta configuración, la aplicación de Cyber Protect realizará una copia de seguridad de los datos solo cuando se disponga de una conexión Wi-Fi. En el caso de perder la conexión, no se iniciará el proceso de copia de seguridad. Si quiere que la aplicación también pueda usar los datos móviles, desactive esta opción.
- La optimización de batería de su dispositivo podría impedir que la aplicación Cyber Protect funcione correctamente. Para ejecutar copias de seguridad en el momento preciso, deberá detener la optimización de batería para la aplicación.
- Existen dos métodos para ahorrar batería:
  - La función **Realizar cop. de seg. durante la carga**, que está deshabilitada de forma predeterminada. Si se activa esta configuración, la aplicación de Cyber Protect realizará una copia de seguridad de los datos solo cuando el dispositivo esté conectado a la corriente. En el caso de que el dispositivo se desconecte de la corriente durante un proceso de copia de seguridad continua, se pausará la copia de seguridad.
  - El **modo de ahorro de energía**, que está habilitado de forma predeterminada. Si se activa esta configuración, la aplicación de Cyber Protect realizará una copia de seguridad de los datos solo cuando el dispositivo tenga un nivel de batería adecuado. Cuando el nivel de batería sea bajo, se pausará la copia de seguridad continua.
- 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 de Cyber Protect solo puede recuperar la versión más reciente de los datos. Si necesita recuperar datos de una versión de copia de seguridad específica, use la consola de Cyber Protect en una tableta 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 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 mostrará si no tiene ninguna copia de seguridad en el 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:
   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 Cyber Protect.
2. Pulse **Examinar**.
3. Pulse el nombre del dispositivo.
4. Realice uno de los siguientes procedimientos:

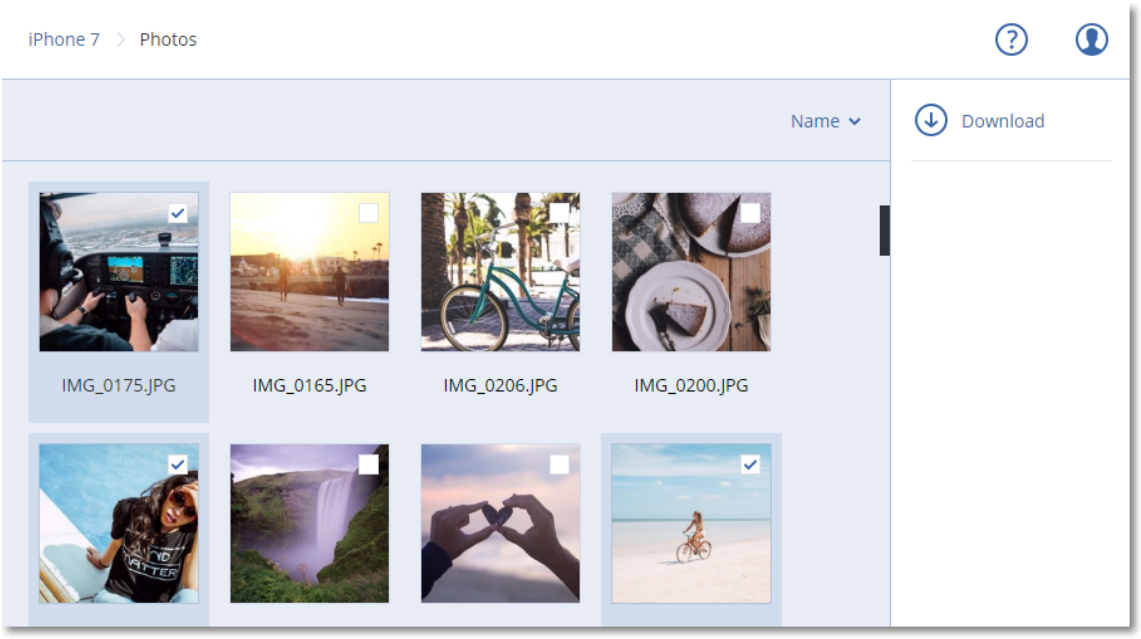
- Para recuperar todos los datos incluidos en la copia de seguridad, pulse **Recuperar todos**. No es necesario realizar más acciones.
- Para recuperar una o más categorías de datos, pulse **Seleccionar** y después seleccione las casillas de verificación de las categorías elegidas. Pulse **Recuperar**. 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 **Recupera** bajo el nombre de su dispositivo móvil.
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.

Protección de datos de Hosted Exchange

¿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. También puede llevar a cabo copias de seguridad de buzones de correo de archivos comprimidos (**archivo comprimido local**) de los buzones de correo seleccionados.

¿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
- Entradas del diario
- Notas

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.

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 Exchange Online

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 Exchange Online

1. Haga clic en **Dispositivos > Hosted Exchange**.
2. Si se añadieron varias organizaciones de Hosted Exchange 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 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 de usuarios individuales o de los compartidos, amplíe el nodo **Usuarios**, seleccione **Todos los usuarios**, elija los usuarios cuyos buzones de correo quiera recuperar 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 crearan en el futuro), amplíe el nodo **Grupos**, seleccione **Todos los grupos** y haga clic en **Agrupar copia de seguridad**.
   - Para realizar una copia de seguridad de los buzones de correo de grupos individuales, amplíe el nodo **Grupos**, seleccione **Todos los grupos**, elija los grupos de cuyos buzones de correo quiera realizar una copia de seguridad y 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 **Dispositivos > Hosted Exchange**.
2. Si se añadieron varias organizaciones de Hosted Exchange 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.
5. Haga clic en **Recuperar** > **Todo el buzón de correo**.
6. Si se han añadido varias organizaciones de Hosted Exchange al servicio Cyber Protection, haga clic en **la organización de Hosted Exchange** 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.
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 **Dispositivos > Hosted Exchange**.
2. Si se añadieron varias organizaciones de Hosted Exchange 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.
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.
   - 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 Hosted Exchange al servicio Cyber Protection, haga clic en **la organización de Hosted Exchange** 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.
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.

Protección de los datos de Microsoft 365

Motivos por los que hacer una copia de seguridad de los datos de Microsoft 365

Si bien Microsoft 365 es un conjunto de servicios en la nube, las copias de seguridad periódicas 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 el periodo de retención de Microsoft 365 haya caducado. Asimismo, puede conservar una copia local de los buzones de correo de Exchange Online si es necesario para cumplir la normativa.

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. 479).

Agente en la nube y agente local

Para las cargas de trabajo de Microsoft 365, hay dos agentes disponibles:

- Agente en la nube

  El agente de la nube proporciona funciones ampliadas de copias de seguridad, a las que se puede acceder directamente desde la consola Cyber Protect. No requiere instalación. Para obtener más información, consulte "Uso del agente en la nube para Microsoft 365" (p. 640).
- Agente local

  El agente local solo permite realizar copias de seguridad de los buzones de correo de Exchange en línea. Este agente debe instalarse en un equipo Windows que esté conectado a internet. Para obtener más información, consulte "Usar el agente instalado localmente para Office 365." (p. 635).

Azure Information Protection (AIP) es compatible con ambos agentes.

Nota
Para los inquilinos en el modo de seguridad mejorada, solo está disponible el agente 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.

La siguiente tabla resume la funcionalidad de los agentes.

	Agente local	Agente en la nube
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)	• **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**: ◦ colecciones de sitios clásicos ◦ sitios de grupo (equipo) ◦ sitios de comunicación ◦ sitios de datos individuales • **Microsoft 365 Teams**: ◦ todos los equipos ◦ canales del equipo ◦ archivos del canal ◦ buzones de correo del

	Agente local	Agente en la nube
		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**)	No	Sí
Programación de copia de seguridad	Definida por el usuario	Hasta seis veces al día*
Ubicaciones de las copias de seguridad	Almacenamiento en la nube, o bien la carpeta local o de red	Solo Almacenamiento en el cloud (incluido el almacenamiento alojado en partners)
Protección automática de sitios, grupos, usuarios y equipos de Microsoft 365	No	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**
Protección de más de una organización de Microsoft 365	No	Sí
Recuperación granular	Sí	Sí
Recuperación en otro usuario de la organización	Sí	Sí
Recuperación en otra organización	No	Sí
Recuperación en un servidor de Microsoft Exchange local	No	No
Número máximo de elementos que se pueden incluir en copias de seguridad sin que se produzca ninguna	Al realizar copias de seguridad en el almacenamiento en la nube: 5000 buzones de correo por empresa	10 000 elementos protegidos (buzones de correo, elementos de OneDrive o sitios) por empresa**

	Agente local	Agente en la nube
degradación del rendimiento	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	No	10 ejecuciones manuales durante una hora
Cantidad máxima de operación de recuperación simultáneas	No	10 operaciones, incluidas operaciones de recuperación de Google Workspace

* La opción predeterminada es **Una vez por día**. Con el paquete de Advanced Backup. 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 https://docs.microsoft.com/en-us/graph/throttling.

** Le recomendamos que haga copias de seguridad de sus elementos protegidos de manera gradual y en este orden:

1. Buzones de correo.
2. Cuando se haya realizado la copia de seguridad de todos los buzones de correo, haga la de los elementos de OneDrive.
3. Cuando se haya realizado la copia de seguridad de los elementos de OneDrive, haga la de los sitios de SharePoint Online.

La primera copia de seguridad completa puede tardar varios días en función del número de elementos protegidos y el tamaño.

Derechos de usuario necesarios

En Cyber Protection

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.

El agente en la nube puede utilizarse tanto a nivel de inquilino del 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. 641).

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 Cyber Protect, como se describe en "Cambio de las credenciales de acceso de Microsoft 365" (p. 637).
- El agente en la nube no inicia sesión en Microsoft 365. Primero debe iniciar sesión en Microsoft 365 como administrador global para conceder al agente en la nube los permisos necesarios para su funcionamiento.

  Se requieren los siguientes permisos en Microsoft 365:
  - Iniciar sesión y leer los perfiles 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
  - Leer y escribir elementos y listas en todas las recopilaciones de sitios
  - Tener control total de todas las recopilaciones de sitios
  - Leer y escribir elementos en todas las colecciones de sitios
  - Utilizar Exchange Web Services con acceso completo a todos los buzones de correo
- 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.

Limitaciones

- Con el agente local, puede proteger hasta 5000 cargas de trabajo. Con el agente en la nube, puede proteger hasta 50 000 cargas de trabajo.
- La consola de Cyber Protect muestra todos los usuarios con un buzón de correo o 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.
- No puede aplicar más de un plan de copias de seguridad individual a la misma carga de trabajo.
- Cuando se aplican un plan de copias de seguridad individual y un plan de copias de seguridad en grupo a la misma carga de trabajo, la configuración del plan individual tiene prioridad.

Informe de licencia de usuarios de Microsoft 365

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 carga de trabajo protegida.

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

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**.

Iniciando sesión

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 pueden infringir la privacidad del usuario. Estas acciones se registran en **Supervisión** > **Registro de auditoría** en el Portal de administración.

Usar el agente instalado localmente 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 (Agente local)**.
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. 635) para obtener más información sobre cómo obtenerlos.
6. Haga clic en **Aceptar**.

Como resultado, los elementos de datos de su organización aparecen en la consola de Cyber Protect, en la pestaña **Microsoft Office 365 (Agente local)**.

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

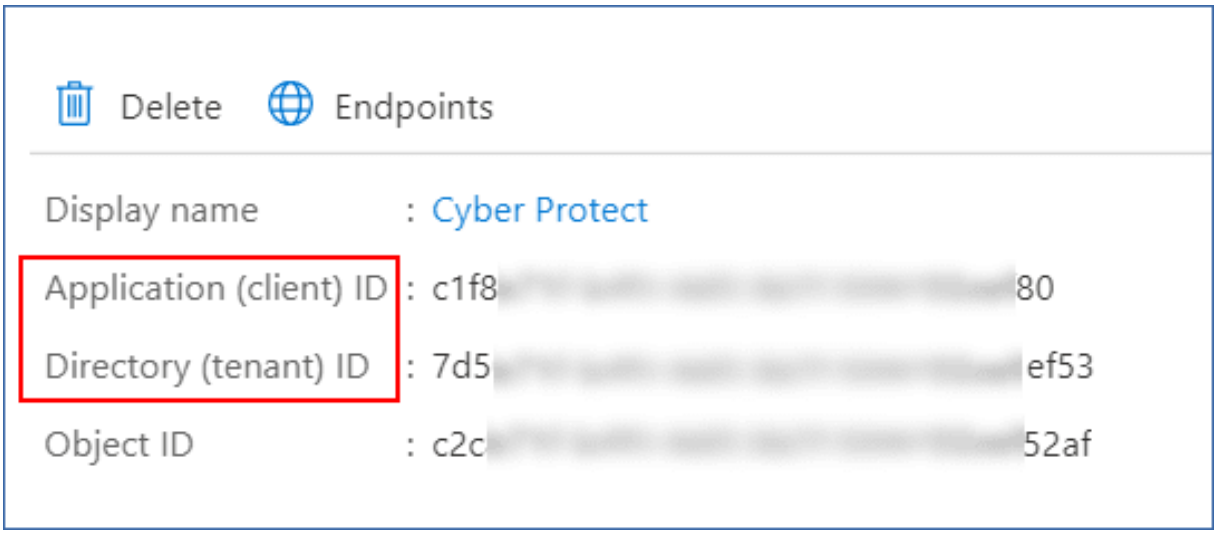
Para utilizar la autenticación moderna para Office 365, debe crear una aplicación personalizada en el centro de administración de Entra y otorgarle permisos específicos para la API. Así, obtendrá el **ID de la aplicación**, el **secreto de la aplicación** y el **ID del directorio (inquilino)** que necesita para entrar en la Cyber Protect consola.

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**.

Su aplicación ya está creada. En el centro de administración de Entra, navegue hasta la página de **Resumen** de la aplicación y verifique su ID de aplicación (cliente) y su ID de directorio (inquilino).



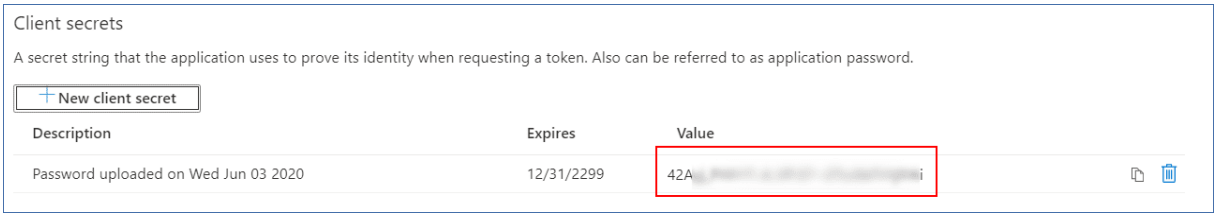
Para obtener más información sobre cómo crear una aplicación en el centro de administración de Entra, consulte la Documentación de Microsoft.

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 <nombre de su aplicación>**.
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 **Añadir**.
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 (Agente local)**.
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. 635) 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
- 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 (agente local)**.
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 (agente local)**.
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**.

Recuperación de elementos de buzón de correo

1. Haga clic en **Microsoft Office 365 (agente local)**.
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.

Uso del agente en la nube para Microsoft 365

Cómo añadir una organización de Microsoft 365

Un administrador puede añadir una o más organizaciones de Microsoft 365 a un inquilino de cliente o a una unidad.

Los administradores de empresa añaden organizaciones a los inquilinos de cliente. Los administradores de la unidad y de cliente que actúan en el nivel de la unidad añaden organizaciones a unidades.

Para añadir una organización de Microsoft 365

1. Según dónde necesite añadir la organización, inicie sesión en la consola de Cyber Protect como administrador de la empresa o de la unidad.
2. [Para los administradores de empresa que actúan en el nivel de la unidad] En el portal de administración, vaya a la unidad que desee.
3. Haga clic en **Dispositivos** > **Añadir** > **Microsoft 365 Business**.
   El software le redirige a la página de inicio de sesión de Microsoft 365.
4. Inicie sesión con las credenciales del 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.
5. Confirme que concede estos permisos al servicio Cyber Protection.

Como resultado, su organización de Microsoft 365 aparecerá en la pestaña **Dispositivos** de la consola de Cyber Protect.

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, seleccione la organización en la página de **Microsoft 365** y, a continuación, haga clic en **Actualizar**.
  Para obtener más información sobre la sincronización de los recursos de una organización de Microsoft 365 y la consola de Cyber Protect, consulte "Detección de recursos de Microsoft 365" (p. 642).
- Si aplica un plan de protección a los grupos **Todos los usuarios**, **Todos los grupos** o **Todos los sitios**, los elementos añadidos recientemente 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. 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**.

Administración de organizaciones de Microsoft 365 añadidas en diferentes niveles

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 protección 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.

Cómo eliminar una organización de Microsoft 365

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.

Consulte "Para eliminar copias de seguridad o archivos de copia de seguridad" (p. 559) para obtener más información sobre cómo eliminar copias de seguridad.

Para eliminar una organización de Microsoft 365

1. Según dónde se añada la organización, inicie sesión en la consola de Cyber Protect como administrador de la empresa o de la unidad.
2. [Para los administradores de empresa que actúan en el nivel de la unidad] En el portal de administración, vaya a la unidad que desee.
3. Vaya a **Dispositivos** > **Microsoft 365.**
4. Seleccione la organización y haga clic en **Eliminar grupo**.

Como resultado, se revocarán los planes de copias de seguridad aplicados a este grupo.

Sin embargo, también deberá revocar de forma manual los derechos de acceso de la aplicación Servicio de copias de seguridad a los datos de la organización de Microsoft 365.

Para revocar derechos de acceso

1. Inicie sesión en Microsoft 365 como administrador global.
2. Vaya a **Admin Center** > **Azure Active Directory** > **Aplicaciones Enterprise** > **Todas las aplicaciones**.
3. Seleccione la aplicación **Servicio de copias de seguridad** y entre en sus detalles.
4. Vaya a la pestaña **Propiedades** y, en el panel de acción, haga clic en **Eliminar**.
5. Confirme la operación de eliminación.

Como resultado, se revocarán los derechos de acceso de la aplicación Servicio de copias de seguridad a los datos de la organización de Microsoft 365.

Detección de recursos de Microsoft 365

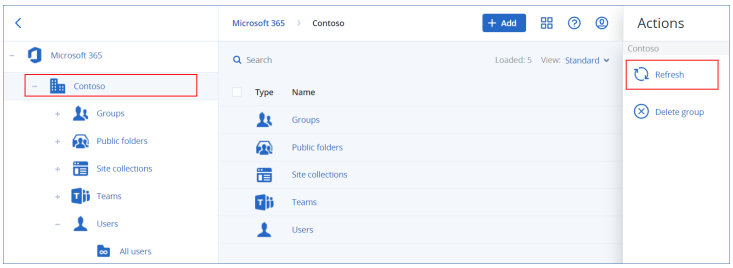
Cuando añade una organización de Microsoft 365 al servicio de Cyber Protection, los recursos de esta organización, como los buzones de correo, los almacenamientos de OneDrive, Microsoft Teams y los sitios de SharePoint, se sincronizan con la consola de Cyber Protect. Esta operación se llama detección y se registra en **Supervisión** > **Actividades**.

Cuando se complete la operación de detección, verá los recursos de la organización de Microsoft 365 en la pestaña **Dispositivos** > **Microsoft 365** 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** > **Microsoft 365**.
2. Seleccione su 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.

Configuración de la frecuencia de las copias de seguridad de Microsoft 365

Por defecto, las copias de seguridad de Microsoft 365 se ejecutan una vez al día y no hay otras opciones de programación disponibles.

Si el paquete de Advanced Backup está habilitado en su inquilino, puede configurar copias de seguridad con mayor frecuencia. 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 por día	24 horas
Dos veces al día (por defecto)	12 horas
Tres veces al día	8 horas
Seis veces al día	4 horas

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.

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 la versión 8.0 del servicio Cyber Protection, es posible realizar copias de seguridad de carpetas públicas. Si se agregó su organización al servicio Cyber Protection antes de la publicación de la versión 8.0, debe volver a agregar la organización para obtener esta funcionalidad. No elimine la organización, simplemente repita los pasos descritos en "Cómo añadir una organización de Microsoft 365" (p. 640). Como resultado, el servicio Cyber Protection obtiene permiso para usar la API correspondiente.

¿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
- 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 tal como se describe a continuación y luego especifique otros ajustes del plan de protección según corresponda.

Pasos para seleccionar buzones de correo de Exchange 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:
   - 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 de usuarios individuales o de los compartidos, amplíe el nodo **Usuarios**, seleccione **Todos los usuarios**, elija los usuarios cuyos buzones de correo quiera recuperar 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 crearan en el futuro), amplíe el nodo **Grupos**, seleccione **Todos los grupos** y haga clic en **Agrupar copia de seguridad**.
   - Para realizar una copia de seguridad de los buzones de correo de grupos individuales, amplíe el nodo **Grupos**, seleccione **Todos los grupos**, elija los grupos de cuyos buzones de correo quiera realizar una copia de seguridad y haga clic en **Copia de seguridad**.

     Nota
     El agente para Microsoft 365 en la nube utiliza una cuenta con los derechos apropiados para acceder al buzón de correo del grupo. Por lo tanto, para realizar una copia de seguridad del buzón de correo de un grupo, como mínimo uno de los propietarios del grupo debe tener la licencia de usuario de Microsoft 365 con un buzón de correo. Si el grupo es privado o tiene miembros ocultos, el propietario tiene que ser también miembro del grupo.

4. En el panel del plan de protección:
   - Asegúrese de que el elemento **Buzones de correo de Microsoft 365** esté seleccionado en **Qué incorporar en la copia de seguridad**.

     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.
   - Si no quiere incluir los buzones de correo comprimidos en la copia de seguridad, deshabilite el conmutador **Buzones de correo comprimidos**.

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 panel del plan de protección, asegúrese de que el elemento **Buzones de correo de Microsoft 365** esté seleccionado en **Qué incorporar en la copia de seguridad**.

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 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.

   - 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.
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
El archivo comprimido local no se puede ser restaurar como parte de la recuperación en forma de archivos PST. Para restaurar el archivo comprimido local junto con el buzón, consulte "Recuperación de buzones de correo" (p. 646).

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**.
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 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 copias 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.

Recuperación de elementos del buzón de correo en archivos PST

Nota
El archivo comprimido local no se puede ser restaurar como parte de la recuperación en forma de archivos PST. Para restaurar el archivo comprimido local junto con el buzón, consulte "Recuperación de buzones de correo" (p. 646).

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.

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 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 copias 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.

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:

   - Cuando un mensaje de correo electrónico o una 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	Todos los archivos existentes en la ubicación de destino se sobrescribirán.

Opción	Descripción
elementos existentes	
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.

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

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 panel del plan de protección:
   - Asegúrese de que el elemento **OneDrive** esté seleccionado en **Qué incorporar en la copia de seguridad**.

     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 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 un solo usuario.
   - [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, es decir, si especifica el mismo archivo en los dos campos, este archivo se omitirá durante el proceso de realización de la copia de seguridad.

- [Opcional] Para hacer copias de seguridad de los 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:

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

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.

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 colecciones de sitios clásicos de SharePoint, sitios de grupo (equipo moderno) y sitios de comunicación. Además, es posible elegir subsitios, listas y bibliotecas individuales para incluirlos en la copia de seguridad.

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.
- 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:
   - 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**.
- 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**.

4. En el panel del plan de protección:
   - Asegúrese de que el elemento de los **Sitios de SharePoint** esté seleccionado en **Qué incorporar en la copia de seguridad**.
   - 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/**`

       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.
   - [Opcional] Para hacer copias de seguridad de los 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.

   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.
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 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.

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?

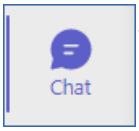
- Todo el equipo
- Canales del equipo
- Archivos del canal

- 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 Teams

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.
- 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 panel del plan de protección:
   - Asegúrese de que el elemento **Microsoft Teams** esté seleccionado en **Qué incorporar en la copia de seguridad**.
   - [Opcional] En **Cuánto tiempo se conservarán**, establezca las opciones de limpieza.
   - [Opcional] Si desea cifrar su copia de seguridad, active el conmutador **Cifrado** y, a continuación, establezca su contraseña y seleccione el algoritmo de cifrado.
   - [Opcional] Para hacer copias de seguridad de los 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.

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: `<Nombre del equipo>_<Nombre del canal>_conversations_backup_<fecha de recuperación>T<hora de recuperación>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.
   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: `<Nombre del equipo>_<Nombre del canal>_conversations_backup_<fecha de recuperación>T<hora de recuperación>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.
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

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

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 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 copias 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.
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.
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. 657) o "Recuperación de archivos de OneDrive" (p. 658).
- Para copias de seguridad de Teams, consulte "Recuperación de un equipo completo" (p. 666), "Cómo recuperar canales de equipo o archivos de canales de equipo" (p. 667) o "Recuperación de un sitio de equipo o de elementos específicos de un sitio" (p. 673).
- Para copias de seguridad del sitio de SharePoint, consulte "Recuperación de datos de SharePoint Online" (p. 663).

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/<Nombre del equipo>/SiteAssets/<Nombre del bloc de notas de OneNote>"*.

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
- 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.

Protección de los datos de Google Workspace

Nota
Esta función no está disponible para los inquilinos en el modo de Cumplimiento. Para obtener más información, consulte "Modo de cumplimiento normativo" (p. 1149).

¿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. 479).

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**).

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. 678) 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.

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.

La opción predeterminada es **Una vez por día**. Con el paquete de Advanced Backup. 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 muestra solo usuarios que tienen asignada una licencia de Google Workspace y un buzón de correo o Google Drive.
- 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 Cyber Protect, como .docx o .pptx, por ejemplo. Los documentos se convierten de nuevo a su formato original durante la recuperación.
- No se pueden realizar más de 10 ejecuciones de copias de seguridad manuales durante una hora.
- No se pueden realizar más de 10 operaciones de recuperación simultáneas (esto incluye tanto la recuperación de Google Workspace como de Microsoft 365).
- No puede recuperar elementos de diferentes puntos de recuperación de forma simultánea, incluso aunque pueda seleccionar esos elementos en los resultados de búsqueda.
- 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.
- No puede aplicar más de un plan de copias de seguridad individual a la misma carga de trabajo.
- Cuando se aplican un plan de copias de seguridad individual y un plan de copias de seguridad en grupo a la misma carga de trabajo, la configuración del plan individual tiene prioridad.

Iniciando sesión

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 pueden 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. 679).

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** > **Añadir** > **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.

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. 683).
- 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

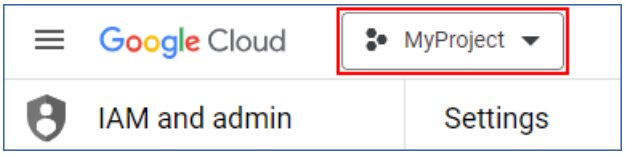
Para añadir su organización de Google Workspace al servicio Cyber Protection mediante un proyecto especializado de Google Cloud, haga lo siguiente:

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

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**.
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**.
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. 678).

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**.
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

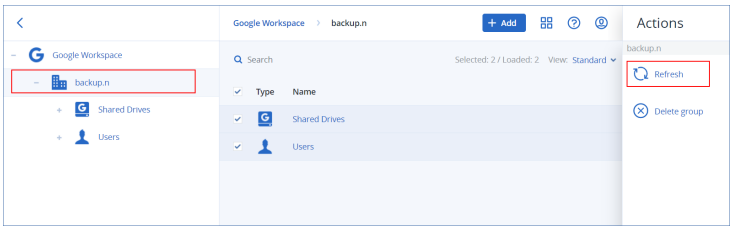
Cuando añade una organización de Google Workspace al servicio de Cyber Protection, los recursos de esta organización, como los buzones de correo y Google Drive, se sincronizan con la consola de Cyber Protect. Esta operación se llama detección y se registra en **Supervisión** > **Actividades**.

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 de Advanced Backup está habilitado en su inquilino, puede configurar copias de seguridad con mayor frecuencia. 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 por día	24 horas
Dos veces al día (por defecto)	12 horas
Tres veces al día	8 horas
Seis veces al día	4 horas

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.

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

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 panel del plan de protección:
   - Asegúrese de que el elemento **Gmail** esté seleccionado en **Qué incorporar en la copia de seguridad**.
   - Si quiere realizar una copia de seguridad de los calendarios que se comparten con los usuarios seleccionados, habilite el conmutador **Incluir calendarios compartidos**.
   - Decida si necesita la búsqueda en todo el texto en la copia de seguridad de los mensajes de correo electrónico. Para acceder a esta opción, haga clic en el ícono de engranaje > **Opciones de copia de seguridad** > **Búsqueda en todo el texto**.

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**.

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.

   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 de texto completo** 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.

    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.

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 panel del plan de protección:
   - Asegúrese de que el elemento **Google Drive** esté seleccionado en **Qué incorporar en la copia de seguridad**.
   - 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 un solo usuario.

- [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, es decir, si especifica el mismo archivo en los dos campos, este archivo se omitirá durante el proceso de realización de la copia de seguridad.
- Si quiere habilitar la notarización de todos los archivos seleccionados para realizar una copia de seguridad, habilite el conmutador **Notarización**. Para obtener más información sobre la notarización, consulte "Notarización".

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**.

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.

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,

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:

- 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 panel del plan de protección:
   - 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.

- [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, es decir, si especifica el mismo archivo en los dos campos, este archivo se omitirá durante el proceso de realización de la copia de seguridad.
- Si quiere habilitar la notarización de todos los archivos seleccionados para realizar una copia de seguridad, habilite el conmutador **Notarización**. Para obtener más información sobre la notarización, consulte "Notarización".

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.
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**.
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.

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.
   - 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.

En las copias de seguridad no cifradas, la búsqueda siempre está disponible. Solo se soporta la búsqueda mejorada (basada en índice).

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.

En las copias de seguridad cifradas, también puede habilitar la búsqueda mejorada (basada en índices). 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 todas las demás cargas de trabajo, la búsqueda no estará disponible.

La tabla a continuación resume las opciones disponibles para 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
	Mensajes de correo electrónico	La búsqueda básica (no basada en índice) está disponible	La búsqueda mejorada (basada en índice) está disponible
	Sitio de Teams	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	Archivos/carpetas	La búsqueda no está disponible	La búsqueda mejorada (basada

Tipo de carga de trabajo	Qué recuperar	La búsqueda mejorada está desactivada	La búsqueda mejorada está habilitada
compartidas			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 ocupado por 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 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 **Copia de seguridad y almacenamiento**, 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
Recomendamos que se ponga en contacto con el equipo de Soporte antes de actualizar, reconstruir o eliminar un índice.

Para actualizar, reconstruir o eliminar un índice

1. Inicie sesión como administrador en la consola de Cyber Protect.
2. En la pestaña **Copia de seguridad y almacenamiento**, haga clic en **Copia de seguridad de aplicaciones en la nube**.
   Seleccione el archivo comprimido cuyo índice desea actualizar, reconstruir o eliminar.
   La disponibilidad de estas acciones depende del nivel y rol del administrador, como sigue:

Nivel de cuota	Rol	Puede actualizar índices	Puede reconstruir índices	Puede eliminar índices
Inquilino de partner	Administrador de la compañía	+	+	+
	Administrador de ciberprotección	+	-	-
	Administrador de protección	+	-	-
	Administrador de protección (de) solo lectura	-	-	-
Inquilino de cliente	Administrador de la compañía	+	-	-
	Administrador de protección	+	-	-
	Administrador de protección (de) solo lectura	-	-	-
Unidad	Administrador de la unidad	+	-	-
	Administrador de protección	+	-	-
	Administrador de protección (de) solo lectura	-	-	-

3. 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.

4. [Para archivos cifrados] Especifique la contraseña de cifrado y luego haga clic en **OK**.
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

Al crear un plan de copias de seguridad para la copia de seguridad de la nube a la nube cifrada, puede habilitar una búsqueda mejorada (basada en índice).

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. 700).

Nota
Esta funcionalidad está disponible en una selección de centros de datos y puede que no sea accesible para todos los clientes.

Para habilitar la búsqueda en copias de seguridad cifradas

1. Al crear un plan de copias de seguridad, habilite el interruptor **Cifrado**.
2. Especifique y confirme la contraseña de cifrado.
3. Seleccione la casilla de verificación **Permitir búsqueda mejorada en copias de seguridad cifradas**.
4. Haga clic en **Listo**.

Nota
No puede deshabilitar el cifrado ni cambiar la contraseña de cifrado más tarde. Para crear una copia de seguridad sin cifrado o cambiar la contraseña de cifrado, cree un plan de copias de seguridad.

Habilitar o deshabilitar la búsqueda mejorada en planes existentes

Puede editar un plan existente para la copia de seguridad cifrada para habilitar o deshabilitar la búsqueda mejorada (basada en índices).

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. 700).

En las copias de seguridad no cifradas, la búsqueda mejorada siempre está disponible. Esta opción no se puede desactivar.

Para habilitar o deshabilitar la búsqueda mejorada en copias de seguridad cifradas

1. Al editar un plan de copias de seguridad en el que el cifrado está habilitado, haga clic en el icono de engranaje en la esquina superior derecha.
2. En la pestaña **Opciones de búsqueda**, cambie el interruptor según sea necesario.
3. Haga clic en **Listo**.
4. Haga clic en **Guardar configuración**.

Nota
Si vuelve a habilitar la búsqueda mejorada, todos los archivos comprimidos creados por este plan de copias de seguridad se indexarán de nuevo. Esta es una operación que consume mucho tiempo.

Deshabilitar la búsqueda de texto completo para las copias de seguridad de Gmail

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.

Es posible que quiera deshabilitar la búsqueda de texto completo si necesita mantener el tamaño del índice de búsqueda al mínimo.

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 de texto completo**, 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**.

Nota
Si 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.

Protección de Oracle Database

Nota
Esta función está disponible con el paquete Advanced Backup.

La protección de Oracle Database 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 Copia de seguridad avanzada.

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 lo tanto solo puede instalarse en sistemas operativos basados en Linux de 64 bits. Consulte "Sistemas operativos y entornos compatibles" (p. 23).

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. 82) o "Instalación o desinstalación sin supervisión en Linux" (p. 108). 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.

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.
   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 (`*.*`)
      - `SELECCIONAR` 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

* 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 "Recuperar un equipo" (p. 522).

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**.
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.
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`
   - 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 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.
   ```

¿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 **Administración** > **Planes de protección**.

Copia de seguridad de un sitio web

Cómo añadir un sitio web

1. Haga clic en **Dispositivos** > **Añadir**.
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.

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.

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 copias 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

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.

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.

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.

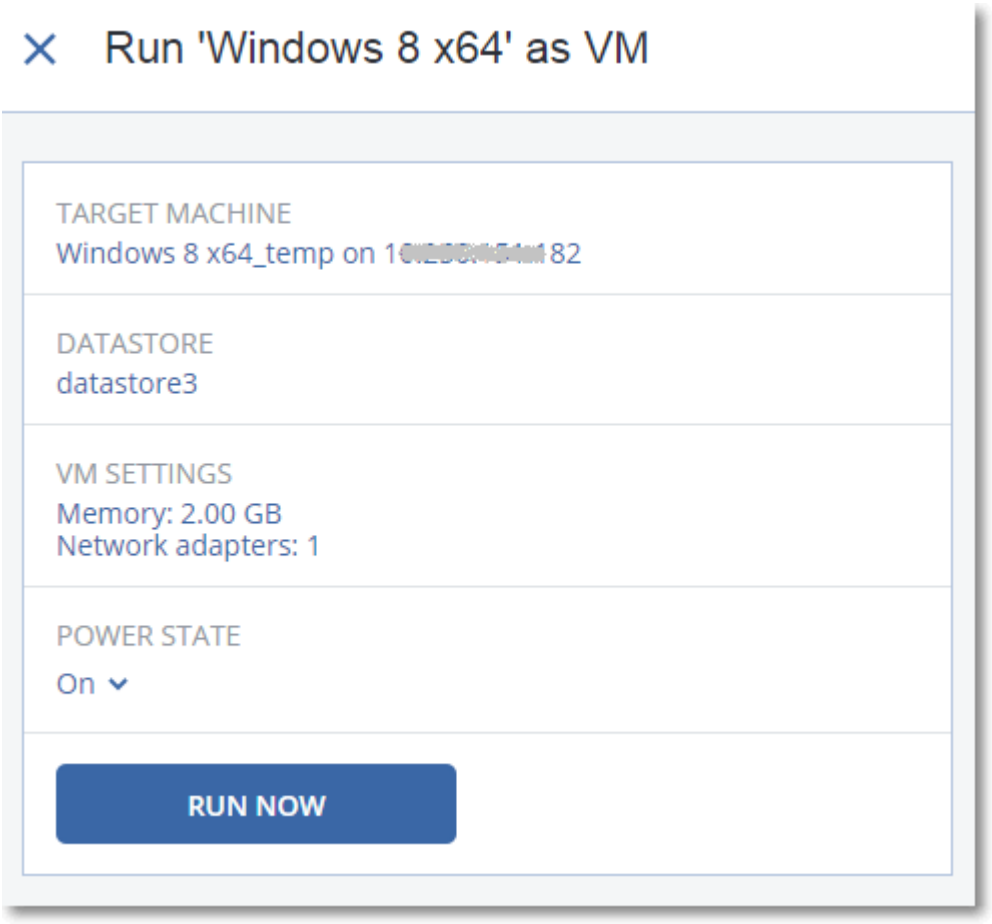
Requisitos previos

- 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.

   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.

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 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. 140). 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 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**.

   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 ícono 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

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.

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**.

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.

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.

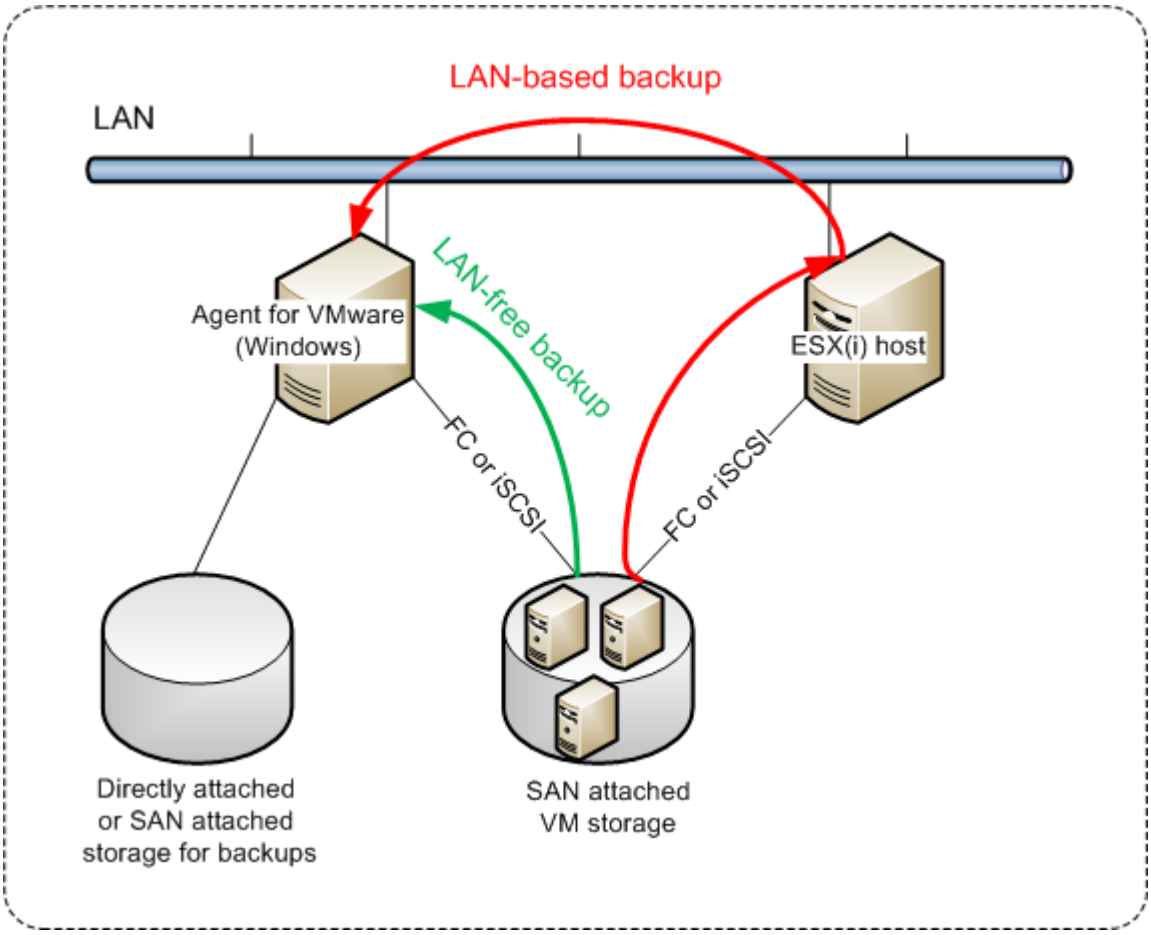
4. Exporte los archivos del equipo virtual (o de la réplica) a un disco duro externo.
   a. Conecte el disco duro externo al equipo donde se ejecuta vSphere Client.
   b. Conecte vSphere Client al vCenter\ESXi original.
   c. Seleccione la réplica recién creada en el inventario.
   d. Haga clic en **Archivo** > **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 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.

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.

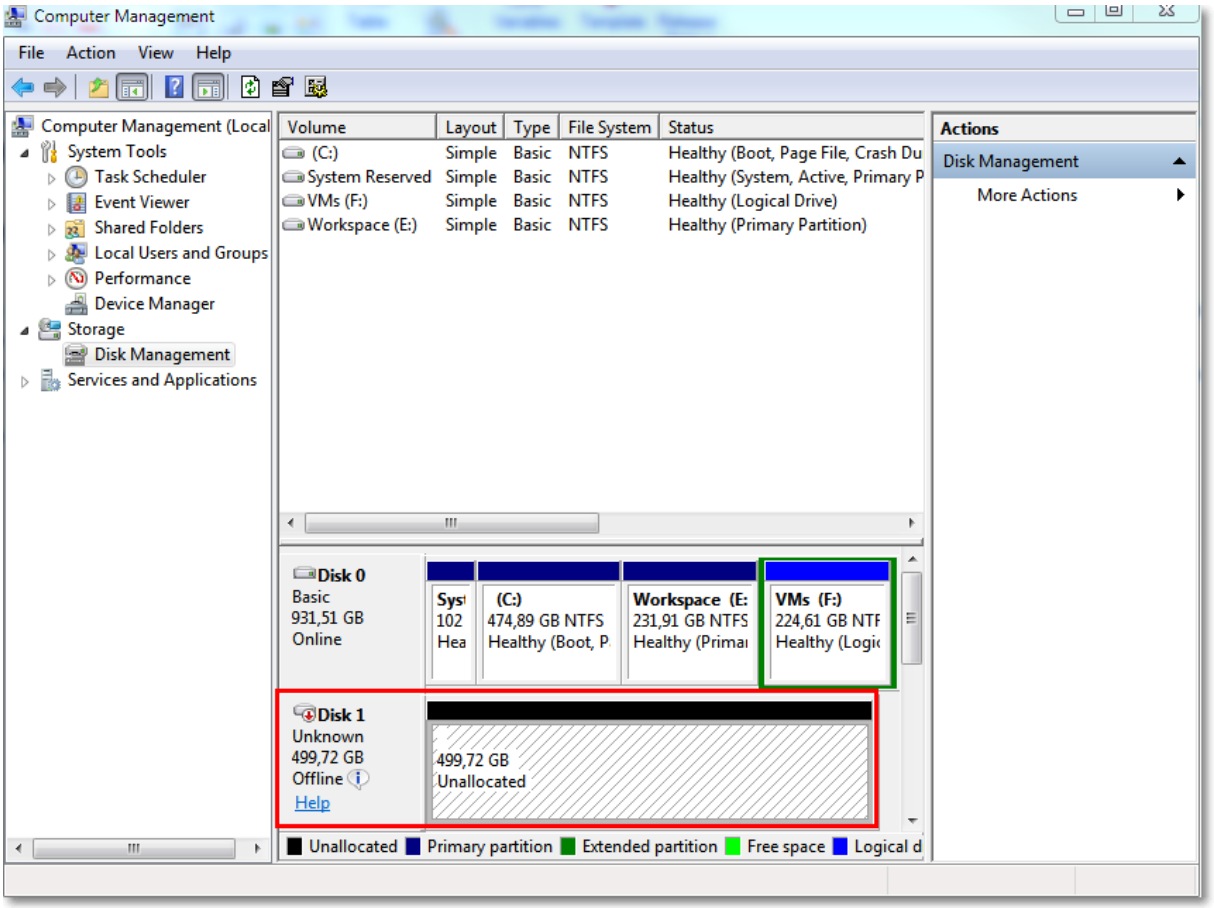
Para configurar un iniciador iSCSI

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**.
   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 un almacenamiento conectado localmente

Puede conectar un disco adicional a Agent for VMware (Virtual Appliance) para que el agente pueda realizar la copia de seguridad en este almacenamiento conectado localmente. Este enfoque elimina el tráfico de red entre el agente y la ubicación de copia de seguridad.

Un dispositivo virtual que se ejecute en el mismo servidor o clúster que los equipos virtuales de los que se ha realizado la copia de seguridad tiene acceso directo a los almacenes de datos donde residan los equipos. Esto significa que el dispositivo puede adjuntar los discos de los que se ha realizado la copia de seguridad mediante el transporte HotAdd y, por tanto, la transferencia de datos de la copia de seguridad se dirige desde un disco local a otro. Si el almacén de datos está conectado como **Disco/LUN** en lugar de **NFS**, la copia de seguridad no dependerá en ningún momento de LAN. En el caso de un almacén de datos NFS, habrá tráfico de red entre el almacén de datos y el servidor.

Utilizar un almacenamiento conectado localmente presume que el agente siempre realiza la copia de seguridad de los mismos equipos. Si múltiples agentes trabajan con vSphere y uno o más de ellos utiliza almacenamientos conectados localmente, necesita enlazar manualmente cada agente a los equipos de los que tiene que realizar la copia de seguridad. De lo contrario, si el servidor de gestión redistribuye los equipos entre los agentes, las copias de seguridad de un equipo pueden dispersarse en varios almacenamientos.

Puede añadir el almacenamiento a un agente ya en funcionamiento o cuando implemente el agente desde una plantilla OVF.

Para conectar un almacenamiento a un agente que ya está trabajando

1. En el inventario de VMware vSphere, haga clic con el botón derecho en Agent for VMware (Virtual Appliance).
2. Añada el disco al editar los ajustes del equipo virtual. El tamaño del disco deben ser de al menos 10 GB.

   Advertencia.
   Tenga cuidado al añadir un disco ya existente. Una vez creado el almacenamiento, todos los datos incluidos previamente en este disco se perderán.

3. Vaya a la consola del dispositivo virtual. El enlace **Crear almacenamiento** estará disponible en la parte inferior de la pantalla. Si no lo está, haga clic en **Actualizar**.
4. Haga clic en el enlace **Crear almacenamiento**, seleccione el disco y especifique una etiqueta para el mismo. La longitud de la etiqueta está limitada a 16 caracteres debido a las restricciones del sistema de archivos.

Para seleccionar un almacenamiento conectado localmente como el destino de la copia de seguridad

- Al crear un plan de protección, en **Dónde realizar copias de seguridad**, seleccione **Carpetas locales** y, a continuación, escriba la letra correspondiente al almacenamiento conectado localmente, por ejemplo, **D:**.

Nota
El almacenamiento con conexión local (LAS, por sus siglas en inglés) está diseñado para entornos relativamente pequeños con un único agente (dispositivo virtual). Hemos probado unidades de almacenamiento con conexión local de hasta 5 TB de tamaño. Puede conectar discos más grandes bajo su propia responsabilidad, pero estas configuraciones no son compatibles. Para más de 5 TB de datos de copia de seguridad, le recomendamos que utilice otros tipos de almacenamiento. Por ejemplo, puede crear y adjuntar un disco virtual VMware a cualquier máquina virtual aleatoria y crear un recurso compartido de red en él, que luego se utilizará como destino de la copia de seguridad en lugar de un LAS.

Enlace de equipos virtuales

Esta sección le proporciona información general sobre cómo el servicio de Cyber Protection organiza la operación de múltiples agentes en 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.

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 **Cambiar**.
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 **Cambiar**.
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 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 los VM a un agente si el agente tiene un 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.

  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, que incluye Storage vMotion, no es compatible con una máquina virtual que ejecuta Agente para VMware (dispositivo virtual) y está deshabilitada automáticamente. Esta máquina virtual se añade a la lista **Anulaciones de máquinas virtuales** de la configuración 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 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.

Gestión de entornos de virtualización

Puede visualizar los entornos de vSphere, Hyper-V y Virtuozzo en su presentación nativa. Cuando el agente correspondiente esté instalado y registrado, aparecerá la pestaña **VMware**, **Hyper-V** o **Virtuozzo** en **Dispositivos**.

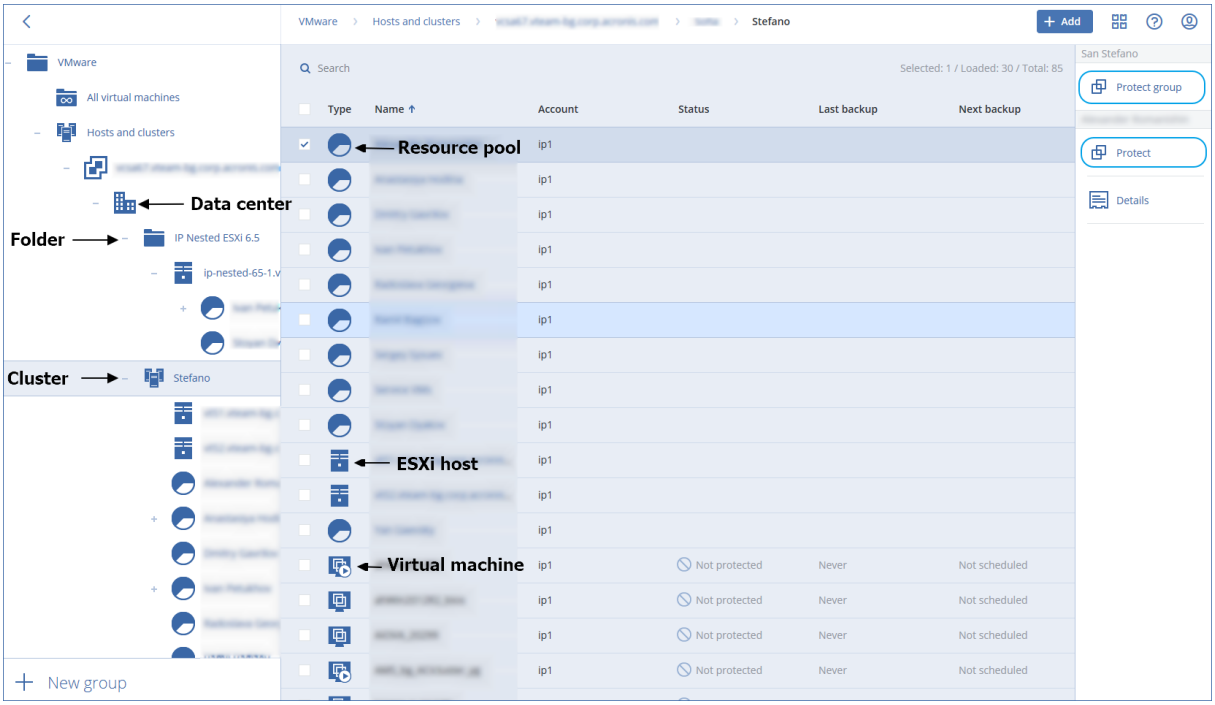
En la pestaña **VMware**, puede realizar una copia de seguridad de los siguientes objetos de la infraestructura vSphere:

- Centro de datos
- Carpeta
- Clúster

- Servidor ESXi
- Grupo de recursos

Todos estos objetos de infraestructura funcionan como objeto del grupo para equipos virtuales. Cuando aplique un plan de protección a cualquiera de estos objetos de grupo, se realizará una copia de seguridad de todos los equipos virtuales incluidos en él. Puede realizar una copia de seguridad de los equipos de los grupos seleccionados al hacer clic en **Proteger**, o bien de los equipos del grupo principal en el que se incluyen los grupos seleccionados al hacer clic en **Proteger grupo**.

Por ejemplo, ha seleccionado el clúster de Stefano y, a continuación, el grupo de recursos que incluye. Si hace clic en **Proteger**, se realizará una copia de seguridad de todos los equipos virtuales incluidos en el grupo de recursos seleccionado. Si hace clic en **Proteger grupo**, se realizará una copia de seguridad de todos los equipos virtuales incluidos en el clúster de Stefano.



En la pestaña **VMware** se pueden modificar las credenciales de acceso a vCenter Server o al servidor ESXi independiente sin tener que reinstalar el agente.

Para modificar las credenciales de acceso a vCenter Server o al servidor ESXi

1. En **Dispositivos**, haga clic en **VMware**.
2. Haga clic en **Servidores y clústeres**.
3. En la lista de **Servidores y clústeres** (situada a la derecha del árbol de **Servidores y clústeres**), seleccione vCenter Server o el servidor ESXi independiente que se especificó durante la instalación del Agente para VMware.
4. Haga clic en **Detalles**.

5. En **Credenciales**, haga clic en el nombre de usuario.
6. Especifique las nuevas credenciales de acceso y, a continuación, haga clic en **Aceptar**.

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**

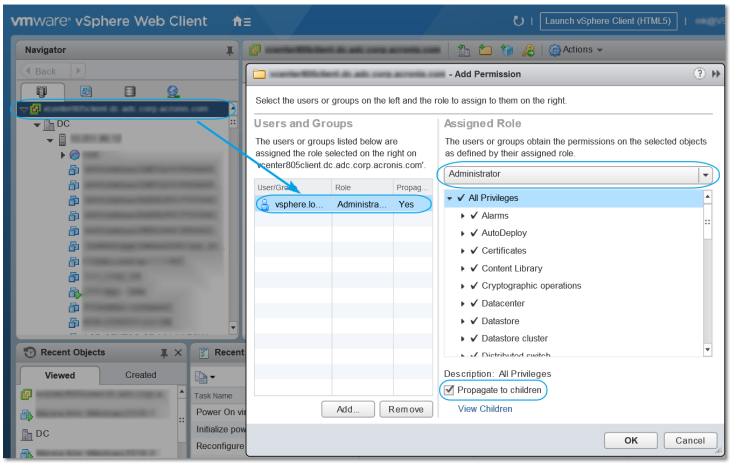
Agente para VMware: privilegios necesarios

Para llevar a cabo cualquier operación con objetos de vCenter, como equipos virtuales, servidores ESXi, clústeres o vCenter, entre otros, Agente para VMware se autentica en el servidor vCenter o ESXi mediante las credenciales de vSphere proporcionadas por el usuario. La cuenta de vSphere, que usa el Agente para VMware para establecer la conexión con vSphere, debe contar con los privilegios necesarios en todos los niveles de la infraestructura de vSphere, empezando desde el nivel de vCenter.

Indique la cuenta de vSphere con los privilegios necesarios durante la instalación o configuración de Agente para VMware. Si necesita cambiar la cuenta en un momento posterior, consulte "Gestión de entornos de virtualización" (p. 736).

Cómo asignar los permisos a un usuario de vSphere en el nivel de vCenter

1. Inicie sesión en el cliente web de vSphere.
2. Haga clic en vCenter y, a continuación, en **Añadir permiso**.
3. Seleccione o añada un nuevo usuario con el rol requerido (el rol debe incluir todos los permisos necesarios de la tabla que aparece a continuación).
4. Seleccione la opción **Propagar a secundarios**.



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 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	**Licencias**	+	+	+	+
	Deshabilitar métodos	+	+	+	
	Habilitar métodos	+	+	+	

	Gestionar atributos personalizados	+	+	+	
	Establecer atributo personalizado	+	+	+	
Servidor > **Configuración**	**Configuración de partición de almacenamiento**				+
Servidor > **Operaciones locales**	**Crear VM**				+
	Eliminar VM				+
	Reconfigurar VM				+
Red	**Asignar red**		+	+	+
Recurso	**Asignar equipo virtual a pool de recursos**		+	+	+
Equipo virtual > **Configuración**	**Añadir disco existente**	+	+		+
	Añadir disco nuevo		+	+	+
	Añadir o quitar dispositivo		+		+
	Avanzado	+	+	+	
	Cambiar recuento de CPU		+		
	Seguimiento de cambios de disco	+		+	
	Disco arrendado	+		+	
	Memoria		+		
	Quitar disco	+	+	+	+
	Cambiar nombre		+		
	Establecer anotación				+

	Configuración		+	+	+
Equipo virtual >**Operaciones de huésped**	**Ejecución de programa de operación de huésped**	+**			
	Consultas de operación de huésped	+**			
	Modificaciones de operaciones de huésped	+**			
Equipo 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		+	+	+
Equipo virtual > **Inventario**	**Crear desde existente**		+	+	+
	Crear nuevo		+	+	+
	Registrar				+
	Eliminar		+	+	+
	Anular el registro				+
Equipo virtual > **Aprovisionamiento**	**Permitir acceso a disco**		+	+	+
	Permitir acceso a disco de solo	+		+	

	lectura				
	Permitir descarga de equipo virtual	+	+	+	+
Equipo virtual > **Estado** **Equipo virtual** > **Administración de instantáneas** (vSphere 6.5 y versiones posteriores)	**Crear instantánea**	+		+	+
	Eliminar instantánea	+		+	+
vApp	**Agregar equipo virtual**				+

***** Este privilegio solo es obligatorio para realizar copias de seguridad de equipos cifrados.

****** Este privilegio solo es obligatorio para copias de seguridad compatibles con aplicaciones.

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**.

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_
```

```
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 al Agente para VMware (dispositivo virtual), el Agente para Scale Computing, el Agente para Virtuozzo Hybrid Infrastructure y el Agente para oVirt.

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/Global.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`.

Migración de equipos

Puede realizar la migración de un equipo recuperando su copia de seguridad en un equipo no original.

La siguiente tabla resume las opciones de migración disponibles.

Tipo de equipo incluido en la copia de seguridad	Destinos de recuperación disponibles							
	Equipo físico	Equipo virtual ESXi	Equipo virtual Hyper-V	Virtuozzo		Equipo virtual de Virtuozzo Hybrid Infrastructure	Equipo virtual de Scale Computing HC3	Máquina virtual de RHV/oVirt
				Equipo virtual	Contenedor			
Equipo físico	+	+	+	-	-	+	+*	+
Equipo virtual VMware ESXi	+	+	+	-	-	+	+*	+
Equipo virtual Hyper-V	+	+	+	-	-	+	+*	+
Equipo virtual Virtuozzo	+	+	+	+	-	+	+*	+
Contenedor Virtuozzo	-	-	-	-	+	-	-	-
Equipo virtual de Virtuozzo Hybrid Infrastructure	+	+	+	-	-	+	+*	+
Equipo virtual de Scale Computing HC3	+	+	+	-	-	+	+	+
Máquina virtual de Red Hat Virtualization/oVirt	+	+	+	-	-	+	+*	+

* Si está habilitado el arranque seguro en el equipo de origen, no se podrá iniciar la máquina virtual recuperada hasta que deshabilite el arranque seguro en la consola de la máquina virtual después de la recuperación.

Nota
No puede recuperar equipos 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.

Para obtener más información sobre cómo realizar las operaciones de migración, consulte los temas siguientes:

- Para la migración física a virtual (P2V), consulte "De equipo físico a virtual" (p. 525).
- Para la migración virtual a virtual (V2V), consulte "Recuperación de una máquina virtualPuede recuperar equipos virtuales gracias a sus copias de seguridad.No puede recuperar copias de seguridad en la consola de Cyber Protect para inquilinos en el modo de Cumplimiento. Para obtener más información sobre cómo recuperar dichas copias de seguridad, consulte "Recuperación de copias de seguridad para inquilinos en el modo de Cumplimiento" (p. 1).Requisitos previosDurante la recuperación en un equipo virtual, éste debe permanecer detenido. De forma predeterminada, el software detiene el equipo sin previo aviso. Cuando se complete la recuperación, debe iniciar el equipo manualmente. Puede modificar este comportamiento mediante la opción de recuperación de gestión de energía del equipo virtual (haga clic en Opciones de recuperación > Gestión de energía del equipo virtual).ProcedimientoRealice 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.Haga clic en Recuperar > Todo el equipo.Si desea recuperar el equipo virtual en un equipo físico, seleccione Equipo físico en Recuperar en. De lo contrario, omita este paso.La recuperación en un equipo físico solo es posible si la configuración de disco del equipo de destino coincide exactamente con la configuración de disco de la copia de seguridad.En caso afirmativo, siga con el paso 4 de la sección "Equipo físico". En caso contrario, le recomendamos que realice la migración V2P mediante un dispositivo de arranque.[Opcional] De forma predeterminada, el software selecciona automáticamente el equipo original como equipo de destino. Para recuperar el equipo virtual en otro equipo virtual, haga clic en Equipo de destino y, a continuación, haga lo siguiente:Seleccione el hipervisor (VMware ESXi, Hyper-V, Virtuozzo, Virtuozzo Hybrid Infrastructure, Scale Computing HC3 o oVirt).Solo los equipos virtuales Virtuozzo pueden recuperarse en Virtuozzo. Para obtener más información sobre la migración del entorno virtual al virtual, consulte "Migración de equipos".Seleccione si desea realizar la recuperación en un equipo nuevo o en otro ya existente.Seleccione el servidor y especifique el nuevo nombre de equipo, o bien seleccione un equipo de destino existente.Haga clic en Aceptar.Configure las opciones de recuperación adicionales que necesite.[No disponible para Virtuozzo Hybrid Infrastructure ni para Scale Computing HC3] Haga clic en Almacén de datos para ESXi, Ruta para Hyper-V y Virtuozzo o Dominio de almacenamiento para Red Hat Virtualization (oVirt). A continuación, seleccione el almacén de datos (almacenamiento) para la máquina virtual.Para ver el almacén de datos (almacenamiento), la interfaz y el modo de aprovisionamiento para cada unidad de disco virtual, haga clic en Asignación de discos. Puede modificar esta configuración a menos que esté recuperando un contenedor de Virtuozzo o un equipo virtual de la Virtuozzo

Hybrid Infrastructure.Para la Virtuozzo Hybrid Infrastructure, solo puede seleccionar la directiva de almacenamiento de los discos de destino. Para hacerlo, seleccione el disco de destino deseado y, a continuación, haga clic en Cambiar. En la ficha que se abre, haga clic en el icono de engranaje, seleccione la directiva de almacenamiento y, a continuación, haga clic en Listo.La sección de asignación también permite elegir discos individuales para la recuperación. [Disponible para VMware ESXi, Hyper-V y Virtuozzo] Haga clic en Configuración de VM para cambiar el tamaño de la memoria, el número de procesadores y las conexiones de red de la máquina virtual.[Para Virtuozzo Hybrid Infrastructure] Seleccione Variante para cambiar el tamaño de la memoria y el número de procesadores de la máquina virtual.[Solo disponible para equipos Windows en los que hay instalado un agente de protección] Habilite el conmutador Recuperación segura para garantizar que los datos recuperados están libres de malware. Para obtener más información sobre cómo funciona la recuperación segura, consulte "Recuperación segura" (p. 1).Haga clic en Iniciar recuperación.Al realizar la recuperación en un equipo virtual existente, confirme que desea sobrescribir los discos.El proceso de recuperación se muestra en la pestaña Actividades." (p. 1).

- Para la migración virtual a física (V2P), consulte "Recuperación de una máquina virtualPuede recuperar equipos virtuales gracias a sus copias de seguridad.No puede recuperar copias de seguridad en la consola de Cyber Protect para inquilinos en el modo de Cumplimiento. Para obtener más información sobre cómo recuperar dichas copias de seguridad, consulte "Recuperación de copias de seguridad para inquilinos en el modo de Cumplimiento" (p. 1).Requisitos previosDurante la recuperación en un equipo virtual, éste debe permanecer detenido. De forma predeterminada, el software detiene el equipo sin previo aviso. Cuando se complete la recuperación, debe iniciar el equipo manualmente. Puede modificar este comportamiento mediante la opción de recuperación de gestión de energía del equipo virtual (haga clic en Opciones de recuperación > Gestión de energía del equipo virtual).ProcedimientoRealice 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.Haga clic en Recuperar > Todo el equipo.Si desea recuperar el equipo virtual en un equipo físico, seleccione Equipo físico en Recuperar en. De lo contrario, omita este paso.La recuperación en un equipo físico solo es posible si la configuración de disco del equipo de destino coincide exactamente con la configuración de disco de la copia de seguridad.En caso afirmativo, siga con el paso 4 de la sección "Equipo físico". En caso contrario, le recomendamos que realice la migración V2P mediante un dispositivo de arranque.[Opcional] De forma predeterminada, el software selecciona automáticamente el equipo original como equipo de destino. Para recuperar el equipo virtual en otro equipo virtual, haga clic en Equipo de destino y, a continuación, haga lo siguiente:Seleccione el hipervisor (VMware ESXi, Hyper-V, Virtuozzo, Virtuozzo Hybrid Infrastructure, Scale Computing HC3 o oVirt).Solo los equipos virtuales Virtuozzo pueden recuperarse en Virtuozzo. Para obtener más información sobre la migración del entorno virtual al virtual, consulte "Migración de equipos".Seleccione si desea realizar la recuperación en un equipo nuevo o en otro ya existente.Seleccione el servidor y especifique el nuevo nombre de equipo, o bien seleccione un equipo de destino existente.Haga clic en Aceptar.Configure las opciones de recuperación adicionales que necesite.[No disponible para Virtuozzo Hybrid

Infrastructure ni para Scale Computing HC3] Haga clic en Almacén de datos para ESXi, Ruta para Hyper-V y Virtuozzo o Dominio de almacenamiento para Red Hat Virtualization (oVirt). A continuación, seleccione el almacén de datos (almacenamiento) para la máquina virtual.Para ver el almacén de datos (almacenamiento), la interfaz y el modo de aprovisionamiento para cada unidad de disco virtual, haga clic en Asignación de discos. Puede modificar esta configuración a menos que esté recuperando un contenedor de Virtuozzo o un equipo virtual de la Virtuozzo Hybrid Infrastructure.Para la Virtuozzo Hybrid Infrastructure, solo puede seleccionar la directiva de almacenamiento de los discos de destino. Para hacerlo, seleccione el disco de destino deseado y, a continuación, haga clic en Cambiar. En la ficha que se abre, haga clic en el icono de engranaje, seleccione la directiva de almacenamiento y, a continuación, haga clic en Listo.La sección de asignación también permite elegir discos individuales para la recuperación. [Disponible para VMware ESXi, Hyper-V y Virtuozzo] Haga clic en Configuración de VM para cambiar el tamaño de la memoria, el número de procesadores y las conexiones de red de la máquina virtual.[Para Virtuozzo Hybrid Infrastructure] Seleccione Variante para cambiar el tamaño de la memoria y el número de procesadores de la máquina virtual.[Solo disponible para equipos Windows en los que hay instalado un agente de protección] Habilite el conmutador Recuperación segura para garantizar que los datos recuperados están libres de malware. Para obtener más información sobre cómo funciona la recuperación segura, consulte "Recuperación segura" (p. 1).Haga clic en Iniciar recuperación.Al realizar la recuperación en un equipo virtual existente, confirme que desea sobrescribir los discos.El proceso de recuperación se muestra en la pestaña Actividades." (p. 1) y "Recuperar discos usando dispositivos de arranque" (p. 530).

Migración a través de un dispositivo de arranque

En lugar de llevar a cabo la migración del equipo desde la consola de Cyber Protect, puede recuperar un equipo a través de un dispositivo de arranque.

Le recomendamos usar un dispositivo de arranque en los casos siguientes:

- Realizar una migración que no es compatible a nivel nativo.
  Por ejemplo, utilice un dispositivo de arranque para recuperar un equipo físico o una máquina virtual que no sea de Virtuozzo como una máquina virtual de Virtuozzo en un host de 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 el dispositivo 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. 751).

Máquinas virtuales de Microsoft Azure y Amazon EC2

Para realizar una copia de seguridad de una máquina virtual de Microsoft Azure o Amazon EC2, instale un agente de protección en el equipo. La copia de seguridad y la recuperación son iguales

que con un equipo físico. No obstante, el equipo se cuenta como virtual al definir las cuotas del número de equipos.

La diferencia con respecto a un equipo físico es que las máquinas virtuales de Microsoft Azure y Amazon EC2 no se pueden iniciar desde soportes de arranque. Si necesita realizar una recuperación a una máquina virtual de Microsoft Azure o Amazon EC2 nueva, siga el procedimiento siguiente.

Nota
El siguiente procedimiento de recuperación solo se aplica a las copias de seguridad de equipos que contengan todas las unidades necesarias para ejecutar Microsoft Azure de forma nativa (copias de seguridad creadas a partir de una máquina virtual de Microsoft Azure, un equipo de Hyper-V o el equipo de origen con Windows Server 2016 o una versión posterior). Para obtener información sobre la recuperación multiplataforma, consulte este artículo de la base de conocimientos.

Para recuperar un equipo como una máquina virtual de Microsoft Azure o Amazon EC2

1. Cree una máquina virtual nueva desde una imagen/plantilla en Microsoft Azure o Amazon EC2. El equipo nuevo debe tener la misma configuración de disco que el equipo que desea recuperar.
2. Instale Agente para Windows o Agente para Linux en el equipo nuevo.
3. Recupere el equipo del que se ha realizado la copia de seguridad, como se describe en "Equipo físico". Al configurar la recuperación, seleccione el equipo nuevo como el equipo de destino.

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 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 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. 751).
   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.

¿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 y 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. 753).
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.
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. 755).
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. 764).
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. Seleccione el tipo de archivo del dispositivo de arranque creado:
    - Imagen ISO
    - Archivo ZIP
14. Especifique un nombre de archivo para el archivo del dispositivo de arranque.
15. 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.

- **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**

  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.

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 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/<archivo>**.

- **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.

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.
`default`	cadena si el `tipo` es `string`, `multiString`, `password` o `enum` número si el `tipo` 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`	number	No	El valor de paso del control de número de un cuadro de número. Si no se especifica la pareja, el valor

(solo para `spinner`)			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.
`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,
                "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 WinPE y WinRE

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).

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)

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:

- 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. 764).

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 **Añadir** y, a continuación, especifique la ruta al archivo .inf necesario para el correspondiente controlador SCSI, RAID o SATA, adaptador de red, unidad de cinta u otro dispositivo.
   - 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
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:

  ```
  copie 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

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 **Mostrar nombre**, 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**.

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

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**.

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**.

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. 764).

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 medio o ver información, actividades y alertas sobre el medio.

Importante
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. 751). 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

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. 481).
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. 544).
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. El proceso de recuperación se muestra 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 físicosEn esta sección se describe la recuperación de equipos físicos mediante la interfaz web.Use dispositivos de inicio en vez de interfaz web si necesita recuperar:Una máquina que ejecute macOSUn equipo de un inquilino en el modo de CumplimientoCualquier sistema operativo desde cero o en un equipo sin conexiónLa estructura de los volúmenes lógicos (volúmenes creados por Logical Volume Manager en Linux). El dispositivo le permite recrear automáticamente la estructura del volumen lógico.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.Recuperación con reinicioLa recuperación de un sistema operativo y de los volúmenes cifrados con BitLocker requiere un reinicio. Puede elegir si reiniciar el equipo automáticamente o asignarle el estado Interacción necesaria. El sistema operativo recuperado se conecta a Internet automáticamente.Los volúmenes no cifrados de los que se haya hecho una copia de seguridad se recuperan como no cifrados.La recuperación de los volúmenes cifrados con BitLocker requiere que haya un volumen no cifrado en el mismo equipo y que dicho volumen tenga al menos 1 GB de espacio libre. Si no se cumple alguna de estas condiciones, la recuperación fallará.La recuperación de un volumen del sistema cifrado no requiere ninguna acción adicional. Para recuperar un volumen cifrado que no es del sistema, primero debe bloquearlo, por ejemplo, abriendo un archivo que resida en ese volumen. De lo contrario, la recuperación continuará sin reiniciarse y Windows podría no reconocer el volumen recuperado.Si la recuperación falla y su equipo se reinicia con el error No puede obtenerse el archivo de la partición, pruebe a deshabilitar el arranque seguro. Para obtener más información sobre cómo hacerlo, consulte Deshabilitación del arranque seguro en la documentación de Microsoft.Para recuperar un equipo físicoSeleccione el equipo del que se ha realizado la copia de seguridad.Haga clic en Recuperación.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 una de las siguientes operaciones: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.Recupere el equipo como se describe en "Recuperar discos usando dispositivos de inicio".Haga clic en Recuperar > Todo el equipo.El software asigna automáticamente los discos de las copias de seguridad a los discos del equipo de destino.Para recuperar en otro equipo físico, haga clic en Equipo de destino y, a continuación, seleccione un equipo de destino que esté conectado.Si no está satisfecho con el resultado de la asignación o si la asignación de discos falla, haga clic en

Asignación de volúmenes puede volver a asignar los discos manualmente.La sección de asignación también permite elegir los discos individuales o volúmenes para la recuperación. Podrá cambiar entre recuperar discos y volúmenes utilizando el enlace Cambiar a... ubicado en la esquina superior derecha.[Solo disponible para equipos Windows en los que hay instalado un agente de protección] Habilite el conmutador Recuperación segura para garantizar que los datos recuperados están libres de malware. Para obtener más información sobre cómo funciona la recuperación segura, consulte "Recuperación segura" (p. 1).Haga clic en Iniciar recuperación.Confirme si desea sobrescribir los discos con sus respectivas copias de seguridad. Elija si desea reiniciar el equipo automáticamente.El proceso de recuperación se muestra en la pestaña Actividades." (p. 1).

5. Para la configuración de recuperación avanzada, haga clic en **Opciones de recuperación**. Para obtener más información, consulte "Opciones de recuperación" (p. 544).
6. Haga clic en **Iniciar recuperación**.
7. Confirme si desea sobrescribir los discos con sus respectivas copias de seguridad. Elija si desea reiniciar el equipo automáticamente.
8. El proceso de recuperación se muestra 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.

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.

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
Activar Startup Recovery Manager en un equipo con volumen del sistema no cifrado requiere al menos 100 MB de espacio libre en este equipo. La recuperación que requiere reiniciar el equipo necesita 100 MB más.

Para activar Startup Recovery Manager en un equipo que tiene un volumen cifrado con BitLocker, este equipo debe tener al menos un volumen no cifrado en el que haya al menos 500 MB de espacio libre. La recuperación con reinicio requiere 500 MB adicionales de espacio libre.

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 un equipo Windows o Linux con un agente

1. En la consola 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**, compruebe la fila **Resultado** para confirmar que la activación se ha realizado correctamente y haga clic en **Cerrar**.

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 un equipo Windows o Linux 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**, compruebe la fila **Resultado** para confirmar que la deshabilitación se ha realizado con éxito y haga clic en **Cerrar**.

Implementación de la recuperación ante desastres

Nota
- Esta funcionalidad no admite ubicaciones de copia de seguridad de Microsoft Azure.

Acerca de Cyber Disaster Recovery Cloud

Cyber Disaster Recovery Cloud (DR): parte de Cyber Protection que proporciona un servicio de recuperación ante desastres (DRaaS). Cyber Disaster Recovery Cloud es una solución rápida y estable para iniciar las copias exactas de sus equipos en el sitio en la nube y trasladar la carga de trabajo de los equipos originales dañados a los servidores de recuperación en la nube, en caso de desastre natural o causado por el ser humano.

Puede configurar la recuperación ante desastres de las siguientes maneras:

- Cree un plan de protección que incluya el módulo de recuperación ante desastres y aplíquelo a sus dispositivos. Así se configurará automáticamente la infraestructura predeterminada de recuperación ante desastres. Consulte Crear un plan de protección de recuperación ante desastres.
- Configure la infraestructura en la nube de recuperación ante desastres manualmente y controle cada paso. Consulte "Configuración de servidores de recuperación" (p. 823).

La funcionalidad clave

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

- Gestionar el servicio Cyber Disaster Recovery Cloud 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 ubicaciones locales y en la nube
- Proteger su equipo con el uso de servidores de recuperación en el cloud
- Proteger aplicaciones y dispositivos con el uso de servidores principales en el cloud
- Realizar operaciones de recuperación ante desastres automáticas para copias de seguridad cifradas

[1] [Recuperación ante desastres] 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.

- Realizar una prueba de conmutación por error en la red aislada
- Use runbooks para iniciar el entorno de producción en la nube.

Requerimientos de software

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 16.04, 18.04, 20.x, 21.x
- 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

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 https://kb.acronis.com/content/71616.

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

El dispositivo VPN se ha probado para las siguientes plataformas de virtualización:

- 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

Puede que este software funcione con otras plataformas de virtualización y versiones distintas, pero no se lo podemos asegurar.

Limitaciones

Las siguientes plataformas y configuraciones no son compatibles con Cyber Disaster Recovery Cloud:

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 discos dinámicos no son compatibles.
   - Los sistemas operativos de los equipos de escritorio Windows no son compatibles (debido a las condiciones de los productos de Microsoft).
   - El servicio 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. 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 Cyber Disaster Recovery Cloud

Puede utilizar una versión de prueba de Acronis Cyber Disaster Recovery Cloud durante un periodo de 30 días. En este caso, la recuperación ante desastres 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.

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 recuperación ante desastres no se puede utilizar si se cambia la ubicación primaria de almacenamiento de copia de seguridad por una secundaria con redundancia geográfica.

Compatibilidad de la recuperación ante desastres 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

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. 43).

Puntos de cálculo

En Disaster Recovery, 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.

Todos los servidores que estén funcionando en la nube Acronis 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 cobrarán 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 la recuperación ante desastres 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.

Configuración de la funcionalidad de recuperación ante desastres

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

Para configurar la funcionalidad de recuperación ante desastres:

1. Configure el tipo de conectividad en el sitio en el cloud:
   - Conexión de punto a sitio
   - Conexión OpenVPN de sitio a sitio
   - Conexión VPN de IPsec de varios sitios
   - Modo solo en la nube
2. Cree un plan de protección con el módulo de copia de seguridad habilitado y seleccione todo el equipo o sistema y los volúmenes de arranque de los que quiera realizar una copia de seguridad. Se necesita al menos un plan de protección para crear un servidor de recuperación.
3. Aplique el plan de protección a los servidores locales que quiera proteger.
4. Cree los servidores de recuperación para cada uno de los servidores locales que desee proteger.
5. Realice una prueba de conmutación por error para comprobar cómo funciona.
6. [Opcional] Cree los servidores principales para la replicación de aplicaciones.

Como resultado, habrá configurado la funcionalidad de recuperación ante desastres que protegerá sus servidores locales de un desastre.

Si se produce un desastre, puede realizar una conmutación por error de la carga de trabajo a los servidores de recuperación en la nube. Se debe crear por lo menos un punto de recuperación antes de llevar a cabo una conmutación por error en servidores de recuperación. Cuando su sitio local se recupere del desastre, puede trasladar la carga de trabajo de vuelta a su sitio local realizando una

conmutación por recuperación. Para obtener más información sobre el proceso de conmutación por recuperación, consulte "Requisitos previos" (p. 839) y "Requisitos previos" (p. 844).

Crear un plan de protección de recuperación ante desastres

Cree un plan de protección que incluya el módulo Recuperación ante desastres y aplíquelo a sus dispositivos.

De forma predeterminada, el módulo Recuperación ante desastres se deshabilita al crear un nuevo plan de protección. Al habilitar la funcionalidad de recuperación ante desastres y aplicar el plan a sus dispositivos, se crea la infraestructura de red en la nube, incluido 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 en estado En espera (máquina virtual que no está en ejecución) con la configuración predeterminada. El tamaño del servidor de recuperación se establece automáticamente en función de la CPU y la RAM del dispositivo protegido. La infraestructura de red en la nube predeterminada también se crea automáticamente: Las redes y la puerta de enlace de VPN del sitio en la nube a las que se conectarán los servidores de recuperación.

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 eliminan automáticamente. Puede eliminar la infraestructura de recuperación ante desastres manualmente, en caso necesario.

Nota

- Después de configurar la recuperación ante desastres, podrá realizar una prueba o la conmutación por error de producción desde cualquier punto de recuperación creado después de crear el servidor de recuperación del dispositivo. Los puntos de recuperación que se generaron antes de que el dispositivo estuviese protegido con la recuperación ante desastres (por ejemplo, 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. 813).

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. Haga clic en el interruptor que se encuentra junto al nombre del módulo para habilitar el módulo de recuperación ante desastres.
6. Haga clic en **Crear**.
   Se crea el plan y se aplica a los equipos seleccionados.

Qué hacer a continuación

- Puede editar la configuración predeterminada del servidor de recuperación. Para obtener más información, consulte "Configuración de servidores de recuperación" (p. 823).
- Puede editar la configuración predeterminada del servidor de red. Para obtener más información, consulte "Configuración de conectividad" (p. 784).
- Puede obtener más información sobre los parámetros predeterminados del servidor de recuperación y la infraestructura de las redes en la nube. Para obtener más información, consulte "Edición de los parámetros predeterminados del servidor de recuperación" (p. 782) y "Infraestructura de red en la nube" (p. 784).

Edición de los parámetros predeterminados del servidor de recuperación

Al crear y aplicar un plan de protección de recuperación ante desastres, se crea un servidor de recuperación con parámetros predeterminados. Puede editar estos parámetros predeterminados más adelante.

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.

Para editar los parámetros predeterminados del servidor de recuperación

1. Vaya a **Dispositivos** > **Todos los dispositivos**.
2. Seleccione un dispositivo y haga clic en **Recuperación ante desastres**.
3. Edite los parámetros predeterminados del servidor de recuperación.
   Los parámetros del servidor de recuperación se describen en la siguiente tabla.

Servidor de recuperación parámetro	Predeterminado valor	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 el cloud	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.
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

La infraestructura de red en la nube consta de la puerta de enlace de VPN del sitio en la nube y de las redes en la nube a las que se conectarán los servidores de recuperación.

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.

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" (p. 806).
- Si tiene que configurar la conectividad OpenVPN de sitio a sitio, descargue el dispositivo VPN y configúrelo. Consulte "Configuración de OpenVPN de sitio a sitio" (p. 796). 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 redes predeterminada, haga clic en el enlace **Ir a Conectividad** del módulo de recuperación ante desastres del plan de protección o acceda a **Recuperación ante desastres** > **Conectividad**.

Configuración de conectividad

Esta sección explica los conceptos de red que debe conocer para comprender el funcionamiento de Cyber Disaster Recovery Cloud. Aprenderá a configurar distintos tipos de conectividad al sitio en el cloud, según sus necesidades. Por último, aprenderá a gestionar las redes en el cloud y la configuración del dispositivo VPN y la puerta de enlace de VPN.

Conceptos de redes

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

Cyber Disaster Recovery Cloud 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**

  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, Cyber Disaster Recovery Cloud 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 recuperación ante desastres 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.

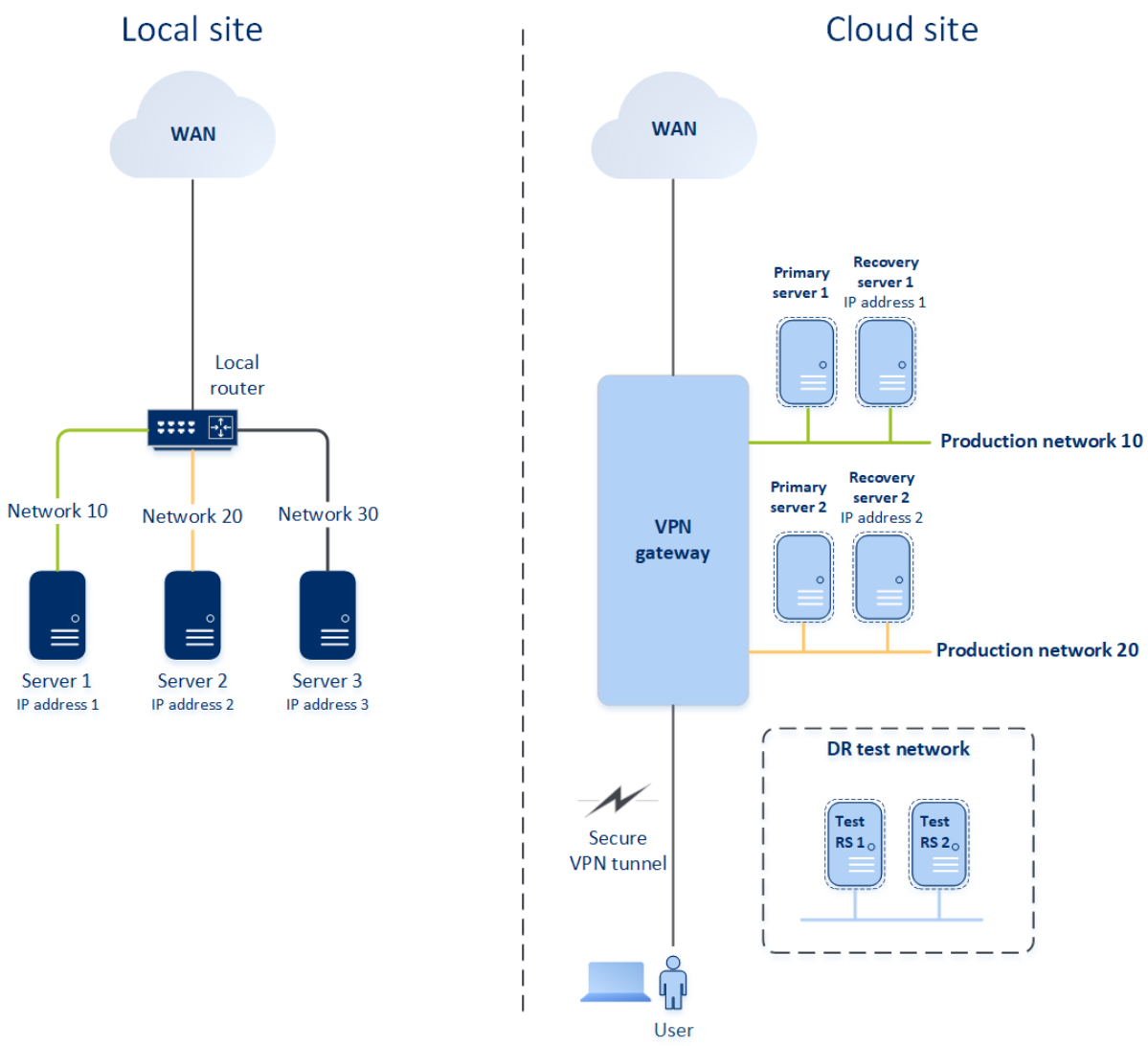
  Para el acceso en un sitio local, este tipo de conexión requiere la implementación de un dispositivo VPN en el sitio local.

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.



Conexión OpenVPN de sitio a sitio

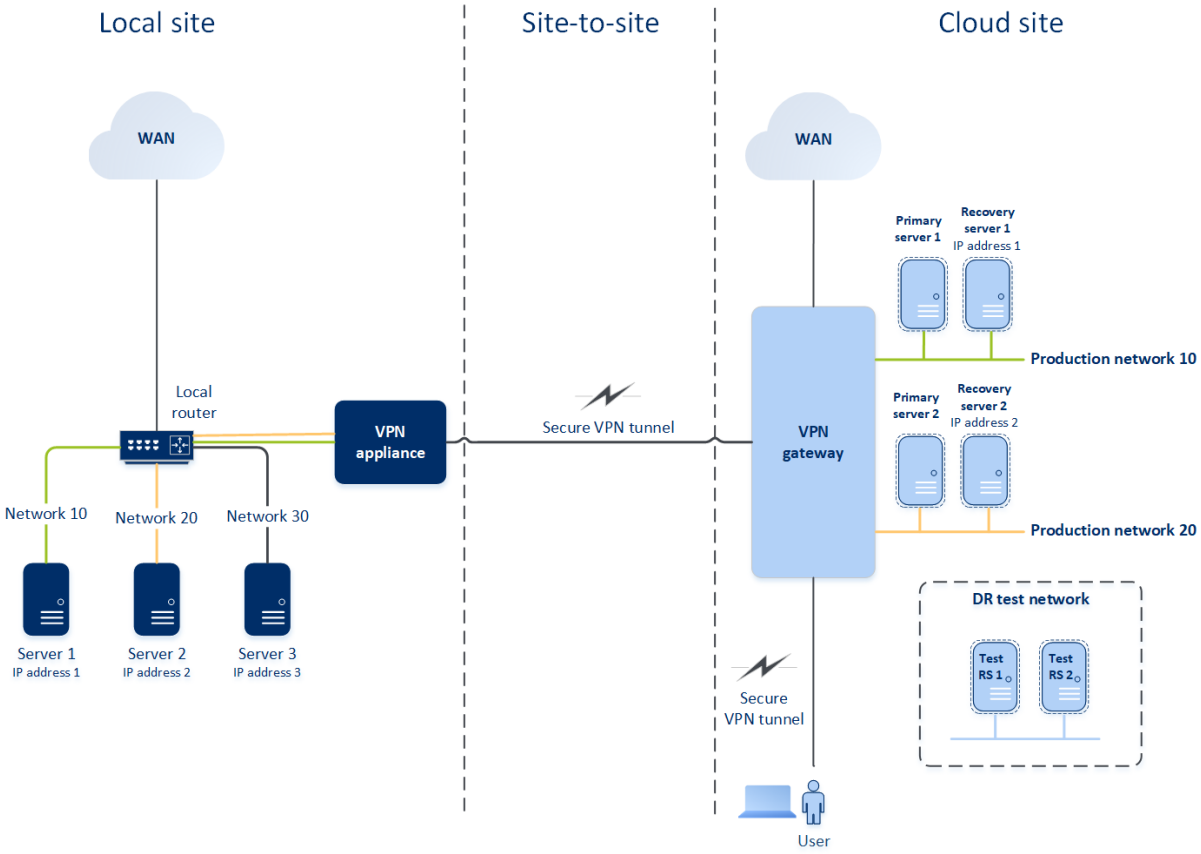
Nota

La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

Para entender cómo funcionan las redes en Cyber Disaster Recovery Cloud, 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 Cyber Disaster Recovery Cloud le permite realizar una conmutación por error de toda la carga de trabajo de los equipos dañados en el sitio local a los servidores en la nube que se encuentran en la nube. Puede proteger hasta 23 redes con Cyber Disaster Recovery Cloud.



Para establecer una comunicación 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 implementará automáticamente la puerta de enlace de VPN en el sitio de la nube. Después, debe implementar el dispositivo VPN en su sitio local, añadir las redes que desea proteger y registrar el dispositivo en la nube. Cyber Disaster Recovery Cloud crea una réplica de su red local en la nube. Se establece un túnel VPN seguro entre el dispositivo VPN y la puerta de enlace de VPN. Permite extender su red local al cloud. Las redes de producción en el cloud están conectadas con sus redes locales. Los servidores locales y en la nube pueden comunicarse mediante este túnel VPN si se encuentran todos en el mismo segmento de Ethernet. La enrutación se realiza con su enrutador 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 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. Puede tener la misma dirección IP asignada que el equipo de origen e iniciarse en el mismo 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 el cloud 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 el cloud, 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 se tratarán en sus respectivas secciones, a continuación.

Cómo funciona el enrutamiento

Cuando se establece la 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 en la nube de una red quiere comunicarse con un servidor de otra red en la nube, el tráfico pasa 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 local y en el cloud es la **puerta de enlace de VPN**. Es una máquina virtual en la nube 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 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.

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 el cloud.

Servidores de recuperación

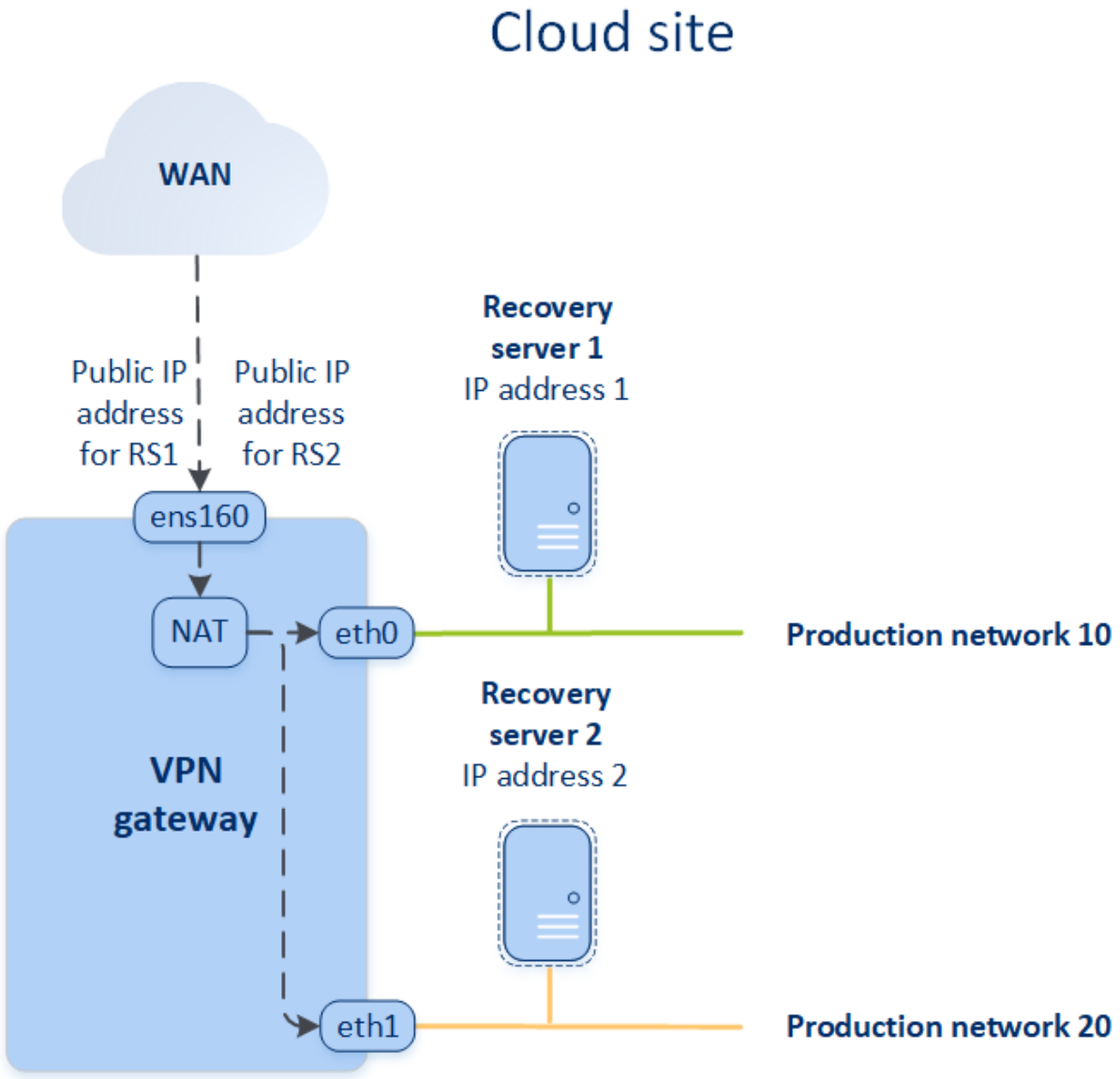
Servidor de recuperación: réplica del equipo original basada en las copias de seguridad del servidor protegido almacenadas en el cloud. Los servidores de recuperación se utilizan para trasladar cargas de trabajo desde los servidores originales en caso de desastre.

Al crear un servidor de recuperación, debe especificar los siguientes parámetros de red:

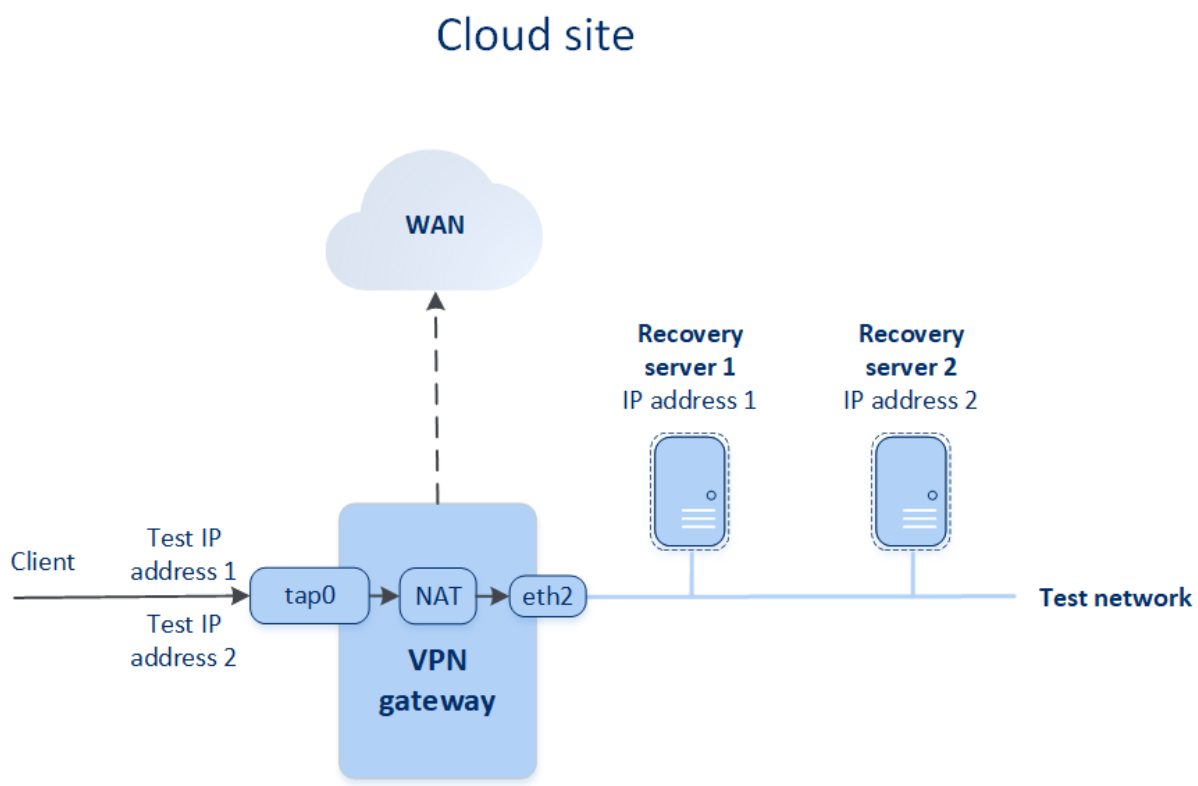
- **Red en el cloud** (obligatoria): una red en el cloud a la que se conecta un servidor de recuperación.
- **Dirección IP en la red de producción** (obligatoria): una dirección IP con la que se inicia un equipo virtual para un servidor de recuperación. Esta dirección se usa tanto para la red de producción como para la de prueba. Antes de iniciar el equipo virtual, este se configura para obtener la dirección IP mediante DHCP.
- **Dirección IP de prueba** (opcional): Una 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): Una 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).

Dirección IP de prueba y pública

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.



Si asigna la dirección 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 continúa funcionando mientras el servidor de recuperación con la misma dirección IP se inicia en la red de prueba en el cloud. 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 a través de sus direcciones IP de prueba, que se vuelven a asignar a las direcciones IP de producción mediante NAT.



Para obtener más información sobre OpenVPN de sitio a sitio, consulte "OpenVPN de sitio a sitio: información adicional" (p. 194).

Servidores principales

Servidor principal: 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:

- **Red en el cloud** (obligatoria): una red en el cloud a la que se conecta un servidor principal.
- **Dirección IP en la red de producción** (obligatoria): 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): Una dirección IP para acceder a un servidor principal desde Internet. Si un servidor no tiene dirección IP pública, solo es alcanzable desde la red local y no desde Internet.
- **Acceso a Internet** (opcional): permite que el servidor principal tenga acceso a Internet.

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 Cyber Disaster Recovery Cloud mediante una conexión VPN de IPsec L3 segura.

Este tipo de conectividad es útil para escenarios de recuperación ante desastres si tiene uno de los siguientes casos de uso:

- 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 están conectados a ellos mediante un túnel VPN de 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.

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 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. 814).
- 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.

Acceso de VPN remoto de punto a sitio

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

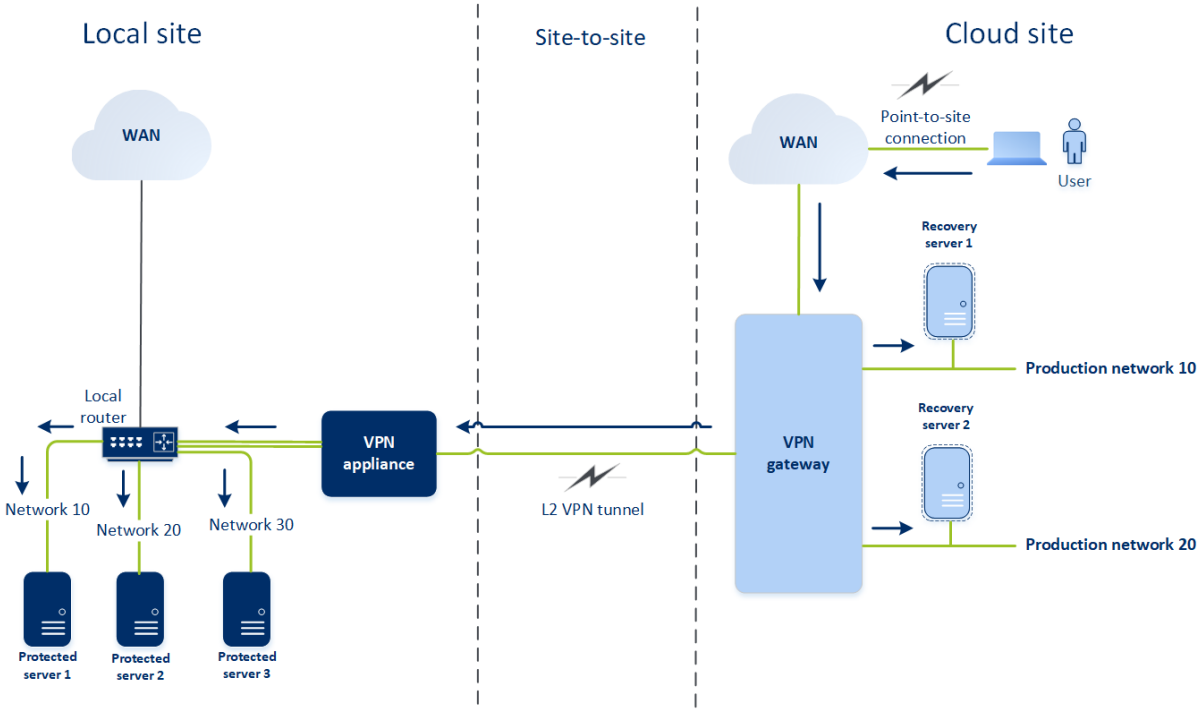
La conexión de punto a sitio es una conexión VPN segura desde el exterior que usa sus dispositivos de endpoint (como un ordenador o portátil) a los sitios en la nube y locales mediante un VPN. Está disponible después de establecer una conexión OpenVPN de sitio a sitio al sitio de Cyber Disaster Recovery Cloud. 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".
- 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.

Eliminación automática de entornos de clientes que no se usan en el sitio en la nube

El servicio de recuperación ante desastres 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.
- Se elimina el registro del dispositivo VPN.

Los inquilinos inactivos se restauran al estado en el que no se había configurado la conectividad.

Configuración de la conectividad inicial

Esta sección describe escenarios de configuración de la conectividad.

Configuración del modo solo en la nube

Para configurar una conexión en el modo solo en la nube

1. En la consola de Cyber Protect, vaya a **Recuperación ante desastres** > **Conectividad**.
2. Seleccione **Solo en la nube** y haga clic en **Configurar**.
   Como resultado, la puerta de enlace de VPN y la red en la nube con la dirección y la máscara definidas se implementarán en el sitio en la nube.

Para aprender a gestionar sus redes en el cloud y establecer la configuración de la puerta de enlace de VPN, consulte "Gestión de redes en el cloud".

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

- 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 **Recuperación ante desastres** > **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 recuperación ante desastres 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.

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 Cyber Disaster Recovery Cloud. La consola de Cyber Protect muestra las interfaces basándose en la información del dispositivo VPN.

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 **Recuperación ante desastres** > **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.

Pasos para configurar una conexión VPN de IPsec de varios sitios desde la pestaña Conectividad

1. En la consola de Cyber Protect, vaya a **Recuperación ante desastres** > **Conectividad**.
2. En la sección **Conexión VPN de varios sitios**, haga clic en **Configurar**.
   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.

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 **Recuperación ante desastres** > **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 **Recuperación ante desastres** > **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. 798).
- 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 firewall 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

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.
   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. 801).
   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. 801).

      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 **Añadir** (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 **Añadir** 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:

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

Parámetro	Descripción
	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. 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

Parámetro	Descripción
	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 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).

Parámetro	Descripción
	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. **Añadir**: 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.

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 recuperación ante desastres.

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. 814).

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. 814).

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

- Se ha configurado una conectividad OpenVPN de sitio a sitio.
- El dispositivo VPN se instala en el sitio local.

Para configurar la conexión de punto a sitio al sitio local

1. En la consola de Cyber Protect, vaya a **Recuperación ante desastres** > **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/.
   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 compañía" o "Ciberprotección".
d. Importe la configuración descargada a OpenVPN.
e. Inicie sesión en el cliente OpenVPN con sus credenciales de usuario de Cyber Protect Cloud (vea el paso 4 anterior).
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, el usuario se podrá conectar al equipo en el sitio local.

Gestión de redes

Esta sección describe escenarios de gestión de redes.

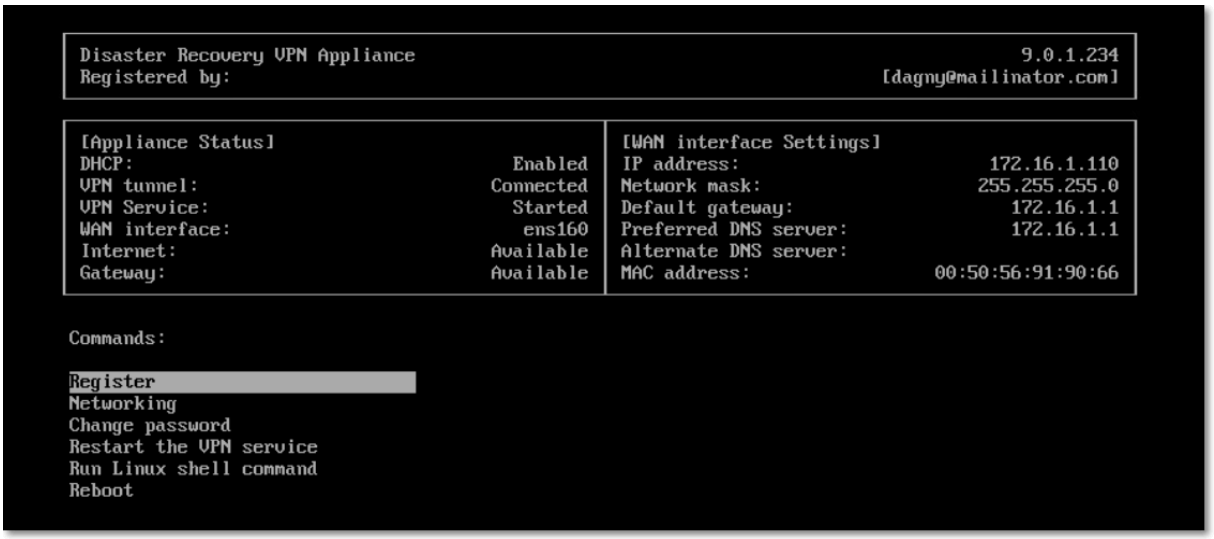
Gestión de redes

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

Conexión OpenVPN de sitio a sitio

Para añadir una red en el sitio local y extenderla al cloud:

1. En el dispositivo VPN, configure la nueva interfaz de red con la red local que desea extender al cloud.
2. Inicie sesión en la consola del dispositivo VPN.
3. En la sección **Redes**, establezca la configuración de red para la nueva interfaz.



El dispositivo VPN comienza a transmitir información sobre las redes de todas las interfaces activas a Cyber Disaster Recovery Cloud. La consola de Cyber Protect muestra las interfaces basándose en la información del dispositivo VPN.

Para eliminar una red extendida al cloud:

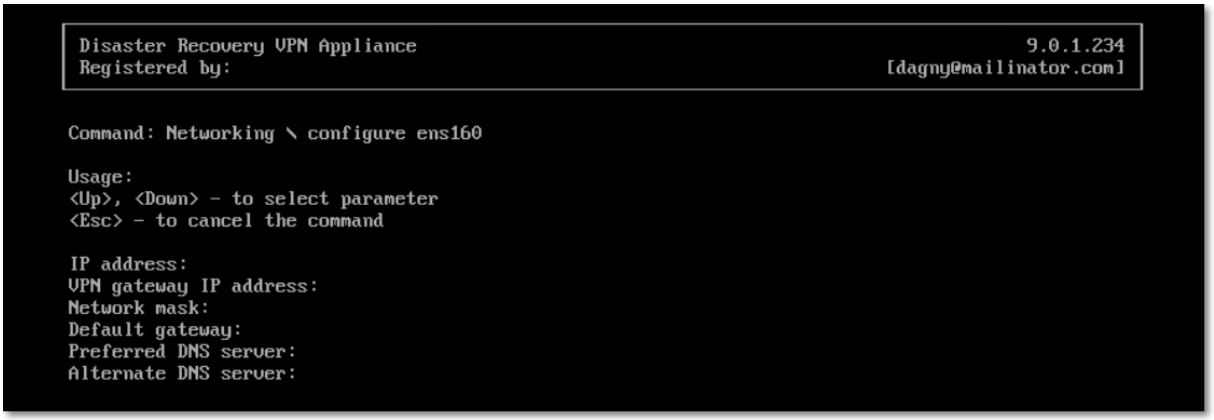
1. Inicie sesión en la consola del dispositivo VPN.
2. En la sección **Redes**, seleccione la interfaz que desea eliminar y haga clic en **Borrar configuración de red**.
3. Confirme la operación.

Como resultado, se detendrá la extensión de red local al cloud mediante un túnel de VPN seguro. Esta red funcionará como un segmento del cloud independiente. Si esta interfaz se usa para pasar el tráfico desde (hacia) el sitio en el cloud, todas sus conexiones de red de (hacia) el sitio en el cloud se desconectarán.

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 dos opciones disponibles:
   - Para la configuración automática de la red mediante DHCP, haga clic en **Usar DHCP**. Confirme la operación.
   - Para la configuración manual de la red, haga clic en **Definir dirección IP estática**. Se pueden editar as siguientes opciones de configuración:
     - **Dirección IP**: la dirección IP de la interfaz en la red local.
     - **Dirección IP de puertas de enlace de VPN**: la dirección IP específica que se reserva para el segmento en la nube de la red para que el servicio de Cyber Disaster Recovery Cloud funcione correctamente.

- **Máscara de red**: máscara de red de la red local.
- **Entrada por defecto**: entrada predeterminada en el sitio local.
- **Servidor DNS preferido**: servidor DNS principal del sitio local.
- **Servidor DNS alternativo**: servidor DNS secundario del sitio local.



- Realice los cambios necesarios y confírmelos al pulsar la tecla Entrar.

Modo solo en la nube

Puede tener hasta 23 redes en la nube.

Para agregar una nueva red al cloud:

1. Vaya a **Recuperación ante desastres** > **Conectividad**.
2. En el **Sitio en la nube**, pulse **Añadir red en la nube**.
3. Defina los parámetros de red en el cloud: la máscara y dirección de red. Haga clic en **Listo** cuando tenga todo a punto.

Como resultado, la red en el cloud adicional se creará en el sitio en el cloud con la máscara y dirección definidas.

Para eliminar una red en el cloud:

Nota
No puede eliminar una red en la nube si hay al menos un servidor en la nube en ella. Primero elimine el servidor en el cloud y después, la red.

1. Vaya a **Recuperación ante desastres** > **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.

Para cambiar los parámetros de la red en el cloud:

1. Vaya a **Recuperación ante desastres** > **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**.

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 **Recuperación ante desastres** > **Conectividad**.

A continuación se enumeran algunos motivos conocidos para la incoherencia entre direcciones IP:

1. Se migró un servidor de recuperación de una red a otra, o se modificó la máscara de la red en el cloud. Como resultado, los servidores en el cloud 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 este escenario, consulte Cambio de conexiones y Reasignación de direcciones IP.
4. Editar los siguientes parámetros de red en el sitio del dispositivo VPN:
   - 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, su estado 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 **Cambiar**, 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 si no hay redes en la que existentes a los 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**.

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 consola de Cyber Protect (**Recuperación ante desastres** > **Conectividad**), puede hacer lo siguiente:

- 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** en el 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).

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 **Recuperación ante desastres** > **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**.

Habilitar y deshabilitar la conexión de sitio a sitio

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

Puede habilitar la conexión 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 conexión de sitio a sitio:

1. Vaya a **Recuperación ante desastres** > **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 Cyber Disaster Recovery Cloud obtiene la configuración de red del dispositivo VPN y extiende las redes locales al sitio en la nube.

Si no necesita que los servidores en la nube del sitio en la nube se comuniquen con los servidores en el sitio local, puede deshabilitar la conexión de sitio a sitio.

Para deshabilitar la conexión de sitio a sitio:

1. Vaya a **Recuperación ante desastres** > **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.

Cambio de tipo de conexión de sitio a sitio

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

	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 **Recuperación ante desastres** -> **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.

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 **Recuperación ante desastres** -> **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.

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).

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.

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
   Cyber Disaster Recovery Cloud 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**.

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, Cyber Disaster Recovery Cloud 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

1. En la consola de Cyber Protect, vaya a **Recuperación ante desastres** > **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 **Añadir** 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, Cyber Disaster Recovery Cloud 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 **Recuperación ante desastres** > **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 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 **Recuperación ante desastres** > **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.

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 Recuperación ante desastres, 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.

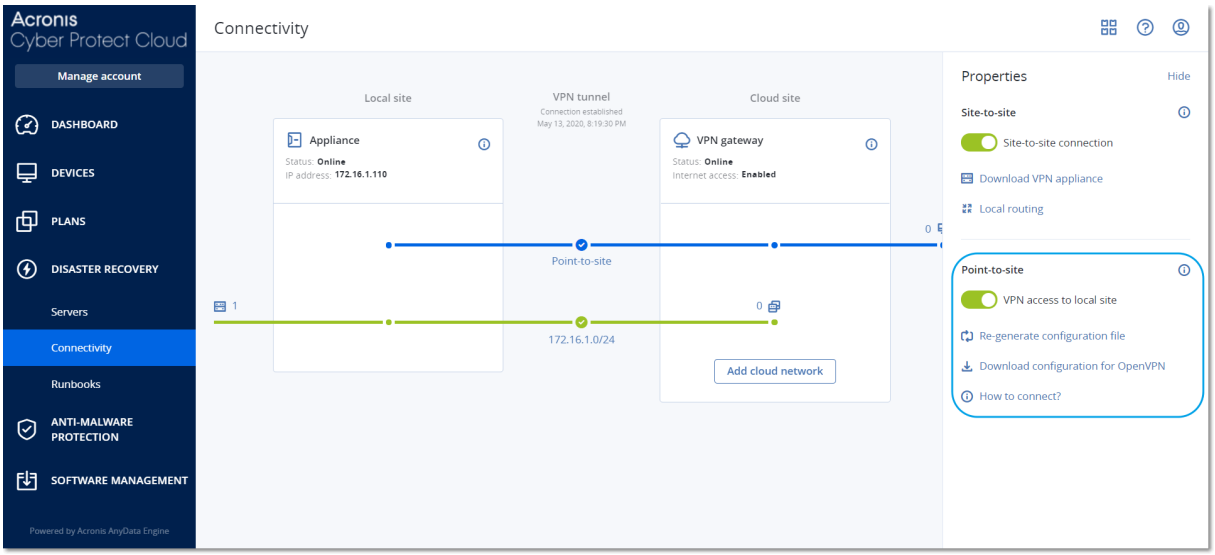
Para permitir el tráfico DHCP a través de la conexión VPN L2

1. Vaya a **Recuperación ante desastres** > pestaña **Conectividad**.
2. Haga clic en **Mostrar propiedades**.
3. Habilite el conmutador **Permitir tráfico DHCP a través de VPN L2**.

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 **Recuperación ante desastres** > **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.

Esta acción es obligatoria en los siguientes casos:

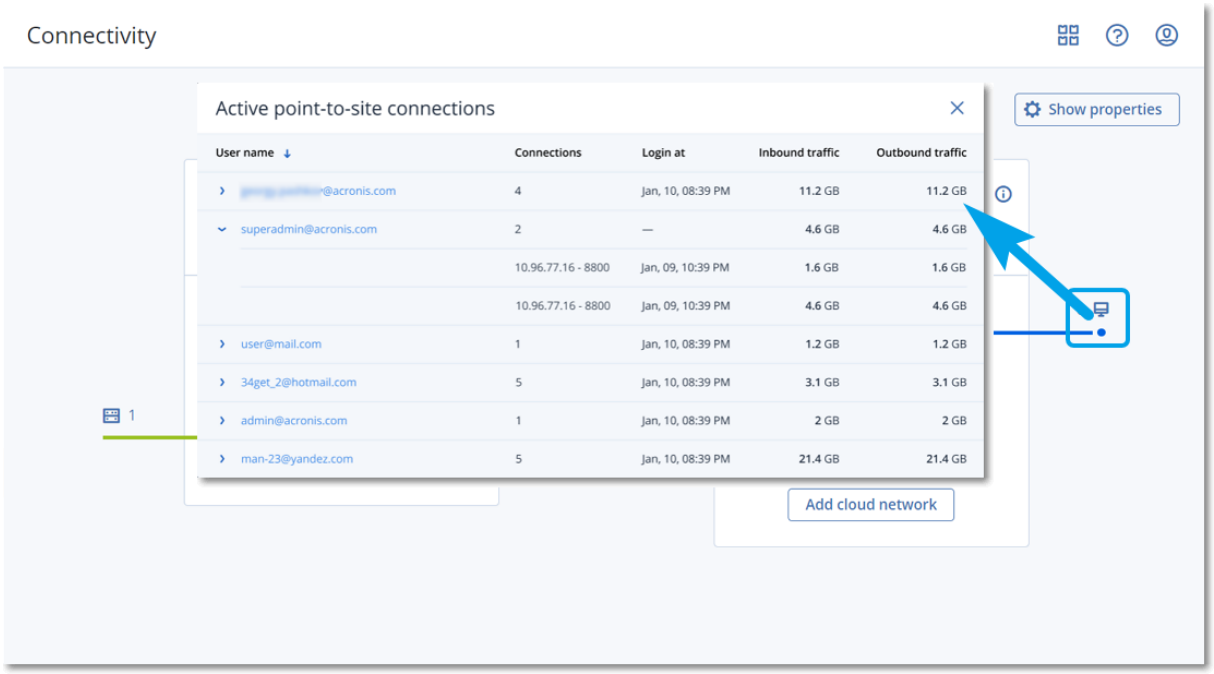
- Si cree que el archivo de configuración está en riesgo.
- Si la autenticación de doble factor estaba habilitada en su cuenta.

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.



Trabajar con registros

La recuperación ante desastres 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.

`dnsmsq.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 de firewall.

`free.txt`: El archivo contiene información sobre la memoria disponible.

`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. 823).

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. 820).
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

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, a continuación, configure los ajustes. Para obtener más información, consulte "Capturar paquetes de red" (p. 820).
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.

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.

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 **Añadir** 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.

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.

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 **Recuperación ante desastres** > **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.

Configuración de servidores de recuperación

Esta sección describe los conceptos de conmutación por error y conmutación por recuperación, la creación de un servidor de recuperación y las operaciones de recuperación ante desastres.

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 el cloud.
- 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. 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. 779).

4. Especifique la red en el cloud a la que se conectará el servidor.
5. Seleccione la opción **DHCP**.

Opción DHCP	Descripción
Proporcionado por Cloud Site	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.

6. [Opcional] 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 de recuperación siempre tenga la misma dirección IP. Puede ejecutar aplicaciones con licencias que se registran en la dirección MAC.

7. 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.

8. [Opcional] Marque la casilla de verificación de **Dirección IP de prueba** y, a continuación, especifique la dirección IP.
   Esto 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.
   Si deja la casilla de verificación desmarcada, la consola será la única forma de acceder al servidor durante una conmutación por error de prueba.

   Nota
   Si usa 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 escribir otra.
9. [Opcional] Marque la casilla de verificación de **acceso a Internet**.
   De esta forma, el servidor de recuperación tendrá acceso a Internet durante una conmutación por error de prueba o real. De forma predeterminada, el puerto TCP 25 está abierto para las conexiones de salida a direcciones IP públicas.
10. [Opcional] Establezca el **umbral de RPO**.
    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. El valor se puede establecer entre 15 y 60 minutos, 1 y 24 horas y 1 y 14 días.
11. [Opcional] Marque la casilla de verificación **Usar dirección IP pública**.
    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 deja la casilla de verificación desmarcada, el servidor solo estará disponible en su red de producción.
    La opción **Usar dirección IP pública** requiere que esté habilitada la opción **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 a direcciones IP públicas.

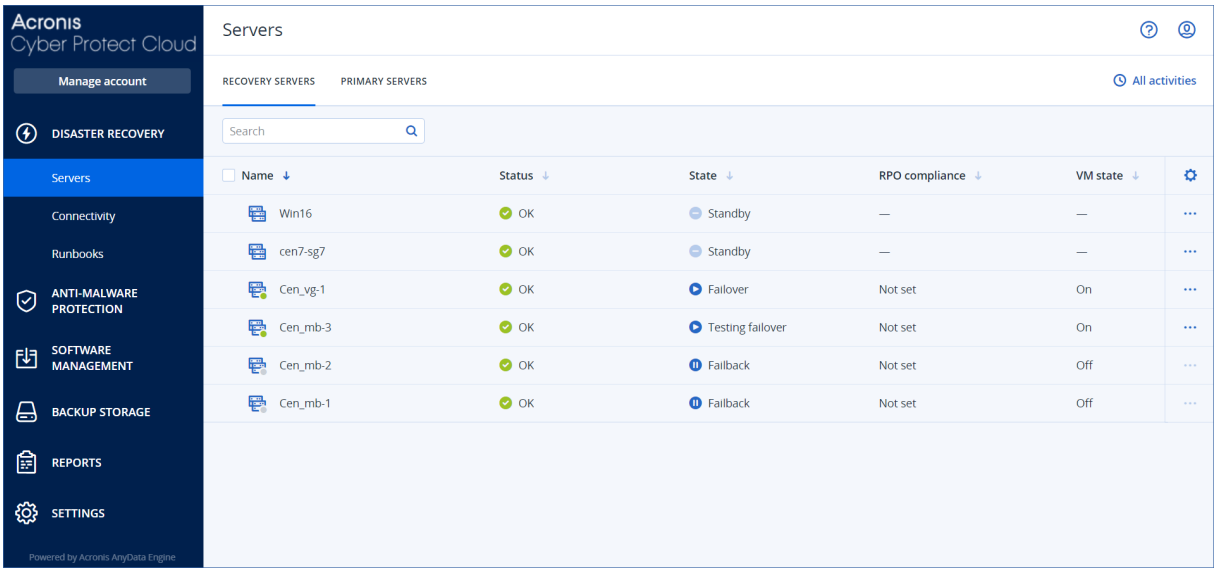
Nota
Si borra la casilla de verificación **Usar dirección IP pública** o elimina el servidor de recuperación, su dirección IP pública no se reservará.

12. [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 **Especificar**, 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. [Opcional] Para ver todas las copias de seguridad, seleccione **Mostrar todas las copias de seguridad**.
    c. Haga clic en **Listo**.

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.

13. [Opcional] Cambie el nombre del servidor de recuperación.
14. [Opcional] Escriba una descripción para el servidor de recuperación.
15. [Opcional] Haga clic en la pestaña **Reglas de cortafuegos de la nube** para editar las reglas de cortafuegos predeterminadas. Para obtener más información, consulte "Configuración de reglas de cortafuegos para servidores en la nube" (p. 854).
16. Haga clic en **Crear**.

En la consola de Cyber Protect, el servidor de recuperación aparece en la pestaña **Recuperación ante desastres** > **Servidores** > **Servidores de recuperación**. Puede ver su configuración si selecciona el equipo original y hace clic en **Recuperación ante desastres**.



Cómo funciona la conmutación por error

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.

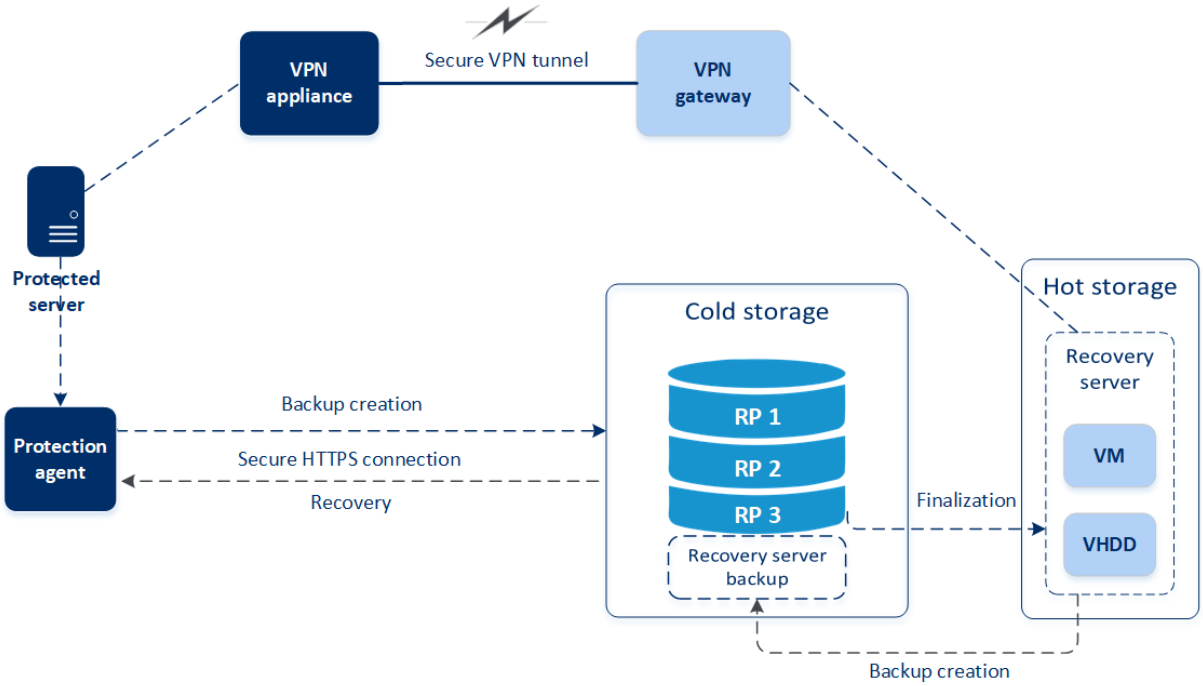
Al iniciar el proceso de conmutación por error, seleccione el punto de recuperación (copia de seguridad) del equipo original a partir del cual se creará una máquina virtual con los parámetros predefinidos. La operación de conmutación por error usa la funcionalidad "ejecutar equipo virtual a partir de 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 del equipo virtual** en la pantalla **Recuperación ante desastres** > **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.



Probar conmutación por error

Durante una **conmutación por error de prueba**, el equipo virtual no se apaga. Esto significa que el agente lee el contenido de los discos virtuales directamente desde la copia de seguridad, es decir, accede aleatoriamente a distintas partes de ella, y su rendimiento puede ser más lento de lo normal. Para obtener más información sobre el proceso de conmutación por error de prueba, consulte "Ejecución de una prueba de conmutación por error" (p. 829).

Conmutación por error de prueba automatizada

Cuando se configura la conmutación por error de prueba automatizada, se ejecuta una vez al mes sin ninguna interacción manual. Para obtener más información, consulte "Conmutación por error de prueba automatizada" (p. 831) y "Configuración de la conmutación por error de prueba automatizada" (p. 832).

Ejecución de una prueba de conmutación por error

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.

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 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 **Recuperación ante desastres**.
   Se abre la descripción del servidor de recuperación.
3. Haga clic en **Conmutación por error**.
4. Seleccione el tipo de conmutación por error **Probar conmutación por error**.
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.

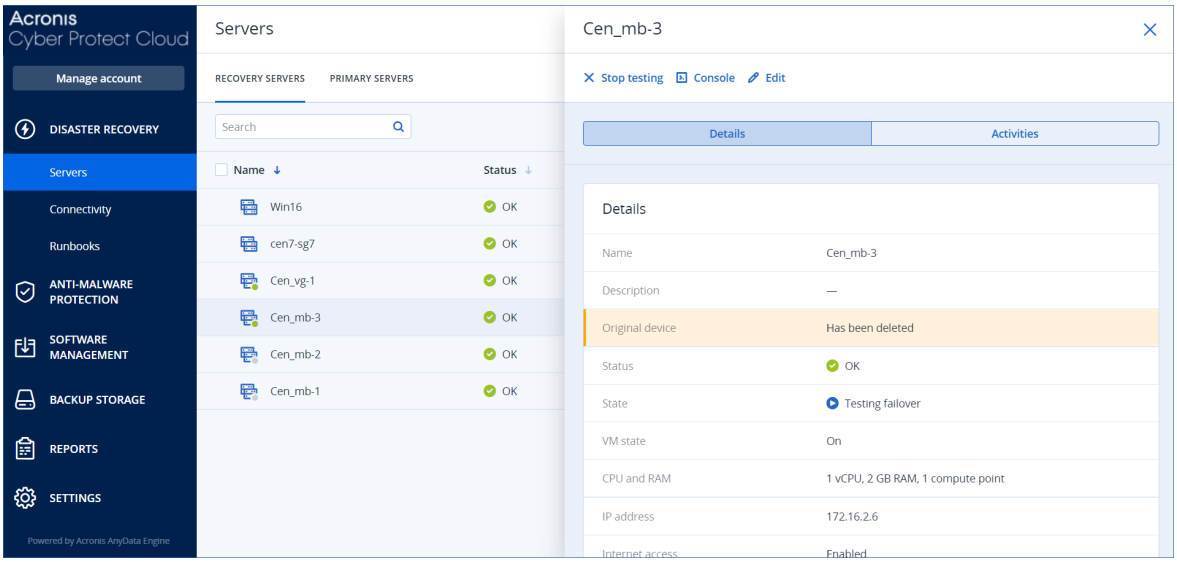
> **Nota**
> Solo se guardará la contraseña temporalmente y se utilizará para la operación de prueba de conmutación por error actual. La contraseña se eliminará automáticamente del almacén de credenciales si se detiene la prueba de conmutación por error o una vez que esta se haya completado.

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 **Recuperación ante desastres** > **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.

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.

Nota
Las acciones **Iniciar servidor** y **Detener servidor** no se aplican a las operaciones de conmutación por error de prueba ni en los runbooks ni cuando se inicia una conmutación por error de prueba manualmente. Si intenta ejecutar dichas acciones, fallarán y aparecerá el siguiente mensaje de error:
Error: La acción no es aplicable al estado actual del servidor.

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. 832).

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. 824).

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 sección **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.

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] Haga clic en **Mostrar captura de pantalla** para ver la captura de pantalla de la máquina virtual.

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.

Pasos para deshabilitar 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 sección **Conmutación por error de prueba automatizada**, en el campo **Planificación**, seleccione **Nunca**.
4. Haga clic en **Guardar**.

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 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 las instrucciones siguientes o ver el tutorial en vídeo.

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 **Recuperación ante desastres** > **Servidores** > **Servidores de recuperación** y seleccione el servidor de recuperación.
3. Haga clic en **Conmutación por error**.
4. Seleccione el tipo de conmutación por error **Conmutación por error de 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**.

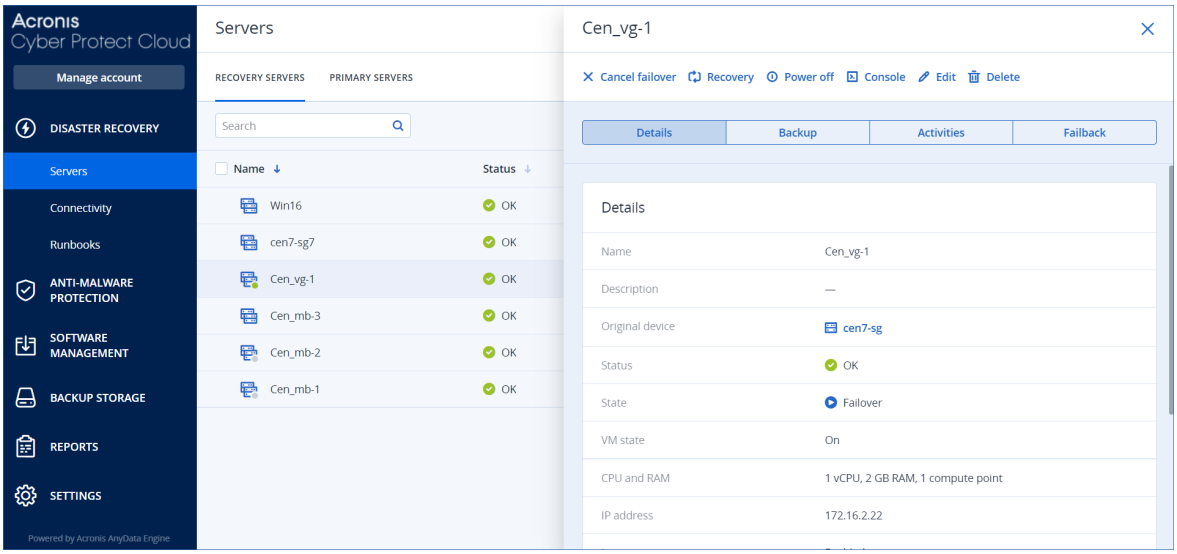
   b. [Opcional] Para guardar la contraseña de la copia de seguridad establecida y utilizarla en las siguientes operaciones de conmutación por error, seleccione la casilla de verificación **Almacenar la contraseña en un almacén de credenciales seguro...** e introduzca un nombre para las credenciales en 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 del equipo virtual** en la pantalla **Recuperación ante desastres** > **Servidores** y en la vista **Detalles** del servidor. Para obtener más información, consulte "Cómo funciona la conmutación por error" (p. 827).



7. Mire la consola del servidor de recuperación para asegurarse de que se ha iniciado. Haga clic en **Recuperación ante desastres** > **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".

Si quiere cancelar la conmutación por error, seleccione el servidor de recuperación y haga clic en **Cancelar conmutación por error**. Se perderán todos los cambios que se hayan realizado desde el momento de la conmutación por error, excepto las copias de seguridad de los servidores de recuperación. El servidor de recuperación volverá al estado **En espera**.

Si quiere llevar a cabo una conmutación tras recuperación, seleccione el servidor de recuperación y haga clic en **Conmutación tras recuperación**.

Cómo realizar una conmutación por error de servidores mediante DNS local

Si usa los servidores DNS en el sitio local para resolver nombres de máquina, en ese caso, después de una conmutación por error los servidores de recuperación, correspondiente a las máquinas que dependen de DNS, no se comunicarán porque los servidores DNS usan en el cloud son distintos. De forma predeterminada, los servidores DNS del sitio de cloud se usan para los servidores de cloud recién creados. Si necesita aplicar configuración de DNS personalizada, póngase en contacto con el equipo de soporte técnico.

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.
- 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.

Cómo funciona la 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 de destino en su sitio local. Durante la conmutación tras recuperación, la máquina virtual en la nube sigue funcionando mientras se transfieren los datos de la copia de seguridad al sitio local. Esta tecnología le ayuda a conseguir un tiempo de inactividad muy corto, que se estima 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 futuro tiempo de inactividad.

El proceso de conmutación tras recuperación es ligeramente diferente si el destino es una máquina virtual o un equipo físico. Para obtener más información sobre las fases del proceso de conmutación por recuperación, consulte "Conmutación por recuperación en una máquina virtual de destino" (p. 837) y "Conmutación por recuperación en una máquina física de destino" (p. 842).

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. 846).

Nota

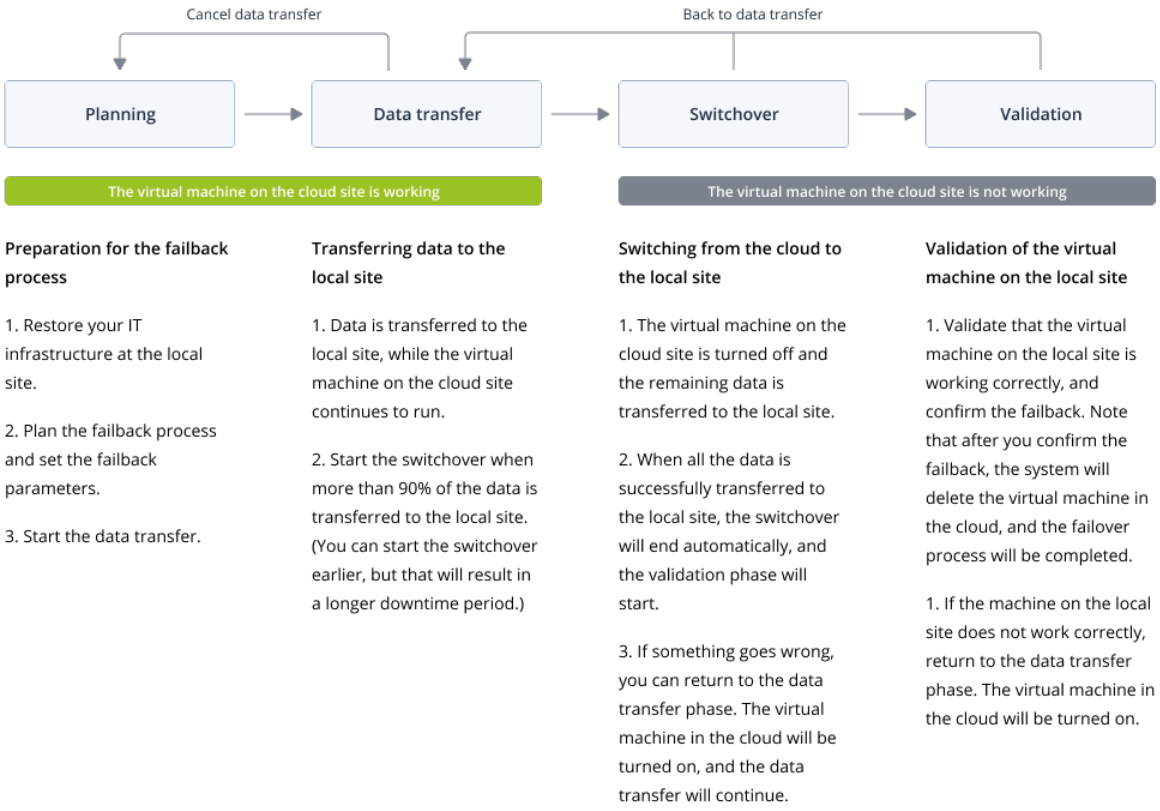
Las operaciones de runbook solo admiten la conmutación tras recuperación en el modo manual. Esto significa que, si inicia el proceso de conmutación tras recuperación mediante la ejecución de un runbook que incluya un paso **Servidor de conmutación tras recuperación**, el procedimiento requerirá una interacción manual: deberá recuperar el equipo de forma manual y confirmar o cancelar el proceso de conmutación tras recuperación desde la pestaña **Recuperación ante desastres** > **Servidores**.

Conmutación por recuperación en una máquina virtual de destino

Nota

La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

El proceso de conmutación por recuperación de una máquina virtual de destino consta de cuatro 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.

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.

   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.

Ejecución de la conmutación por recuperación en un equipo virtual

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

Puede ejecutar una conmutación por recuperación en un equipo virtual de destino en su 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.
- 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 virtual

1. En la consola de Cyber Protect, vaya a **Recuperación ante desastres** > **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** seleccione **Equipo virtual** como **Destino**, y configure el resto de 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.

Parámetro	Descripción
	Nota El valor de la velocidad de su conexión a Internet se reducirá si realiza varios procesos de conmutación por recuperación al mismo tiempo.
Destino	Tipo de carga de trabajo en su sitio local en el que recuperará el servidor en la nube: **Equipo virtual** o **Equipo físico**.
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 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.

Parámetro	Descripción
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**.

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.

Campo	Descripción
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**.

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 por recuperación en una máquina física de destino

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

El proceso de conmutación tras recuperación automática en un equipo físico de destino consiste en las fases siguientes:

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.

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 físico del sitio local estará listo y podrá reiniciarlo con un dispositivo de arranque basado en Linux. Verifique 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.

Ejecución de conmutación por recuperación en una máquina física

Nota

La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

Puede ejecutar una conmutación tras recuperación automática en un equipo físico 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 físico 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 **Recuperación ante desastres** > **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. 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 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:

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 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

1. En la consola de Cyber Protect, vaya a **Recuperación ante desastres** > **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**.

Trabajando con copias de seguridad cifradas

Puede crear servidores de recuperación a partir de las copias de seguridad cifradas. Para su comodidad, puede configurar una aplicación de contraseña automática para una copia de seguridad cifrada durante la conmutación por error de un servidor de recuperación.

Al crear un servidor de recuperación, puede especificar la contraseña para su uso para operaciones de recuperación ante desastres automáticas. Se guardará en el Almacén de credenciales, un almacenamiento seguro de credenciales que puede encontrarse en la sección **Configuración** > **Credenciales**.

Una credencial puede estar vinculada a varias copias de seguridad.

Para gestionar las contraseñas guardadas en el Almacén de credenciales

1. Vaya a **Configuración** > **Credenciales**.
2. Para gestionar una credencial específica, haga clic en el icono en la última columna. Puede ver los elementos enlazados a esta credencial.
   - Para desvincular la copia de seguridad de la credencial seleccionada, haga clic en el icono de papelera de reciclaje cerca de la copia de seguridad. Como resultado, tendrá que especificar la contraseña de forma manual durante la conmutación por error al servidor de recuperación.
   - Para editar la credencial, haga clic en **Editar** y, a continuación, especifique el nombre o contraseña.
   - Para eliminar la credencial, haga clic en **Eliminar**. Tenga en cuenta que tendrá que especificar la contraseña de forma manual durante la conmutación por error al servidor de recuperación.

Operaciones con máquinas virtuales de Microsoft Azure

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

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. 833).

Después de eso, puede ejecutar la conmutación tras recuperación de Acronis Cyber Protect Cloud a las máquinas virtuales de Azure. El proceso de conmutación tras recuperación es igual al de un equipo físico. Para obtener más información, consulte "Requisitos previos" (p. 844).

Nota
Para registrar una nueva máquina virtual de Azure para la conmutación tras recuperación, puede usar la extensión Acronis Backup VM disponible en 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. 798).

Configuración de servidores principales

En esta sección se describe cómo crear y administrar sus servidores principales.

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 **Recuperación ante desastres** > **Servidores** > **Servidores principales**.
2. Haga clic en **Crear**.
3. Seleccione una plantilla para el nuevo equipo virtual.
4. 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	1000
F3	2	8	2000
F4	4	16	4000
F5	8	32	8000
F6	16	64	16000
F7	16	128	32000
F8	16	256	64000

Nota
Puede ver los puntos de cálculo para cada opción. El número de puntos de cálculo indican el coste de funcionamiento del servidor principal por hora. Para obtener más información, consulte "Puntos de cálculo" (p. 779).

5. [Opcional] Cambie el tamaño de las unidades de discos virtuales. Si necesita más de un disco rígido, haga clic en **Agregar disco** y, a continuación, especifique el nuevo disco. Actualmente no puede añadir más de 10 discos en un servidor principal.
6. Especifique la red de cloud en la que se incluirá el servidor principal.
7. Seleccione la opción **DHCP**.

Opción DHCP	Descripción
Proporcionado por Cloud Site	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.

8. [Opcional] 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.
9. 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.

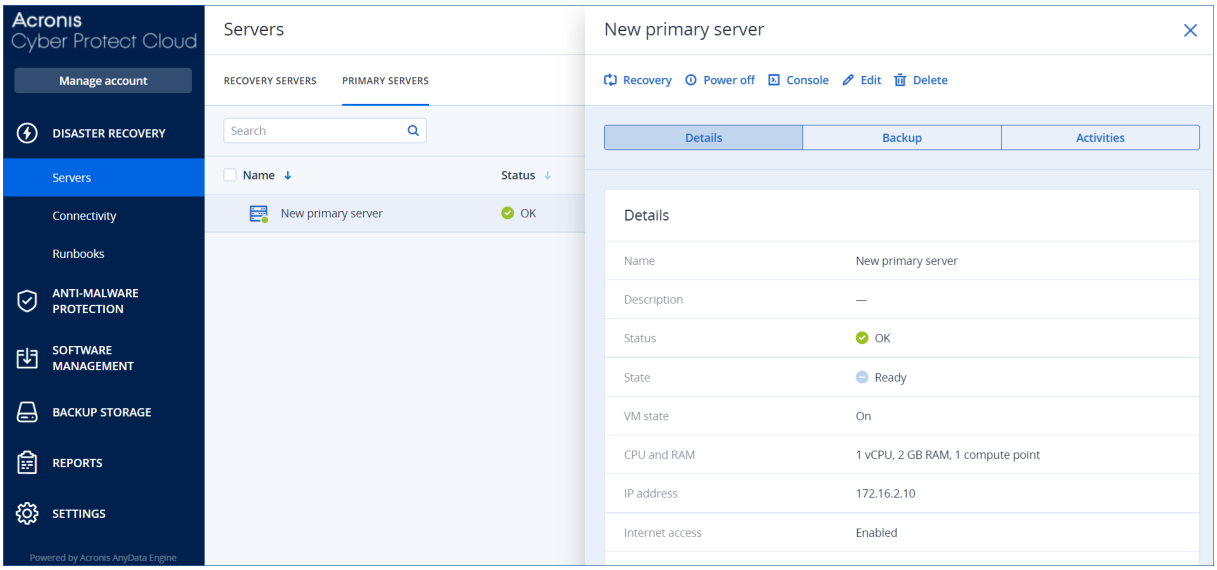
10. [Opcional] Marque la casilla de verificación de **acceso a Internet**.
    De esta forma, el servidor principal tendrá acceso a Internet. De forma predeterminada, el puerto TCP 25 está abierto para las conexiones de salida a direcciones IP públicas.
11. [Opcional] Marque la casilla de verificación **Usar dirección IP pública**.
    El hecho de que el servidor principal cuente con una dirección IP pública conlleva que se pueda acceder a él desde Internet. Si deja la casilla de verificación desmarcada, el servidor solo estará disponible en su red de producción.

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.

12. [Opcional] Seleccione **Establecer el umbral de RPO**.
    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.
13. Defina el nombre del servidor principal.
14. [Opcional] Especifique una descripción para el servidor principal.
15. [Opcional] Haga clic en la pestaña **Reglas de cortafuegos de la nube** para editar las reglas de cortafuegos predeterminadas. Para obtener más información, consulte "Configuración de reglas de cortafuegos para servidores en la nube" (p. 854).
16. 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 un servidor principal

El servidor principal aparece en la pestaña **Recuperación ante desastres** > **Servidores** > **Servidores principales** de la consola de Cyber Protect.

Para iniciar o detener el servidor, haga clic en **Encender** o **Apagar** en el panel del servidor principal.

Para editar la configuración del servidor principal, deténgalo y haga clic en **Editar**.

Para aplicar un plan de protección al servidor principal, selecciónelo en la pestaña **Plan** y haga clic en **Crear**. Verá un plan de protección predefinido en el que 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".

Gestión de servidores en el cloud

Para gestionar servidores en el cloud, vaya a **Recuperación ante desastres** > **Servidores**. Allí encontrará dos pestañas: **Servidores de recuperación** y **Servidores principales**. Para mostrar todas las columnas opcionales en 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
Último punto de recuperación	La fecha y la hora en las que se creó el último punto de recuperación.

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 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 **Recuperación ante desastres** > **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:
   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**

Parámetro de cortafuegos	Descripción
	• **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.

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 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 de firewall 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.

Realización de copias de seguridad de servidores en la cloud

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.

Organización (runbooks)

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

Un runbook es un conjunto de instrucciones que describen cómo iniciar el entorno de producción en la nube. Puede crear runbooks en la consola de Cyber Protect. Para acceder a la pantalla **Runbooks**, seleccione **Recuperación ante desastres** > **Runbooks**.

¿Por qué usar runbooks?

Con los runbooks, puede:

- Automatizar una 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.

Creación de un runbook

Un runbook consiste en pasos que se ejecutan consecutivamente. Un paso consiste en acciones que comienzan simultáneamente.

Puede seguir las instrucciones siguientes o ver el tutorial en vídeo.

Para crear un runbook

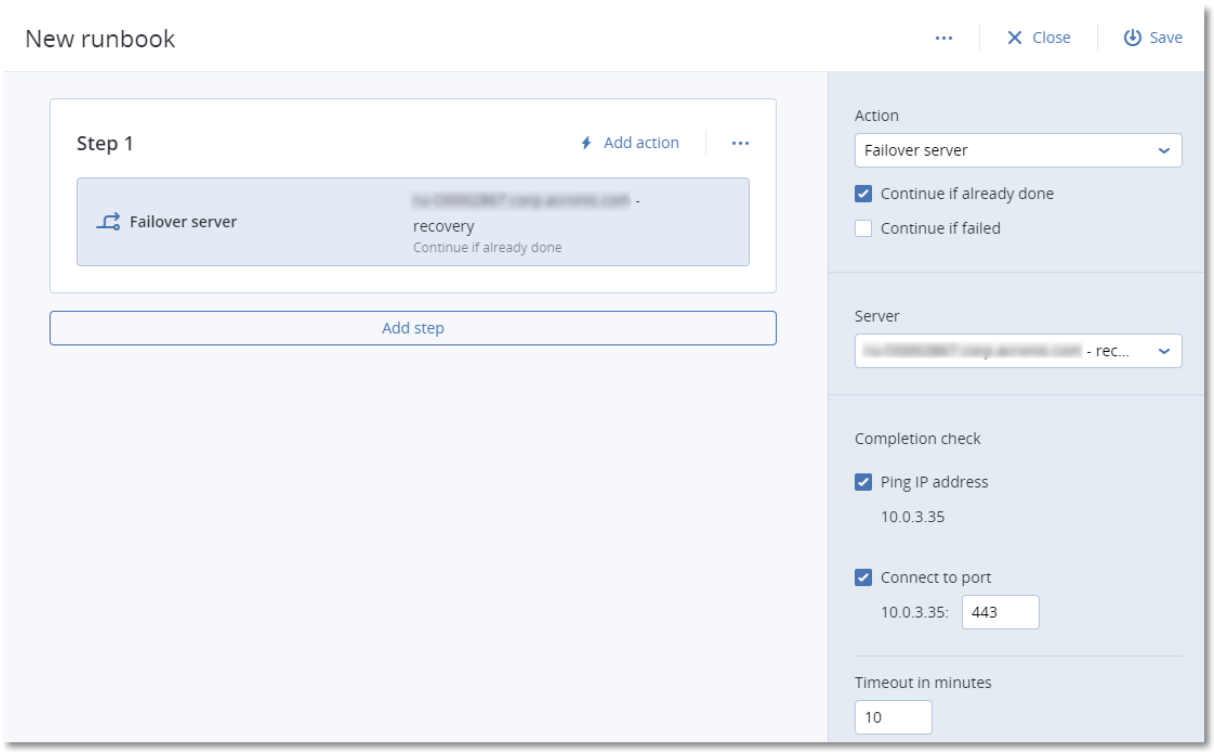
1. En la consola de Cyber Protection, vaya a **Recuperación ante desastres** > **Runbooks**.
2. Haga clic en **Crear runbook**.
3. Haga clic en **Añadir paso**.
4. Haga clic en **Añadir acción** y seleccione la acción que quiere añadir al paso.

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. 861).

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 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. 861). **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 **Recuperación ante desastres** > **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. 861). **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. 861). **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.

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. 861).
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.

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.

Parámetro de runbook	Categoría	Disponible para actuar	Descripción
			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.
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.

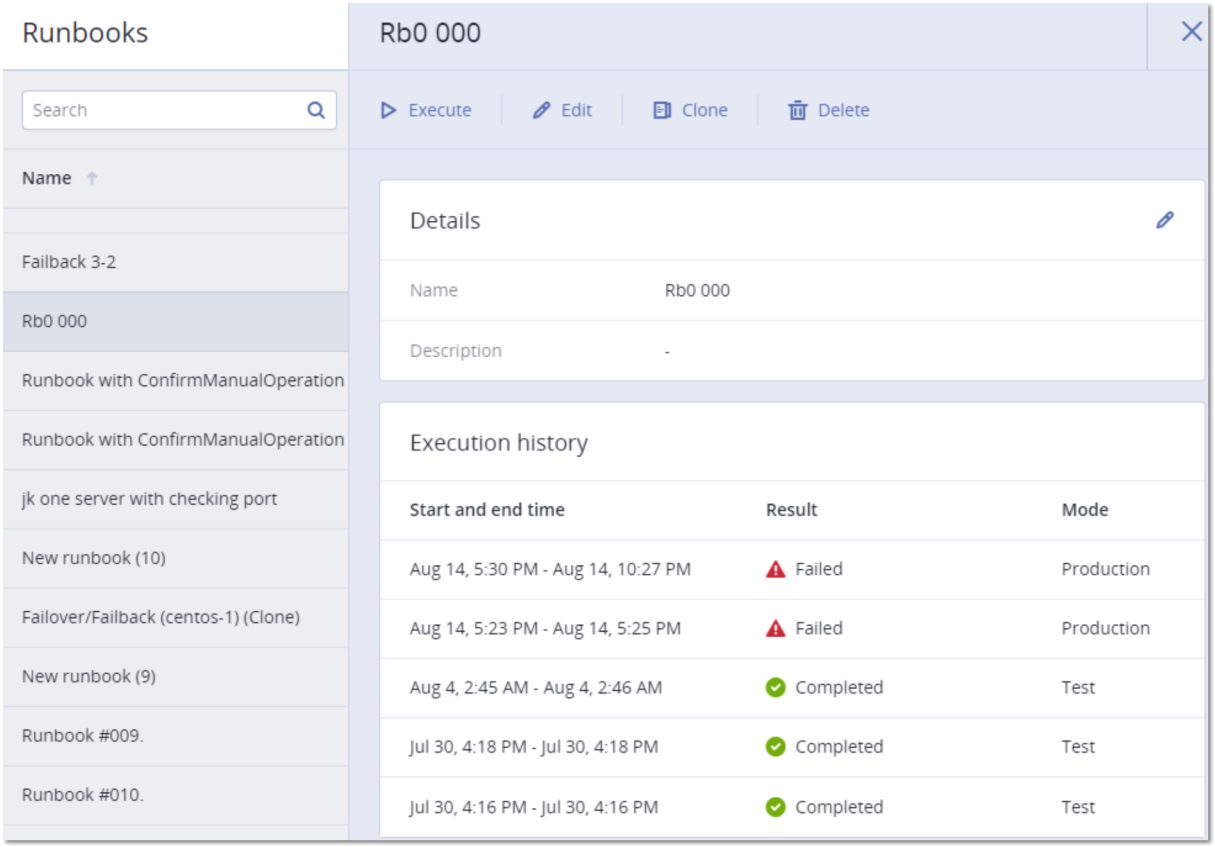
- **Modo conmutación por error y conmutación por recuperación**
  Elija si quiere ejecutar una conmutación por error de prueba (opción predeterminada) o una real (producción). El modo de conmutación por recuperación se corresponderá con el modo de conmutación por error elegido.
- **Punto de recuperación 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.

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.



Configuración de la protección antivirus y antimalware

Nota
En las máquinas Windows, la función de protección antimalware requiere la instalación del agente de protección antimalware y la función de filtrado de URL requiere la instalación del agente para el filtrado de URL. Estos agentes se instalan automáticamente en el caso de las cargas de trabajo protegidas si los módulos de **Protección antivirus y antimalware** o **Filtrado de URL** están habilitados 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.

Plataformas compatibles

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

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
macOS	macOS 10.13.x y posterior

Funciones compatibles por plataforma

Nota
La protección antimalware para Linux y macOS está disponible con el paquete de antimalware avanzado.

Conjunto de características	Windows	Linux	macOS
Protección antivirus y antimalware			
Funcionalidad Active Protection integrada por completo	Sí	No	No
Protección contra malware en tiempo real	Sí	Sí, con el pack de antimalware avanzado	Sí, con el pack de antimalware avanzado
Protección contra malware en tiempo real avanzada con detección basada en firmas locales	Sí	Sí	Sí

Conjunto de características	Windows	Linux	macOS
Protección antivirus y antimalware			
Análisis estadístico para archivos ejecutables portátiles	Sí	No	Sí*
Análisis antimalware bajo demanda	Sí	Sí**	Sí
Protección de carpetas de red	Sí	Sí	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	Sí***
Exclusiones de procesos	Sí	No	Sí
Motor de análisis de comportamiento	Sí	No	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 firewall****	Sí	No	No
Gestión del antivirus Microsoft Defender*****	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
Para obtener más información sobre los sistemas operativos y sus versiones, consulte "Plataformas compatibles" (p. 865).			

* En macOS, el análisis estadístico para archivos ejecutables portátiles solo se admite en los análisis programados.

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

*** En macOS, las exclusiones de archivos y carpetas solo se admiten cuando especifica los archivos y las carpetas que no se analizarán mediante la protección en tiempo real ni a través de análisis planificados.

**** La gestión del firewall es compatible con Windows 8 y versiones posteriores. Windows Server no es compatible.

***** La gestión del antivirus Windows Defender es compatible con Windows 8.1 y versiones posteriores.

Conjunto de características	Windows	Linux	macOS
Active Protection			
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
Protección de carpetas de red	Sí	Sí	Sí
Protección del servidor	Sí	No	No
Protección de Zoom, Cisco Webex, Citrix Workspace y Microsoft Teams	Sí	No	No
Para obtener más información sobre los sistemas operativos y sus versiones, consulte "Plataformas compatibles" (p. 865).			

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 "Plataformas compatibles" (p. 865).

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.

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.
- **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. 223).

Se pueden configurar las siguientes funciones en el módulo de protección antivirus y antimalware para un plan de protección:

- "Active Protection" (p. 871)
- "Antimalware avanzado" (p. 872)

- "Protección de carpetas de red" (p. 872)
- "Protección del servidor" (p. 873)
- "Autoprotección" (p. 874)
- "Detección del proceso de criptominería" (p. 875)
- "Cuarentena" (p. 876)
- "Motor de comportamiento" (p. 876)
- "Prevención de vulnerabilidades" (p. 877)
- "Protección en tiempo real" (p. 879)
- "Planificar análisis" (p. 880)
- "Exclusiones de protección" (p. 883)

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 "Plataformas compatibles" (p. 865). Algunas funciones requieren una licencia específica para estar disponibles en su plan de protección.

Active Protection

Active Protection protege su sistema del software malicioso conocido como ransomware, el cual cifra los archivos y pide un rescate para obtener la clave de cifrado.

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 "Plataformas compatibles" (p. 865).

Pasos para configurar Active Protection

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:

   Configuración predeterminada: **Revertir usando la caché**

   - **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.

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.

Importante
Esta función solo está disponible si tiene el paquete de protección Advanced Security habilitado. Para obtener más información, consulte https://www.acronis.com/es-es/products/cloud/cyber-protect/security/

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.

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 **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.

Configuración predeterminada: **Apagado**.

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 **Añadir** 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`.
7. En el campo **Nombre del host**, escriba el nombre del host 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 **Añadir** 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 host**, escriba el nombre del host 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.

Para habilitar la Protección con contraseña

1. Una vez que se haya habilitado la función **Autoprotección**, puede marcar el conmutador de la opción **Protección con contraseña** para habilitarla.
2. Haga clic en **Generar nueva contraseña** para generar una contraseña que le permite modificar o eliminar agentes locales.
3. Haga clic en **Copiar** y péguela en un lugar seguro, ya que se le solicitará cuando quiera modificar la lista de componentes localmente.

   Importante
   La contraseña no estará disponible cuando cierre la ventana. Para aplicar esta contraseña a los dispositivos, debe guardar la configuración del plan de protección.

4. Haga clic en **Cerrar**.

La **protección con contraseña** evita que un software o usuario no autorizado desinstale el agente para Windows o modifique sus componentes. Estas acciones solo se pueden realizar con una contraseña provista por un administrador.

Las siguientes acciones nunca requieren contraseña:

- Actualizar la instalación mediante la ejecución local del programa de instalación.
- Actualizar la instalación mediante el uso de la consola de Cyber Protect
- Reparar la instalación.

Configuración predeterminada: **Deshabilitado**

Para obtener más información acerca de cómo habilitar la **protección con contraseña**, consulte Evitar la desinstalación o modificación de agentes no autorizadas.

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**.

Nota
La detección del proceso de criptominería no es compatible con Linux.

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 **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.
   - **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.

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**.

Nota
El motor de comportamiento no es compatible con Linux.

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.

Prevención de vulnerabilidades

Importante
Esta función solo está disponible si tiene el paquete de protección Advanced Security habilitado. Para obtener más información, consulte https://www.acronis.com/es-es/products/cloud/cyber-protect/security/

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 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.

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 los archivos cuyas extensiones son .tibx, .tib o .tia y que se encuentran en carpetas locales.

Con esta configuración, puede especificar los procesos que se siguen para modificar los archivos incluidos en la copia de seguridad, aunque estén protegidos por la autoprotección. Esto es útil, por ejemplo, si elimina archivos de copia de seguridad o los traslada a una ubicación diferente con una secuencia de comandos.

Si esta configuración está deshabilitada, solo los procesos firmados por el proveedor del software de la copia de seguridad pueden modificar los archivos incluidos en ella. Así, el software puede aplicar reglas de retención y eliminar copias de seguridad cuando un usuario lo solicite desde la interfaz web. Otros procesos no podrán llevar a cabo modificaciones en ellas, sin importar si son sospechosos o no.

Si esta configuración está habilitada, puede permitir que otros procesos modifiquen las copias de seguridad. Especifique la ruta completa al ejecutable del proceso, empezando por la letra de unidad de disco.

Configuración predeterminada: **Deshabilitado**.

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**.

Importante
Esta función solo está disponible si tiene el paquete de protección Advanced Security habilitado. Para obtener más información, consulte https://www.acronis.com/es-es/products/cloud/cyber-protect/security/

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.

   - **Bloquear y notificar**

     El software bloquea el proceso y genera una alerta del proceso sospechoso de actividades de malware.

   - **Cuarentena**
4. El software genera una alerta, detiene el proceso y traslada el archivo ejecutable a la carpeta de cuarentena.
5. 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.

6. 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.

> **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: • **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.

Campo	Descripción
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 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**

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.

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 sabrá que debe excluir esos procesos de la supervisión. **Nota** Los procesos firmados por Microsoft siempre son de confianza. Por ejemplo, si añade la ruta C:\Users\user1\application\nppInstaller.exe, este proceso específico se excluirá de la supervisión y el antivirus no interferirá con dicho proceso.
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. Abra el plan de protección.
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 **Añadir** 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. En la sección **Descripción**, escriba una breve descripción para que pueda reconocer el cambio en la lista de elementos de confianza.
  - 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:\carpeta\, /inicio/Carpeta/carpeta2, 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.

    Nota
    Especifique la ruta completa al ejecutable del proceso, empezando por la letra de unidad de disco. Por ejemplo, `C:\Windows\Temp\er76s7sdkh.exe`.

    Nota
    Se admiten rutas de red local. Por ejemplo, \\localhost\folderpath\file.exe

- Seleccione la opción **Hash** para añadir hash MD5 a la lista de elementos de confianza. Se mostrará 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.

Configuración predeterminada: no se define ninguna exclusión de forma predeterminada.

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**.

   En la sección **Elementos bloqueados**, haga clic en **Añadir** para seleccionar 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. En el campo **Descripción**, escriba una breve descripción para que pueda reconocer el cambio en la lista de elementos bloqueados.

     Nota
     Estos procesos no podrán iniciarse mientras Active Protection esté habilitado en el equipo.

- Para bloquear hash, seleccione la opción **Hash**. Se mostrará la ventana **Añadir hash**.
  - En el campo **Hash**, escriba el hash de cada proceso en una nueva línea. En el campo **Descripción**, escriba una breve descripción para que pueda reconocer el cambio en la lista de elementos bloqueados.

Configuración predeterminada: no se define ninguna exclusión de forma predeterminada.

Comodines

Para especificar carpetas, puede utilizar los caracteres comodín * y ?. El asterisco (*) sustituye a cero o más caracteres. La interrogación (?) sustituye exactamente a un carácter. No se pueden usar 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\

Variables

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\

Descripción

Puede usar el campo **Descripción** para introducir notas sobre las exclusiones añadidas en la lista de exclusiones de protección. A continuación, puede ver algunas sugerencias de notas que puede añadir:

- Motivo y objetivo de la exclusión.
- Nombre del archivo actual de una exclusión hash.
- La fecha y la hora.

Si se añaden varios elementos en una única entrada, solo podrá haber 1 comentario para todos los elementos.

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.

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 "Plataformas compatibles" (p. 865).

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:

- **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**.

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.

Para habilitar la Protección con contraseña

1. Una vez que se haya habilitado la función **Autoprotección**, puede marcar el conmutador de la opción **Protección con contraseña** para habilitarla.
2. Haga clic en **Generar nueva contraseña** para generar una contraseña que le permite modificar o eliminar agentes locales.
3. Haga clic en **Copiar** y péguela en un lugar seguro, ya que se le solicitará cuando quiera modificar la lista de componentes localmente.

   Importante
   La contraseña no estará disponible cuando cierre la ventana. Para aplicar esta contraseña a los dispositivos, debe guardar la configuración del plan de protección.

4. Haga clic en **Cerrar**.

La **protección con contraseña** evita que un software o usuario no autorizado desinstale el agente para Windows o modifique sus componentes. Estas acciones solo se pueden realizar con una contraseña provista por un administrador.

Las siguientes acciones nunca requieren contraseña:

- Actualizar la instalación mediante la ejecución local del programa de instalación.
- Actualizar la instalación mediante el uso de la consola de Cyber Protect
- Reparar la instalación.

Configuración predeterminada: **Deshabilitado**

Para obtener más información acerca de cómo habilitar la **protección con contraseña**, consulte Evitar la desinstalación o modificación de agentes no autorizadas.

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**.

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.

Configuración predeterminada: **Apagado**.

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 **Añadir** 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`.
7. En el campo **Nombre del host**, escriba el nombre del host 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 **Añadir** 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 host**, escriba el nombre del host 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**.

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**.

Nota
La detección del proceso de criptominería no es compatible con Linux.

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 **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.
   - **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.

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.

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 sabrá que debe excluir esos procesos de la supervisión. **Nota** Los procesos firmados por Microsoft siempre son de confianza. Por ejemplo, si añade la ruta C:\Users\user1\application\nppInstaller.exe, este proceso específico se excluirá de la supervisión y el antivirus no interferirá con dicho proceso.
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. Abra el plan de protección.
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 **Añadir** 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. En la sección **Descripción**, escriba una breve descripción para que pueda reconocer el cambio en la lista de elementos de confianza.
  - 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:\carpeta\, /inicio/Carpeta/carpeta2, 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.

    Nota
    Especifique la ruta completa al ejecutable del proceso, empezando por la letra de unidad de disco. Por ejemplo, `C:\Windows\Temp\er76s7sdkh.exe`.

    Nota
    Se admiten rutas de red local. Por ejemplo, \\localhost\folderpath\file.exe

- Seleccione la opción **Hash** para añadir hash MD5 a la lista de elementos de confianza. Se mostrará 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.

Configuración predeterminada: no se define ninguna exclusión de forma predeterminada.

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**.

   En la sección **Elementos bloqueados**, haga clic en **Añadir** para seleccionar 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. En el campo **Descripción**, escriba una breve descripción para que pueda reconocer el cambio en la lista de elementos bloqueados.

     Nota
     Estos procesos no podrán iniciarse mientras Active Protection esté habilitado en el equipo.

- Para bloquear hash, seleccione la opción **Hash**. Se mostrará la ventana **Añadir hash**.
  - En el campo **Hash**, escriba el hash de cada proceso en una nueva línea. En el campo **Descripción**, escriba una breve descripción para que pueda reconocer el cambio en la lista de elementos bloqueados.

Configuración predeterminada: no se define ninguna exclusión de forma predeterminada.

Comodines

Para especificar carpetas, puede utilizar los caracteres comodín * y ?. El asterisco (*) sustituye a cero o más caracteres. La interrogación (?) sustituye exactamente a un carácter. No se pueden usar 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\

Variables

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\

Descripción

Puede usar el campo **Descripción** para introducir notas sobre las exclusiones añadidas en la lista de exclusiones de protección. A continuación, puede ver algunas sugerencias de notas que puede añadir:

- Motivo y objetivo de la exclusión.
- Nombre del archivo actual de una exclusión hash.
- La fecha y la hora.

Si se añaden varios elementos en una única entrada, solo podrá haber 1 comentario para todos los elementos.

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.

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.

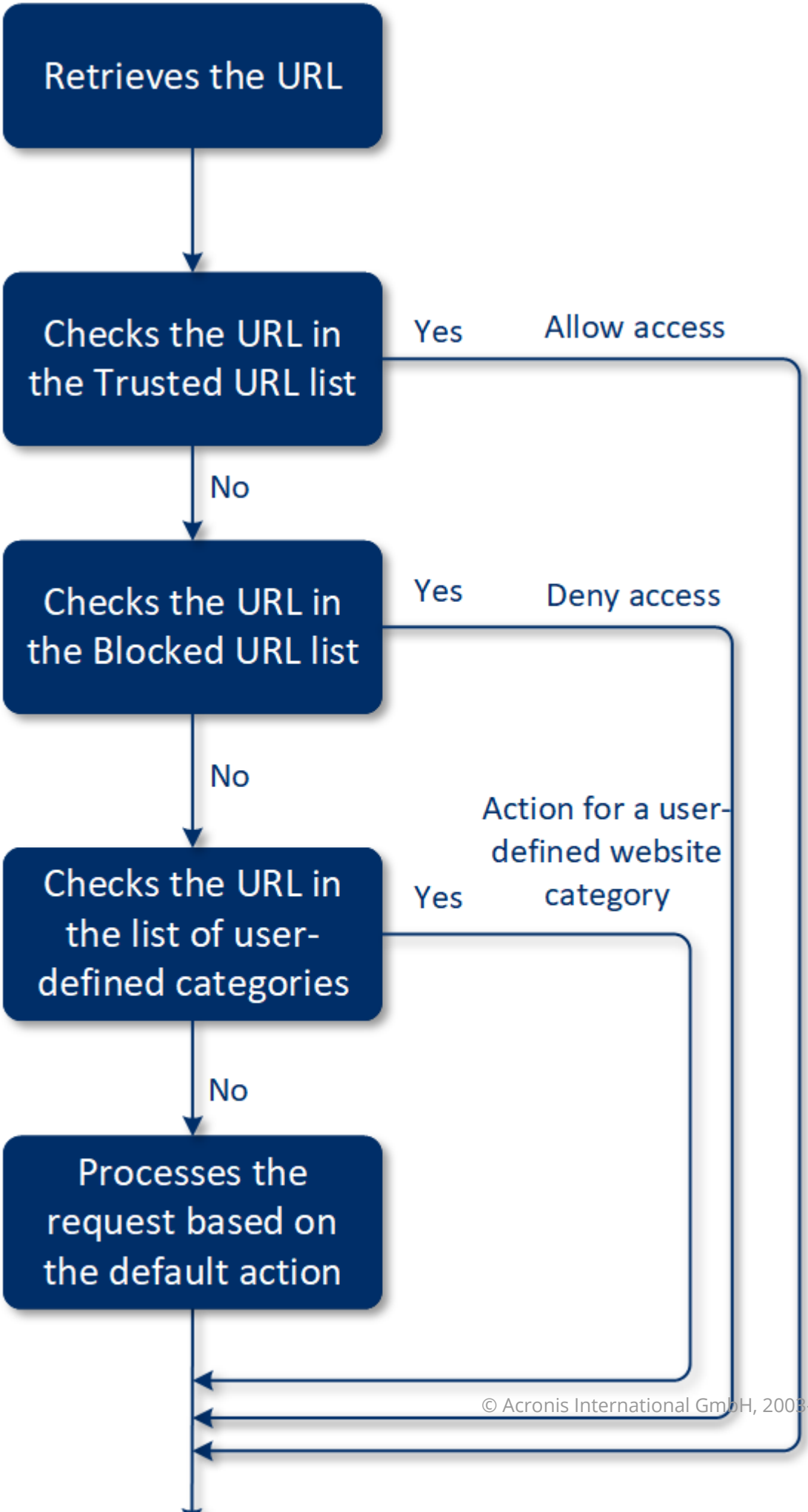
Actualmente las conexiones HTTP/HTTPS de los equipos Windows las comprueba el agente de protección.

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

Un usuario introduce el enlace de un 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 a un usuario a la página con el mensaje con distintas acciones para que continúe manualmente a la página solicitada.

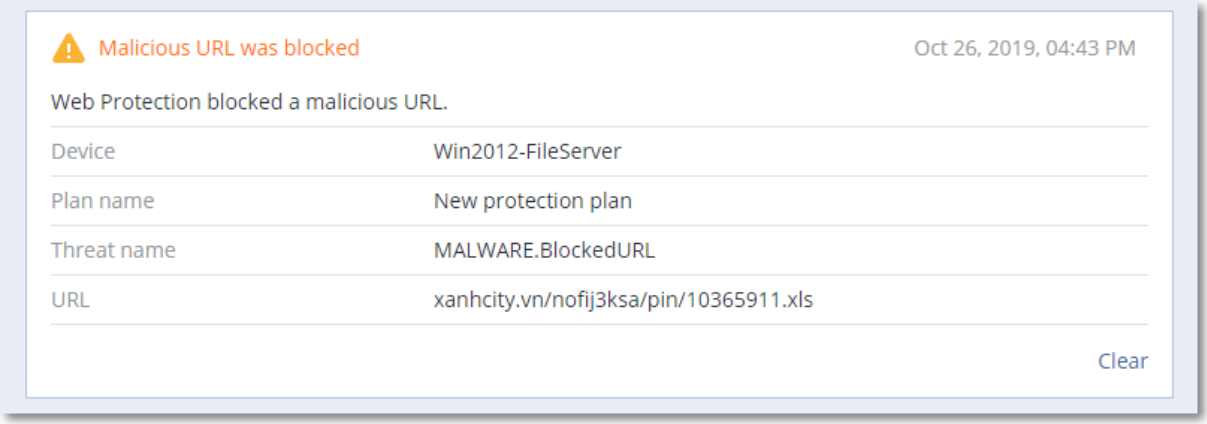


Flujo de trabajo de la configuración del filtrado de URL

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.

Mostrar todas las notificaciones de las URL bloqueadas por categorías: si esta opción está habilitada, recibirá organizadas por categorías todas las notificaciones que se muestran en la bandeja de URL bloqueadas. Si un sitio web tiene varios subdominios, el sistema también genera notificaciones para ellos, por lo que el número de notificaciones puede ser muy elevado.

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 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 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.
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.
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 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. • 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.

Pasos para especificar las URL que siempre serán de confianza o bloqueadas

1. En el módulo filtrado de URL de un plan de protección, haga clic en **Exclusiones de URL**.
   Se mostrará la ventana **Exclusiones de URL**.
   Se mostrarán las siguientes opciones:

Elementos de confianza: haga clic en **Añadir** para seleccionar 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. En el campo **Descripción**, escriba una breve descripción para que pueda reconocer el cambio en la lista de elementos de confianza.
- **Procesos**: si selecciona esta opción, se mostrará la ventana **Añadir proceso**.
  - En el campo **Proceso**, escriba la ruta de cada proceso en una nueva línea. En la sección **Descripción**, escriba una breve descripción para que pueda reconocer el cambio en la lista de elementos de confianza.

Elementos bloqueados: haga clic en **Añadir**. Se mostrará la ventana **Añadir dominio**.

En el campo **Dominio**, escriba cada dominio en una nueva línea. En el campo **Descripción**, escriba una breve descripción para que pueda reconocer el cambio en la lista de elementos bloqueados.

Nota
Se admiten rutas de red local. Por ejemplo, \\localhost\folderpath\file.exe.

Descripción

Puede usar el campo **Descripción** para introducir notas sobre las exclusiones añadidas en la lista de exclusiones de URL. A continuación, puede ver algunas sugerencias de notas que puede añadir:

- Motivo y objetivo de la exclusión.
- La fecha y la hora.

Si se añaden varios elementos en una única entrada, solo podrá haber 1 comentario para todos los elementos.

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.

Este módulo se aplica a cargas de trabajo en las que esté instalado el Antivirus de Microsoft Defender.

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.

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.

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.

  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 de firewall

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

La gestión de firewall le permite ajustar fácilmente la configuración del firewall en las cargas de trabajo protegidas.

Esta funcionalidad en Cyber Protect se proporciona a través de un componente integrado del Firewall de Microsoft Defender de Microsoft Windows. El Firewall de Microsoft Defender bloquea el tráfico de red no autorizado que entra o sale en las cargas de trabajo.

Esta gestión de firewall se aplica a cargas de trabajo en las que esté instalado el Firewall de Microsoft Defender.

Sistemas operativos Windows compatibles

Los siguientes sistemas operativos Windows son compatibles para la gestión de firewall:

Windows

- Windows 8
- Windows 8.1
- Windows 10
- Windows 11

Windows Server no es compatible.

Habilitar y deshabilitar la gestión de firewall

Puede habilitar la gestión de firewall al crear un plan de protección. Puede cambiar un plan de protección existente para habilitar o deshabilitar la gestión de firewall.

Pasos para habilitar o deshabilitar la gestión de firewall

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 de firewall** y habilite o deshabilite la **gestión de firewall**.
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 firewall de Microsoft Defender** en el área de **gestión de firewall** del panel del plan de protección aparece como **activado** o **desactivado**, en función de si ha habilitado o deshabilitado la gestión de firewall.

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 que se encuentra aislada en el disco duro de un equipo. En ella se colocan los archivos sospechosos detectados por la protección antivirus y antimalware para evitar que las amenazas se expandan todavía más.

Gracias a esta opción, puede revisar los archivos sospechosos y potencialmente peligrosos de todos los equipos, y decidir si se deben eliminar o restaurar. Los archivos que estén en cuarentena se borran automáticamente si el equipo se elimina del sistema.

¿Cómo llegan los archivos a la carpeta de cuarentena?

1. Configure el plan de protección y defina la acción predeterminada para los archivos infectados, es decir, ponerlos en cuarentena.
2. Durante el análisis en acceso o planificado, el sistema detecta archivos maliciosos y los coloca en la carpeta segura Cuarentena.
3. El sistema actualiza la lista de elementos en cuarentena de cada equipo.

4. Los archivos se borran automáticamente de la carpeta Cuarentena cuando pasa el periodo de tiempo definido en la configuración **Eliminar archivos en cuarentena después de** del plan de protección.

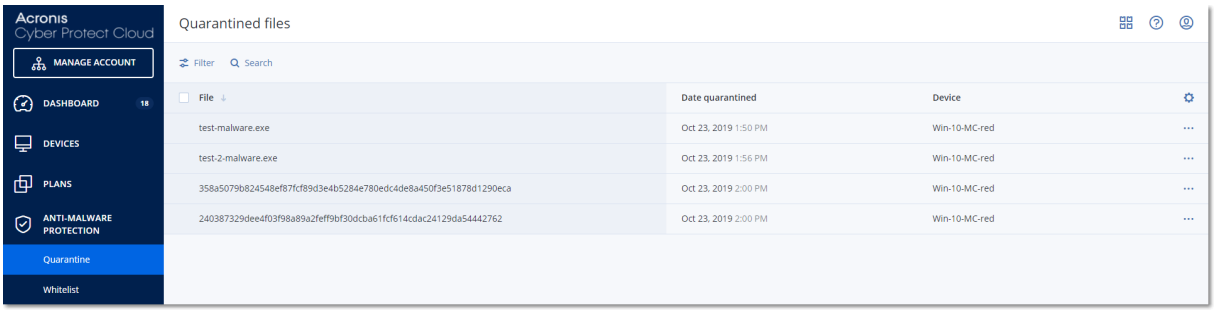
Gestión de los archivos que están en cuarentena

Para gestionar los archivos que están en cuarentena, vaya a **Protección antimalware** > **Cuarentena**. Ahí encontrará una lista con los archivos que están en cuarentena de todos los equipos.

Nombre	Descripción
Archivo	Nombre del archivo.
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	Plan de protección según el que el archivo sospechoso se puso en cuarentena.

Con los archivos que están en cuarentena, puede llevar a cabo dos acciones:

- **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 elimínelos.
- **Restaurar**: restaura un archivo en cuarentena a la ubicación original sin modificaciones. Si actualmente hay un archivo con el mismo nombre en la ubicación original, se sobrescribirá con el archivo restaurado. Tenga en cuenta que el archivo restaurado se agregará a la lista de permitidos y se omitirá durante análisis antimalware adicionales.



Ubicación de la carpeta Cuarentena en los equipos

La ubicación predeterminada para los archivos que están en cuarentena es la siguiente:

- Para un equipo Windows: `%programdata%\Acronis\NGMP\quarantine`
- Para un equipo Mac: `/Library/Application Support/Acronis/NGMP/quarantine`

- Para un equipo 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 blanca corporativa

Alguna solución antivirus podría identificar aplicaciones específicas corporativas legítimas como sospechosas. Para evitar esos falsos positivos, las aplicaciones de confianza se añaden de forma manual a la lista blanca, y eso supone perder bastante tiempo.

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, de modo que dichas aplicaciones pasan a la lista blanca, por lo que se evitan las detecciones de falsos positivos. Además, la lista blanca de 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 blanca. 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 blancas, habilite el conmutador **Generación automática de listas blancas**.

Inclusión manual de aplicaciones en la lista blanca

Cuando el conmutador **Generación automática de listas blancas** esté deshabilitado, podrá añadir archivos a la lista blanca de forma manual.

1. En la consola de Cyber Protect, vaya a **Protección Antimalware** > **Lista blanca**.
2. Haga clic en **Añadir archivo**.
3. Especifique la ruta del archivo y haga clic en **Añadir**.

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 Antimalware** > **Cuarentena**.
2. Seleccione un archivo en cuarentena y haga clic en **Añadir a la lista blanca**.

Configuración de la lista blanca

Cuando habilite el conmutador **Generación automática de listas blancas**, debe especificar uno de los siguientes niveles de protección heurística:

- **Bajo**
  Las aplicaciones empresariales se añadirán a la lista blanca 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 blanca 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 blanca 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

Con un análisis antimalware de las copias de seguridad puede evitar la recuperación de archivos infectados, ya que comprueba si sus copias de seguridad están libres de malware. Los análisis antimalware los realiza un agente de la nube que reside en el Cyber Protection centro de datos y no se utilizan recursos informáticos locales.

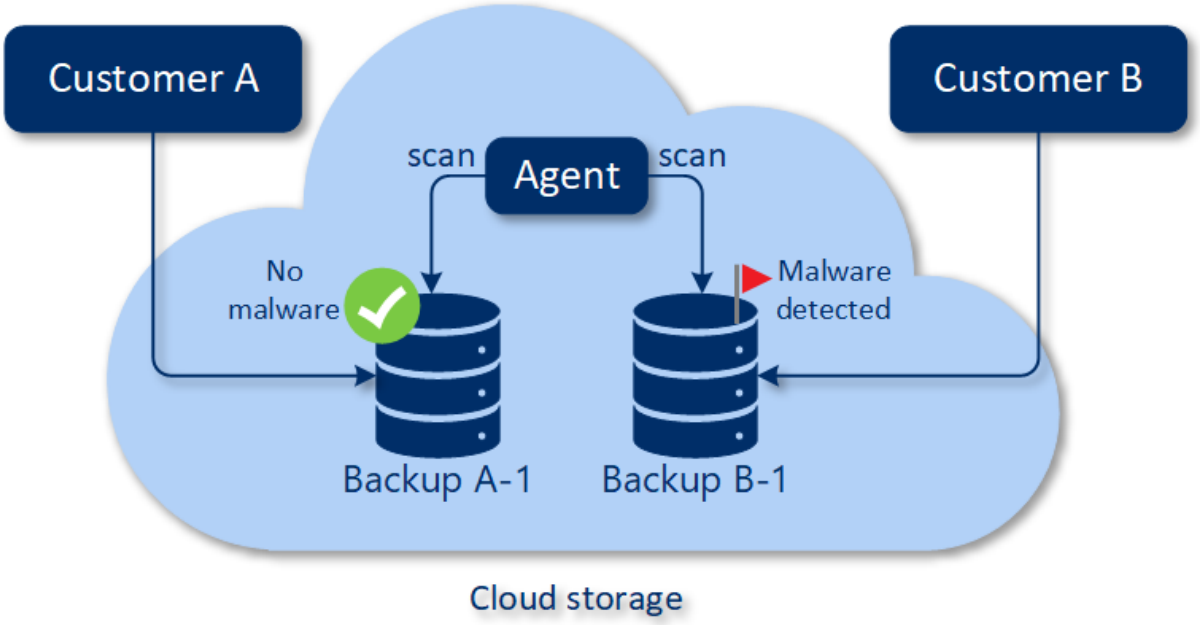
Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

Para llevar a cabo un análisis antimalware, necesita configurar un plan de análisis de copias de seguridad. Para obtener más información sobre cómo hacerlo, consulte "Análisis de planes de copia de seguridad" (p. 204).

Cada plan de análisis de copias de seguridad crea una tarea de análisis para el agente de la nube y añade esta tarea de análisis a una cola, de la que solo hay una por centro de datos. La tarea de análisis se lleva a cabo según su orden en la cola. Además, la duración del análisis depende del tamaño de la copia de seguridad. Ese es el motivo por el que hay un lapso de tiempo entre la creación de un plan de análisis de copias de seguridad y la realización del análisis.

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



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 o el Agente para Scale Computing HC3.
- Solo se pueden escanear los volúmenes con el sistema de archivos NTFS con partición GPT y MBR.
- La única ubicación compatible con la copia de seguridad es el almacenamiento en la nube predeterminado. Los almacenamientos locales y los almacenamientos en la nube propiedad de los partner no son compatibles.
- 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. 426).

- 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**.

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
Copia de seguridad avanzada	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 AlwaysOn (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 en el almacenamiento en la nube pública de Microsoft Azure
Advanced Security + EDR	Protege sus recursos informáticos continuamente de todas las amenazas de malware. Las funciones incluyen:

	• 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 antivirus y antimalware con detección basada en firmas locales (con protección en tiempo real) • Prevención de vulnerabilidades • Filtrado de URL • Gestión de firewall 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
Advanced Management	Le permite aplicar parches a vulnerabilidades en las cargas de trabajo protegidas. Las funciones incluyen: • Gestión de parches • Estado del disco • Inventario de software • 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 • 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
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.

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 **Administración** > **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 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.

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. 934)
- **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. 933)).
- **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.
- **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.
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. 925).

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.
   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. 925).
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 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

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.
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.
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
  - 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 **Administración** > **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	Todas las transferencias de datos confidenciales de las cargas de trabajo de los

Opción	Descripción
todo	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. 933)

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. 927).
- 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 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. 932).
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.
- **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 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

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 tarjeta 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
- 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
- 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)**)**

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
- 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
- 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

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 **Filtrar** 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 **Filtrar**, 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.
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:
  - **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 de Advanced DLP de definiciones de contenido relacionado con la normativa de cumplimiento.

Pasos para crear categorías de confidencialidad personalizadas

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**.
4. Verá una lista de confidencialidades, tanto integradas (como la Información sobre salud protegida o la Información de identificación personal) como personalizadas.
5. Haga clic en **Crear confidencialidad** en la esquina superior derecha de la ventana.
6. En la siguiente ventana, escriba el nombre.
7. Las nuevas confidencialidades personalizadas siempre están deshabilitadas de forma predeterminada. Podrá habilitarlas cuando configure todos los parámetros.
8. Después de crear una nueva confidencialidad, deberá configurar sus detectores de contenido. Haga clic en una flecha para expandir el contenido de su nueva confidencialidad y seleccione **Añadir detector de contenido**.
9. En la siguiente ventana, puede utilizar cualquier detector de contenido existente (haciendo clic en la marca de verificación junto al nombre y luego en **Añadir** en la esquina derecha inferior) o definir uno nuevo.
10. En lugar de crear una nueva confidencialidad desde cero, puede volver a utilizar una existente (ya sea una confidencialidad personalizada integrada o existente) clonándola y ajustando sus parámetros.
    - Para clonar una confidencialidad existente, haga clic en una marca de verificación junto al nombre y seleccione **Clonar** desde el menú desplegable Acción (indicado con tres puntos) en la esquina superior izquierda. Puede seleccionar varios elementos a la vez para clonar más de una confidencialidad.
    - En la siguiente ventana, puede seleccionar qué parámetros de la confidencialidad existente desea conservar. Para ello, haga clic en las marcas de verificación junto a cada parámetro.

Nota
Al copiar las confidencialidades integradas en un inquilino, se creará una nueva sensibilidad formada por los mismos detectores (se vuelve Personalizada una vez copiada)

Pasos para crear un nuevo detector de contenido

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 **Detectores de contenido**.
4. Verá una lista de detectores de contenido, tanto integrados como personalizados.
5. Haga clic en **Crear detector de contenido** en la esquina superior derecha de la ventana.
6. Se abrirá un menú desplegable, donde puede seleccionar el tipo de detector que desea crear. De momento solo está disponible el detector de contenido **Tipo de archivo**, pero habrá más en próximas actualizaciones.
7. En la siguiente ventana, puede configurar el detector de contenido.

Tipo de detector de contenido	Descripción
Detector de contenido de tipo de archivo	a. Hay dos listas: **Tipos de archivos compatibles** y **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 **Añadir seleccionado** de la esquina superior derecha. b. Para eliminar un tipo de archivo de la lista Tipos de archivos seleccionados, haga clic en un icono de papelera a la derecha del nombre. También puede eliminar varios tipos de archivos a la vez con las marcas de verificación y el botón **Eliminar seleccionado**.
Detector de contenido de palabras clave	a. Al crear un nuevo detector de contenido de palabras clave, deberá importar palabras clave desde un archivo. Después de importarlas correctamente, puede fusionar las nuevas palabras clave con la lista de existentes o reemplazar las existentes con las importadas. b. También debe determinar si desea que el detector de contenido coincida con todas las palabras clave de la lista, con cualquier palabra clave de la lista o con un número personalizado de palabras clave.

8. En lugar de crear un nuevo detector de contenido desde cero, también puede volver a utilizar uno existente (ya sea una confidencialidad personalizada integrada o existente) clonándolo y ajustando sus parámetros.
   - Para clonar un detector de contenido existente, haga clic en una marca de verificación junto al nombre y seleccione **Clonar** desde el menú desplegable Acción (indicado con tres puntos) en la esquina superior izquierda. Puede seleccionar varios elementos a la vez para clonar más de un detector de contenido.

Nota
Al copiar el detector de contenido integrado, este pasa a ser 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.

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	**Nombre**

Atributo	Descripción	Etiqueta en la interfaz de usuario
	el mapa de la organización.	
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 **Búsqueda** 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

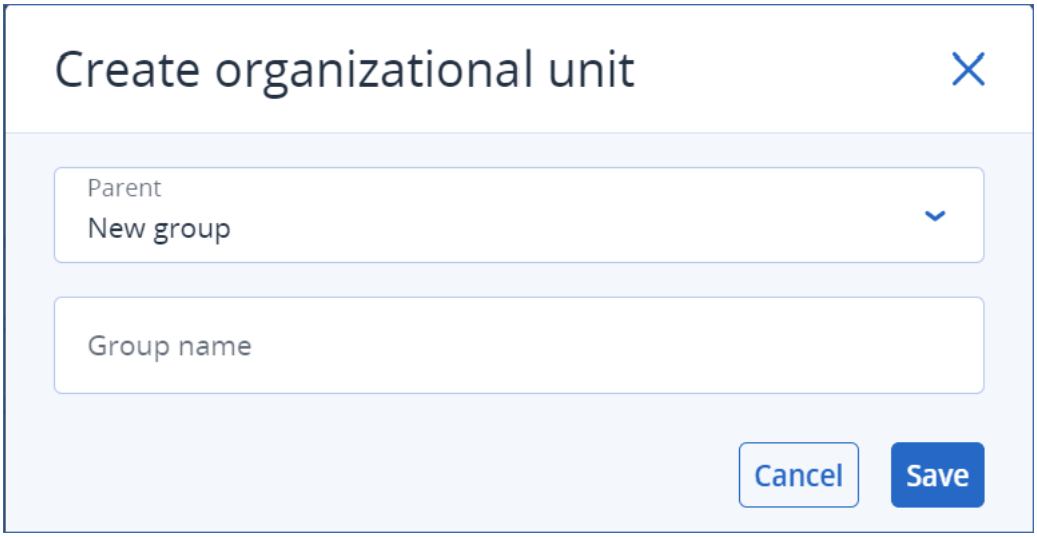
1. En la consola de Cyber Protect Cloud, navegue a **Protección** > **Prevención de pérdida de datos** > **Mapa de la organización**.
2. Para realizar una búsqueda en un grupo específico, haga clic en el nombre del grupo en la lista.
3. En el cuadro de texto **Búsqueda** que figura antes de la lista 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**.
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.

Endpoint Detection and Response (EDR)

Nota
Esta funcionalidad es parte del paquete de protección de Advanced Security + EDR, que a su vez es parte del servicio de ciberprotección. Tenga en cuenta que cuando agrega 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.

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.

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. 962).
- **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. 961)
- **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. 974).
- **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 Cyber Disaster Recovery Cloud. Para obtener más información, consulte "Solución de incidentes" (p. 978).

- **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:

- 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. 954).

Gestionar los incidentes en la página Incidentes

La EDR le permite gestionar todos los incidentes en la página Incidentes (se accede a la lista de incidentes desde el menú Protección de la consola de Cyber Protect). La página Incidentes, que puede filtrarse según sus requisitos, le garantiza que puede 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. 954).

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. 962).

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.

Para obtener más información, consulte "Solución de incidentes" (p. 978).

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. 974).

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.

Requerimientos de software

Endpoint Detection and Response (EDR) es compatible con los siguientes sistemas operativos:

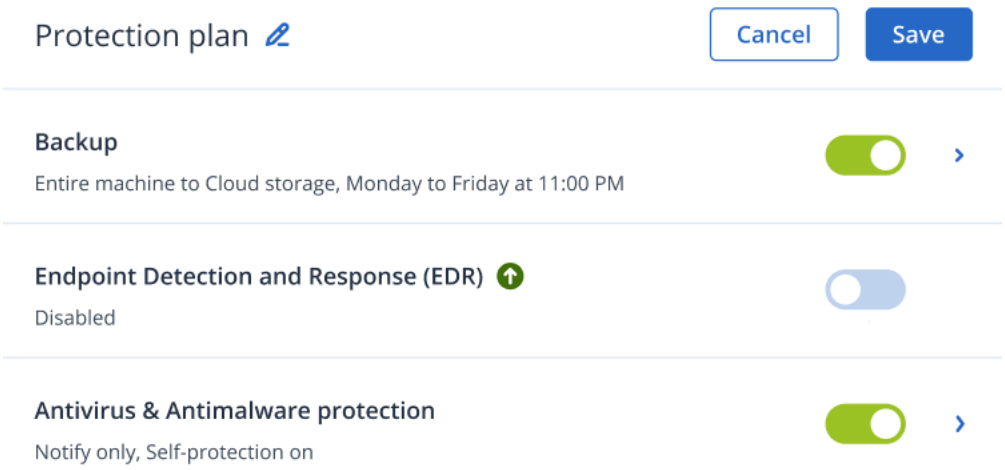
- Microsoft Windows 7 Service Pack 1 y posterior
- Microsoft Windows Server 2008 R2 y posterior

Habilitación de la funcionalidad Endpoint Detection and Response (EDR)

Puede habilitar la EDR en cualquier plan de protección.

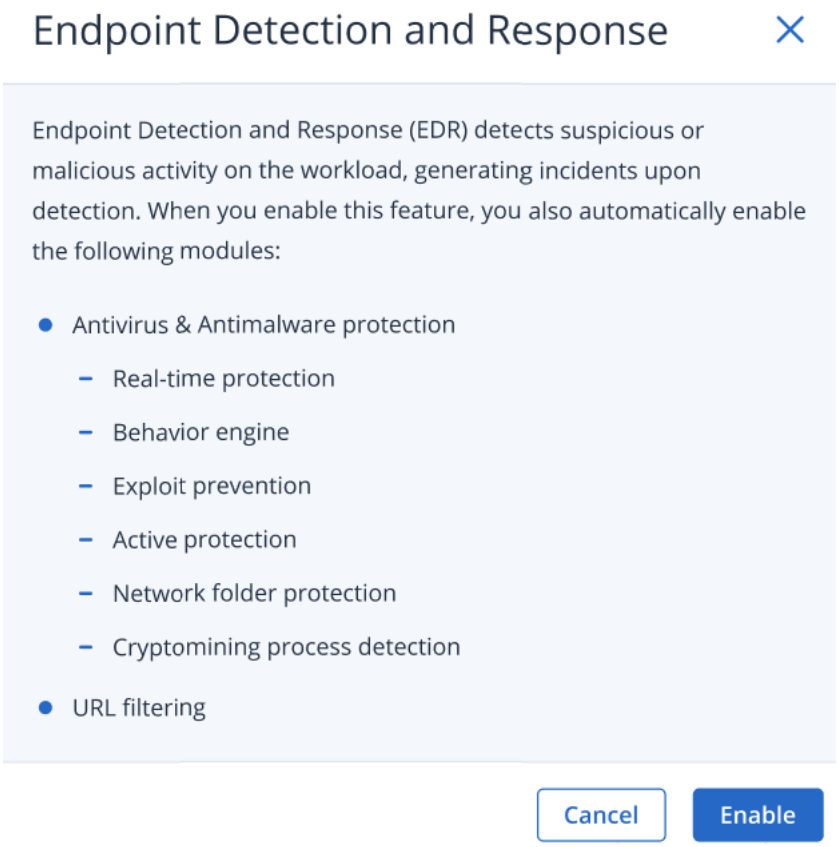
Pasos para habilitar la EDR

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. 223).
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)**.



4. En el diálogo mostrado, haga clic en **Habilitar**. Tenga en cuenta que cuando la EDR está habilitada, también se habilitan otros módulos de protección como se muestra en el diálogo

mostrado.



Nota
Si la **Protección activa**, el **Motor de comportamiento**, la **Prevención de vulnerabilidades** o el **Filtrado de URL** se cambian a **Apagado**, **Endpoint Detection and Response (EDR)** también se cambiaría a **Apagada**.

5. Tal y como se muestra a continuación, el icono del paquete **Advanced Security + EDR** se añadirá a la lista de paquetes de protección necesarios para la implementación del plan de protección, según los paquetes adicionales que seleccione.

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.
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.

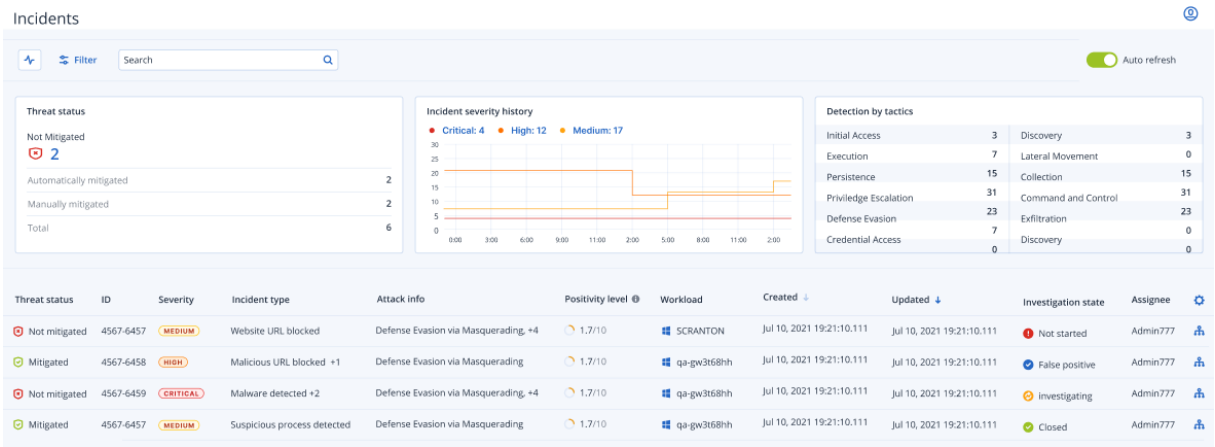
Desde la lista de incidentes, puede determinar rápidamente:

- 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 **Resumen** 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. 957) 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.



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. 962)), 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.

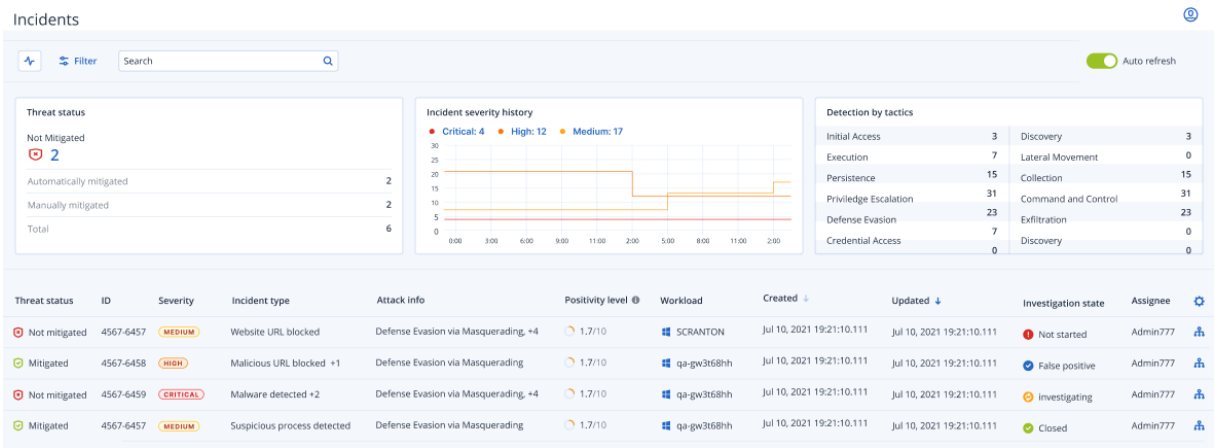
Importante
Para garantizar que sus cargas de trabajo siguen siendo seguras, analice y dé prioridad *siempre* los incidentes que están en progreso o no se han mitigado.

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. 960).

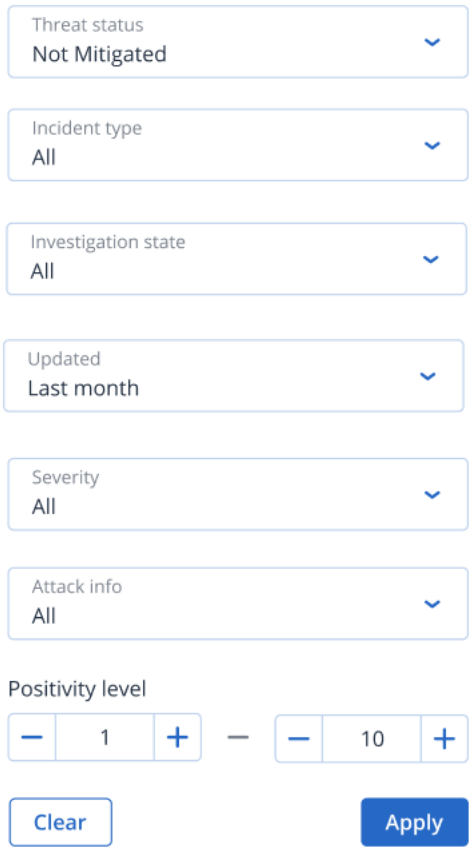


Nota

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

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.



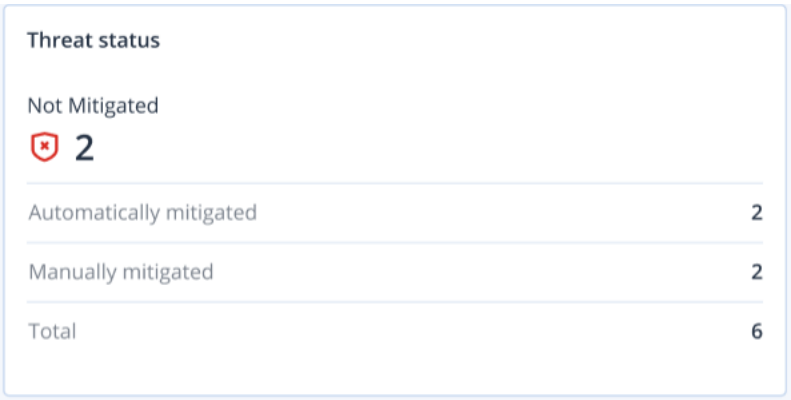
2. Haga clic en **Aplicar** cuando haya finalizado.

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. 961).

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. 957).



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**.

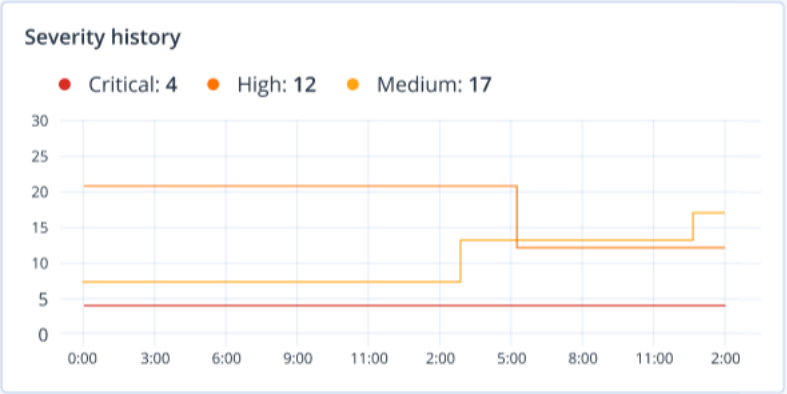
- Obtenga información sobre por qué se creó un incidente en la columna **Tipo de incidente**. El tipo de incidente puede incluir uno o más de los siguientes:
  - **Ransomware detectado**
  - **Malware detectado**

- **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.
- 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. 961)

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.



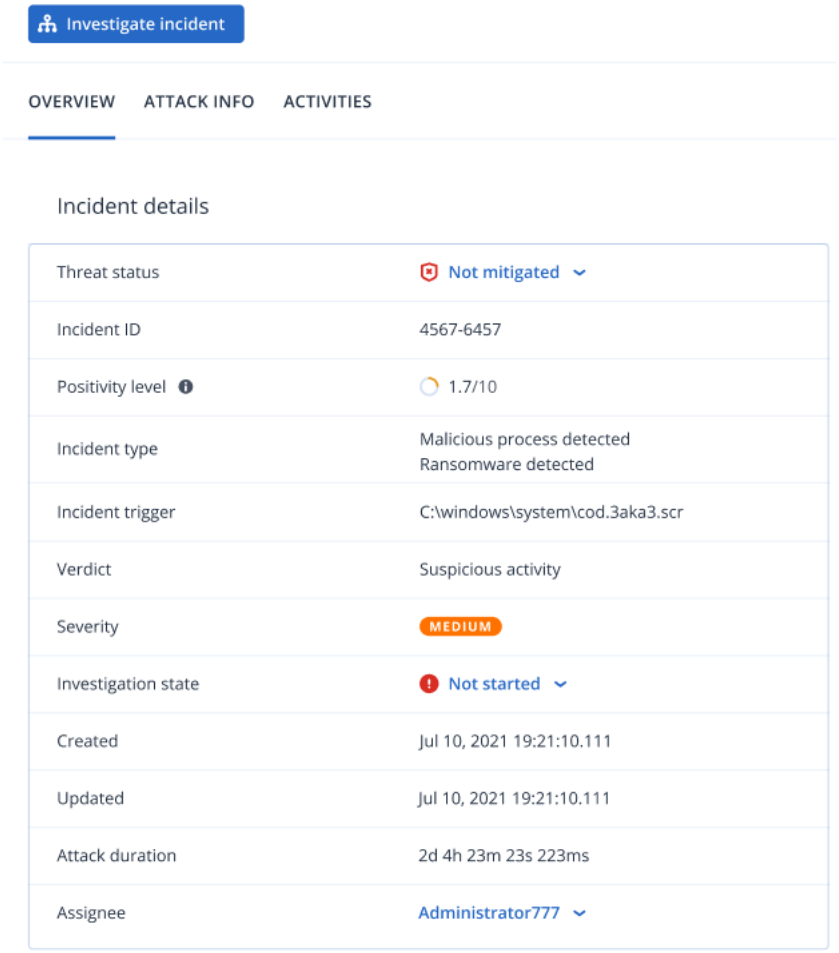
El widget **Detección por tácticas** muestra las distintas técnicas de ataque utilizadas, con valores en verde o rojo que indica el aumento o la disminución con respecto al rango de tiempo especificado anteriormente. Este widget ofrece una visión agregada de todos los objetivos de los incidentes filtrados, 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 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

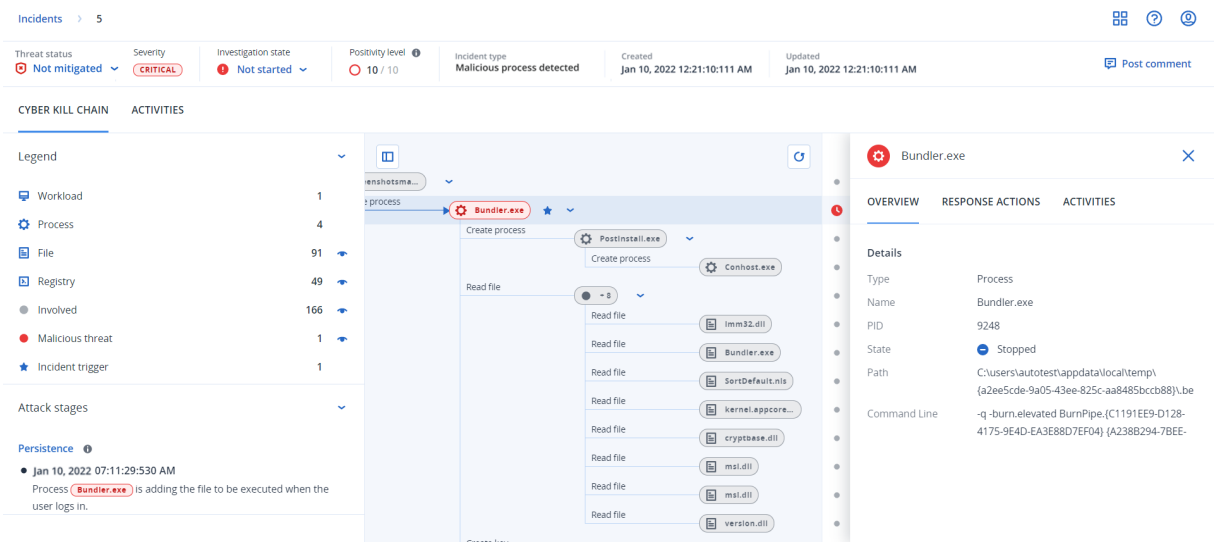
1. En la consola de Cyber Protect, vaya a **Protección > Incidentes**. Se mostrará la lista del incidente.
2. Haga clic en el incidente que desea revisar. Se mostrarán los detalles para el incidente seleccionado.
3. En la pestaña **Información general**, puede revisar la información del incidente y la 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. 962).
   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. 962).

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.



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

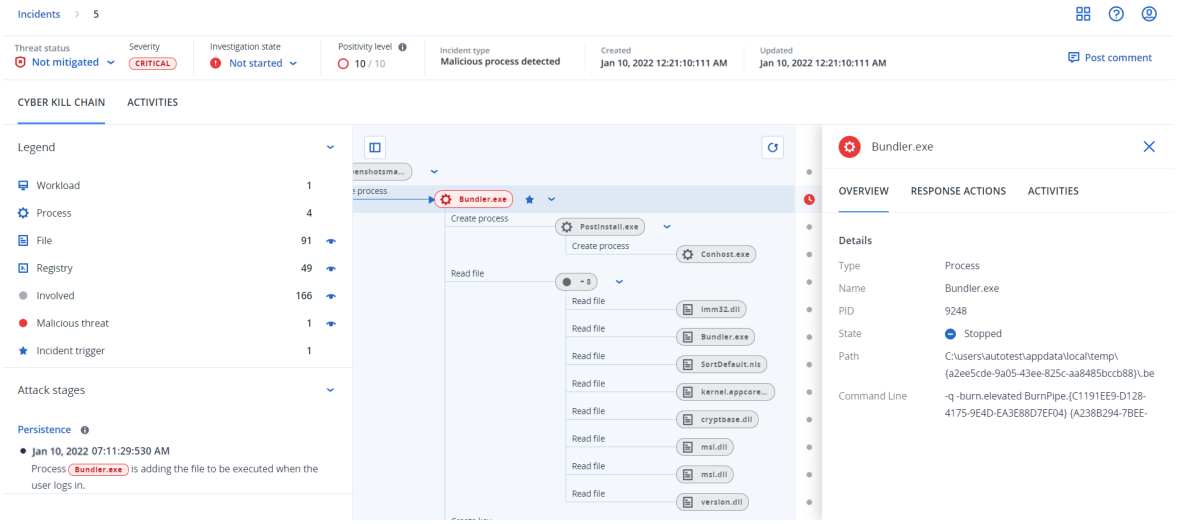
Nota
Cada objeto impactado en el ataque, tanto si es un proceso, registro, tarea programada o dominio, se representa con un nodo en la cyber kill chain.

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 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.

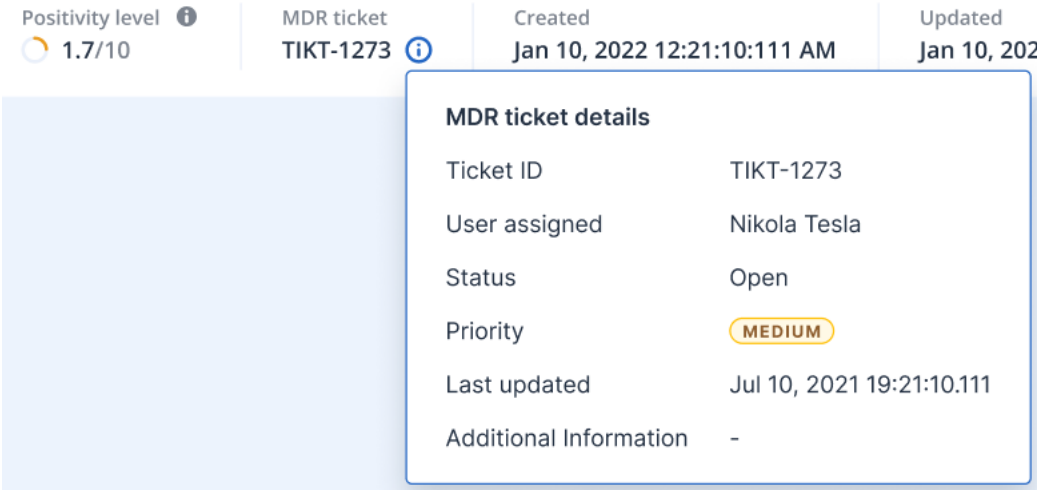
     Un incidente se establece como **No mitigado** cuando no se ha completado correctamente una restauración desde la copia de seguridad o cuando al menos una detección no se ha solucionado correctamente mediante una acción de detención del proceso, cuarentena o reversión.

     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.

   - Gravedad del incidente: **Crítico**, **Alto** o **Intermedio**. Para obtener más información, consulte "Revisar incidentes" (p. 954).
   - 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. 954).
- Tipo de incidente: uno o más casos de **Ransomware detectado**, **Malware detectado**, **Proceso sospechoso detectado**, **Proceso malicioso detectado**, **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. 965).
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.
   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. 967).
   b. Haga clic en **Solucionar todo el incidente** para aplicar las acciones de la solución. Para obtener más información, consulte "Solucionar todo un incidente" (p. 978).

      También puede solucionar nodos individuales en la cyber kill chain, tal y como se describe en "Acciones de respuesta para los nodos individuales de la cyber kill chain" (p. 983).
   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. 971).

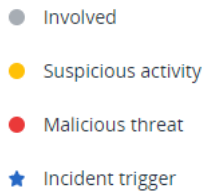
Comprender y personalizar la vista de la cyber kill chain

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. 967).



Pasos para ocultar o mostrar nodos en la cyber kill chain

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.

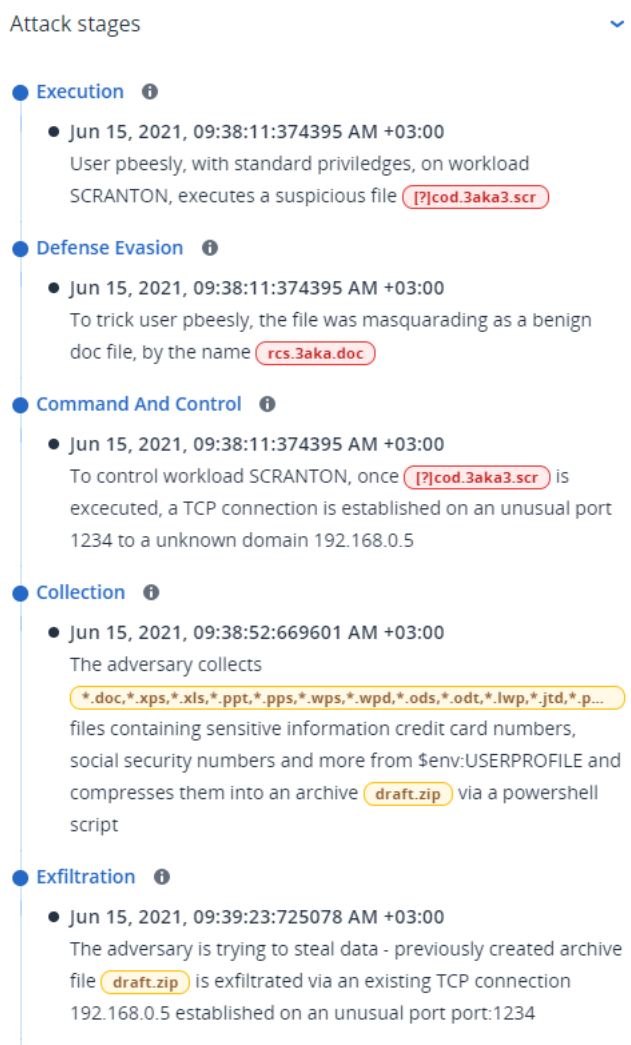
Cada fase del ataque le proporciona la información que necesita para resolver tres cuestiones cruciales:

- ¿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. 967).



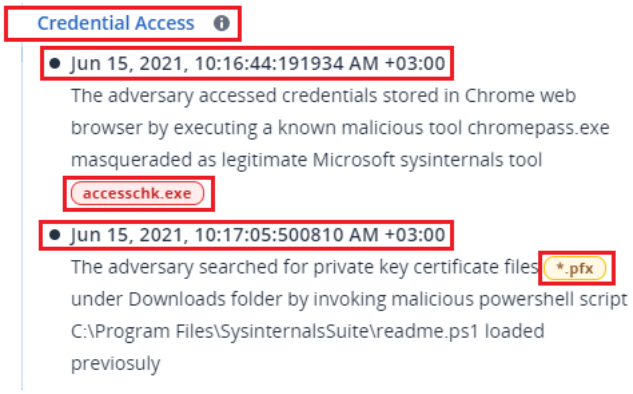
Cómo ir a las fases del ataque

Las fases del ataque se enumeran en orden cronológico. Desplácese hacia abajo para ver la lista completa de fases del ataque para el incidente.

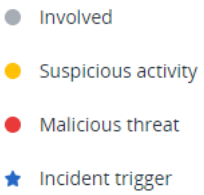
Para investigar más una fase del ataque específica, haga clic en cualquier parte en la fase del ataque para ir al nodo que corresponda en el gráfico de la cyber kill chain. Para obtener más información sobre cómo ir al gráfico de la cyber kill chain y a nodos específicos, consulte "Investigar nodos individuales en la cyber kill chain" (p. 969).

¿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.



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:

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. 969). 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.

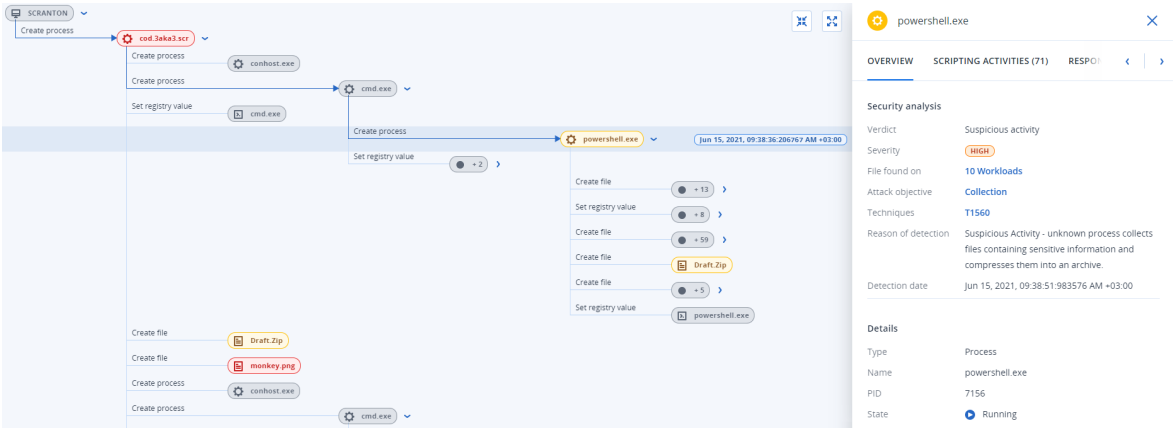
Por ejemplo, puede determinar la probabilidad de que un incidente sea un ataque malicioso de verdad. Según su investigación, también puede aplicar una serie de acciones de respuesta al nodo, incluido el aislamiento de una carga de trabajo o la cuarentena de un archivo sospechoso.

Pasos para investigar nodos individuales en la cyber kill chain

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».

- **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).

- **Acciones 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. 983).
- **Actividades**: Muestra las acciones aplicadas al incidente en orden cronológico. Para obtener más información, consulte "Entienda las acciones emprendidas para mitigar un incidente" (p. 971).

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.

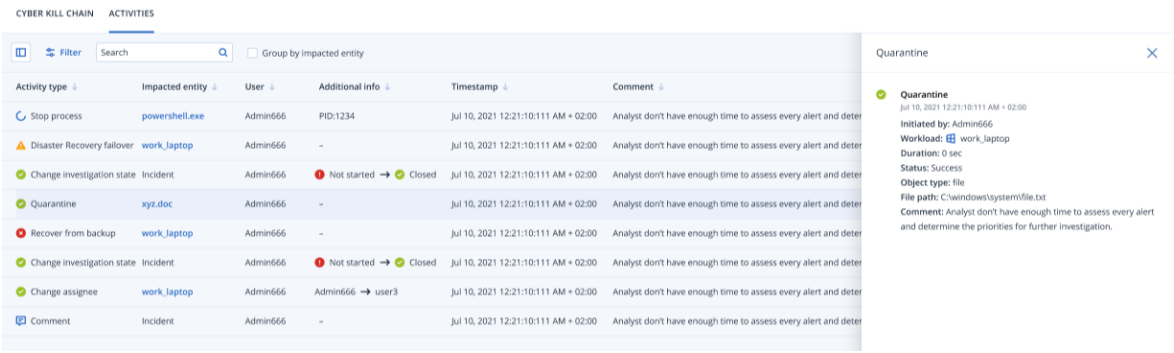
Nota
Los incidentes creados por las capas de prevención se aplican automáticamente a las acciones configuradas en el plan de protección. Para los puntos de detección, debe definir las acciones de respuesta que correspondan para mitigar el escenario de cada ataque.

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.

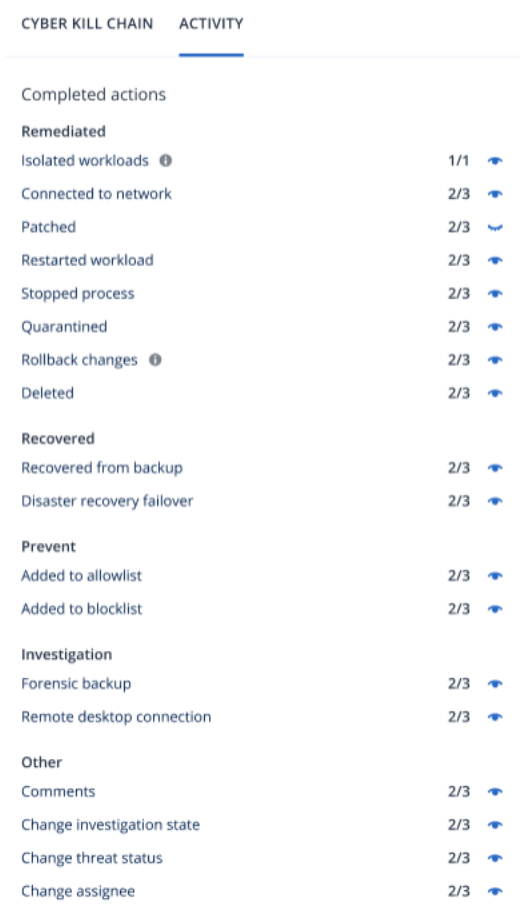
Pasos para ver todas acciones de respuesta aplicadas a un incidente

1. En la consola de Cyber Protect, vaya a **Protección > Incidentes**.

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 acciones de respuesta que ya se han aplicado al incidente.

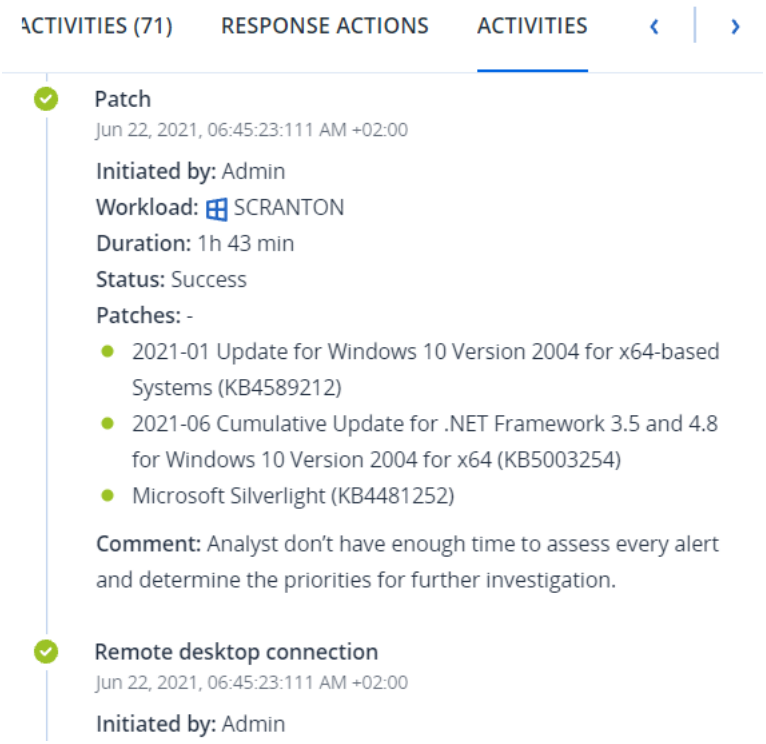


4. Puede llevar a cabo una serie de acciones en la lista mostrada:
   - Haga clic en una fila de tipo de actividad para mostrar más información sobre la actividad seleccionada. La información se muestra en una barra lateral, como se ve en el Paso 3, e incluye información sobre quién inició la acción, 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 **Filtrar** 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 .



Pasos para ver las acciones de respuesta aplicadas a un nodo específico

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).

Busque indicadores de compromiso (IOC) de ataques conocidos públicamente en sus cargas de trabajo

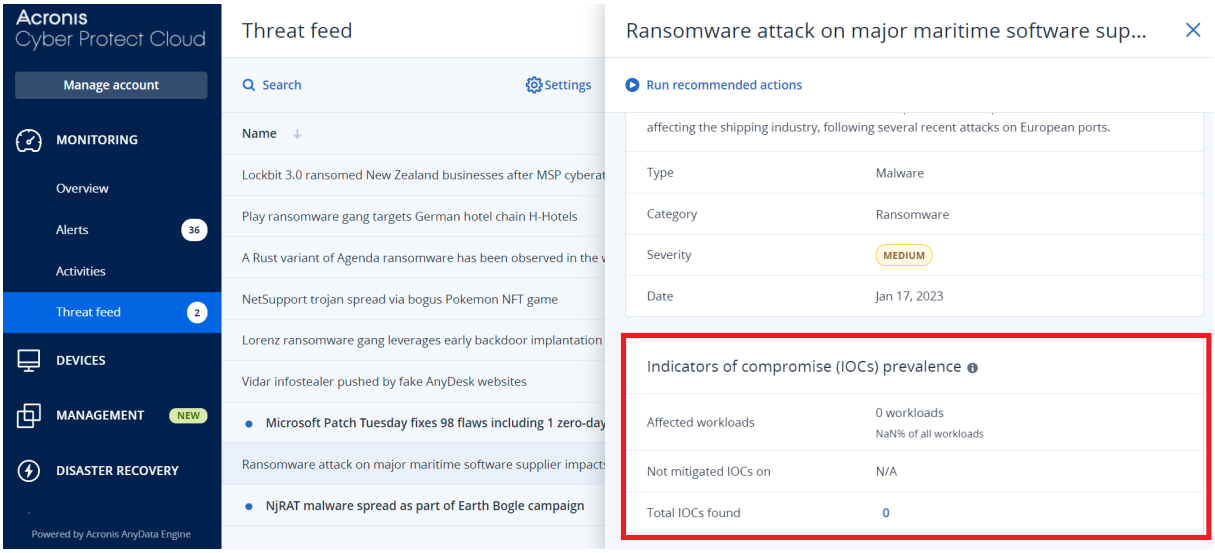
Endpoint Detection and Response (EDR) incluye la capacidad de revisar los ataques conocidos existentes en las fuentes de información sobre amenazas de sus cargas de trabajo. Estas fuentes de información sobre amenazas se generan automáticamente según los datos sobre amenazas recibidos del centro de operaciones 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. 316).

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**.

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.

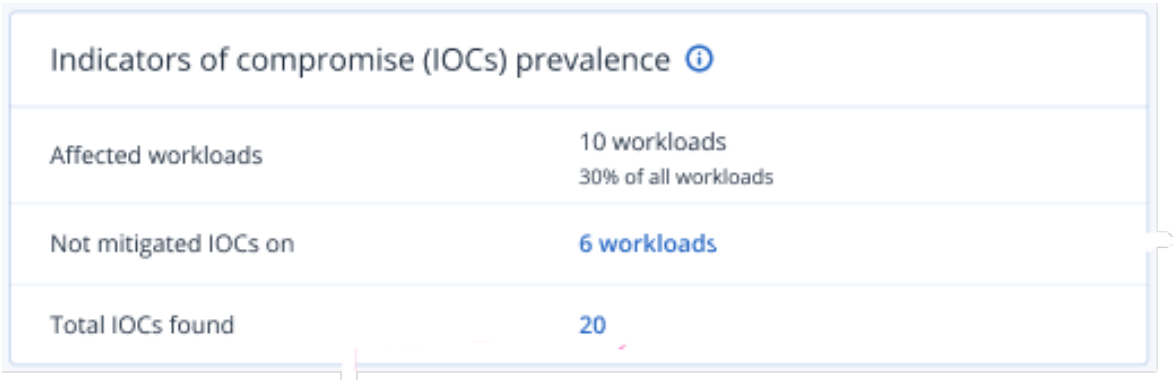
4. Haga clic en **Aplicar**.

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. 975).

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.



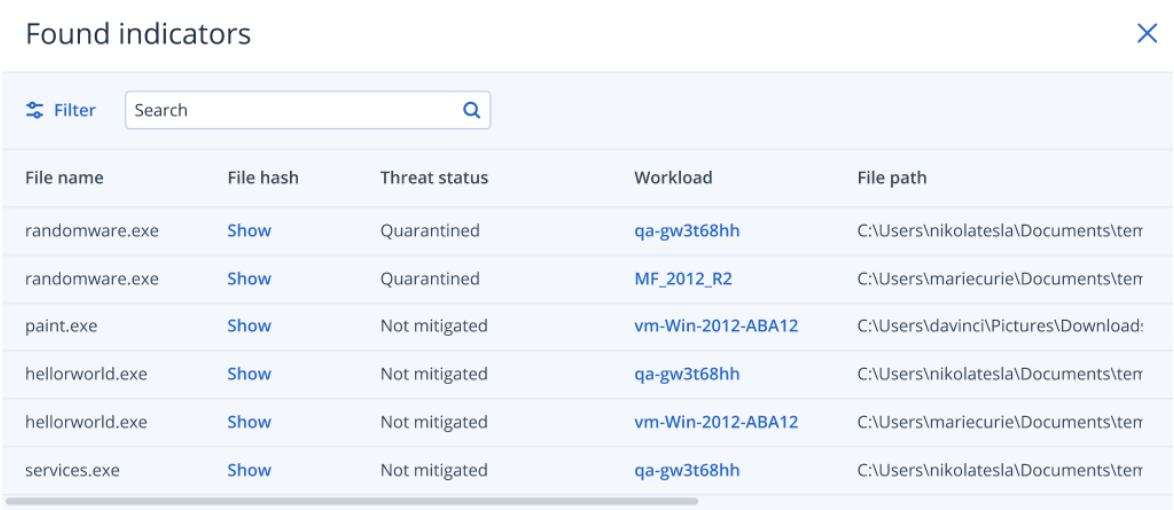
4. En la página Cargas de trabajo que se muestra, haga clic en la carga de trabajo correspondiente y revise la información. Puede ejecutar la funcionalidad específica en la carga de trabajo, incluida la definición de URL adicionales para filtrar (consulte "Filtrado de URL" (p. 895)) y bloquear los procesos maliciosos (consulte la sección Exclusiones en "Configuración de los ajustes de la protección antivirus y antimalware" (p. 870)).
   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. 977). 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.

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.

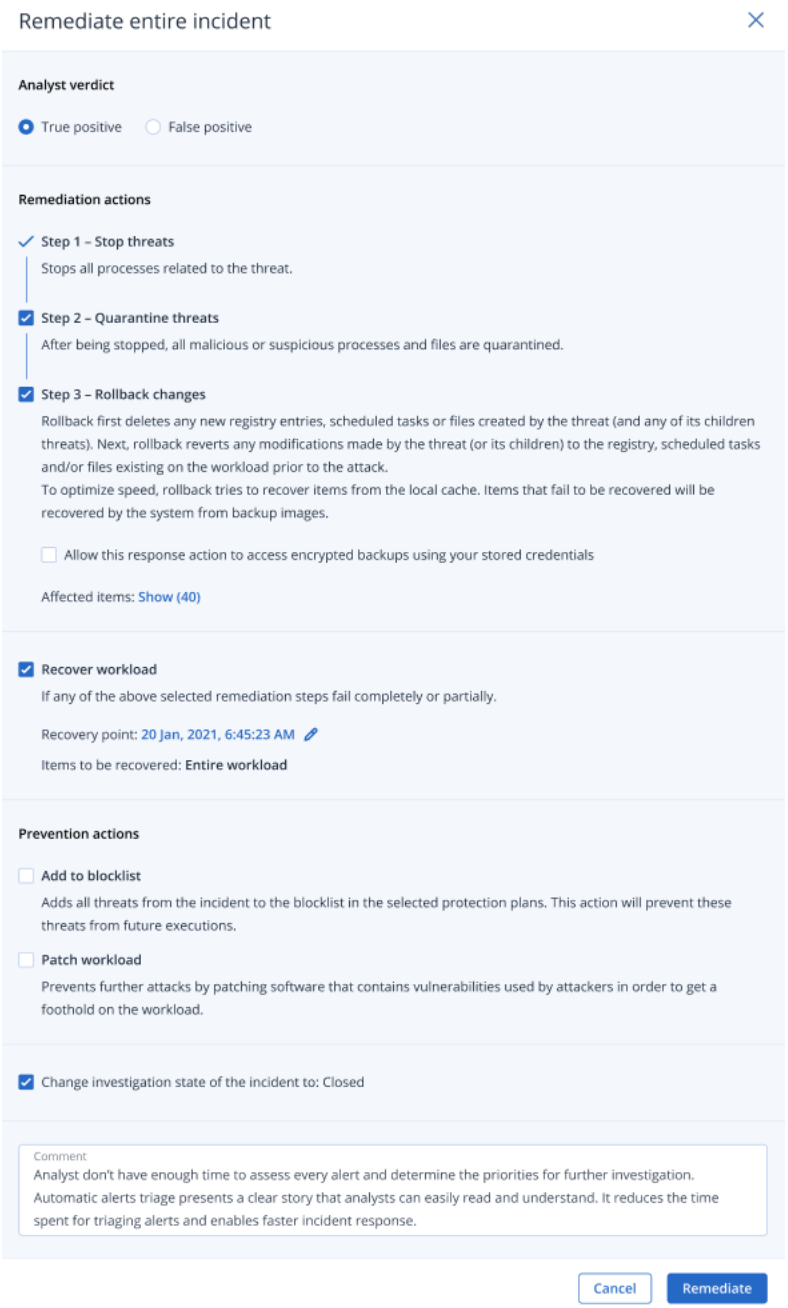
Solucionar todo un incidente

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. 983).

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.



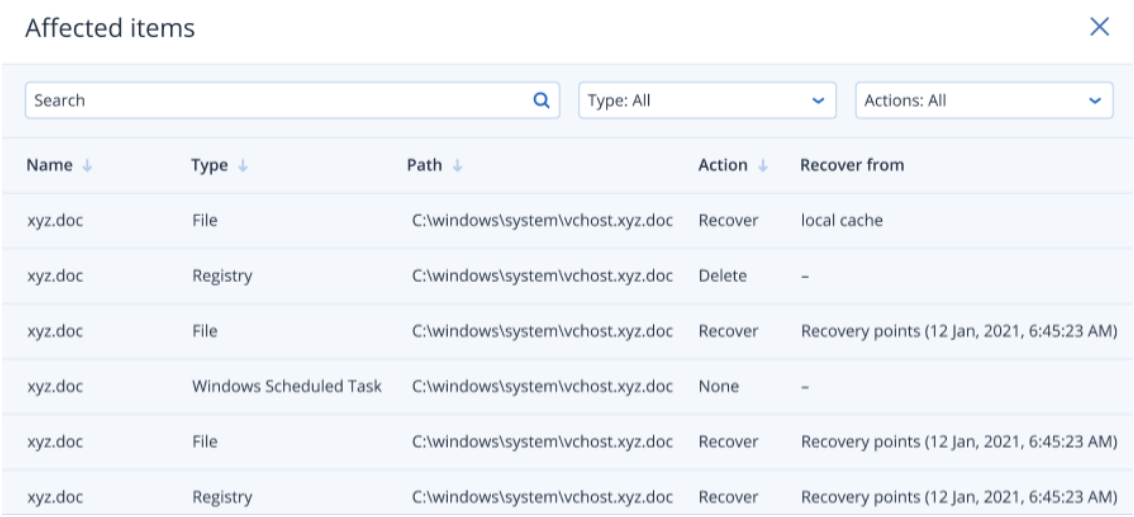
4. En la sección **Veredicto del analista**, según su investigación del incidente, seleccione una de las siguientes opciones:
   - **Verdadero positivo**: Seleccione si está seguro de que es un ataque legítimo. Una vez seleccionado, puede añadir acciones de solución y prevención, tal y como se describe 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.

Nota
Después de seleccionar **Falso positivo**, solo podrá definir acciones de prevención. Para obtener más información, consulte "Solucionar un incidente con falso positivo" (p. 982).

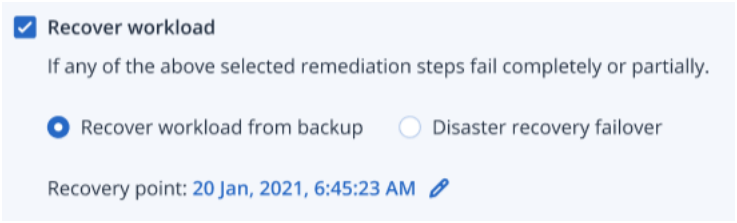
5. En la sección **Acciones de solución**, lleve a cabo los siguientes pasos de solución. Tenga en cuenta que deben seguirse en orden secuencial. Por ejemplo, no puede seleccionar el paso 2 antes de completar el paso 1.
   a. **Paso 1: detenga las amenazas**: Seleccione la casilla de verificación para 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.



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.

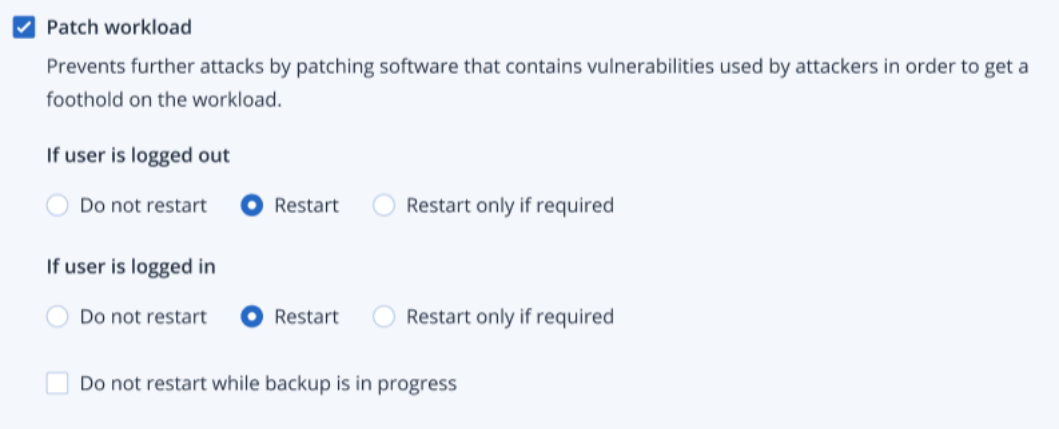


Seleccione uno de las siguientes opciones de recuperación:

- **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. 774).

6. En la sección **Acciones de prevención**, seleccione los pasos de solución que correspondan:
   - **Agregar a la lista negra**: Seleccione 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.
   - **Carga de trabajo del parche**: Seleccione la casilla de verificación para aplicar parches a 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** o **Reiniciar solo si es necesario**), en función de si el usuario ha iniciado sesión o no.

Puede seleccionar la casilla de verificación **No reiniciar si la copia de seguridad está en curso** para asegurarse de que la carga de trabajo no se reinicia durante una copia de seguridad.



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. 971).

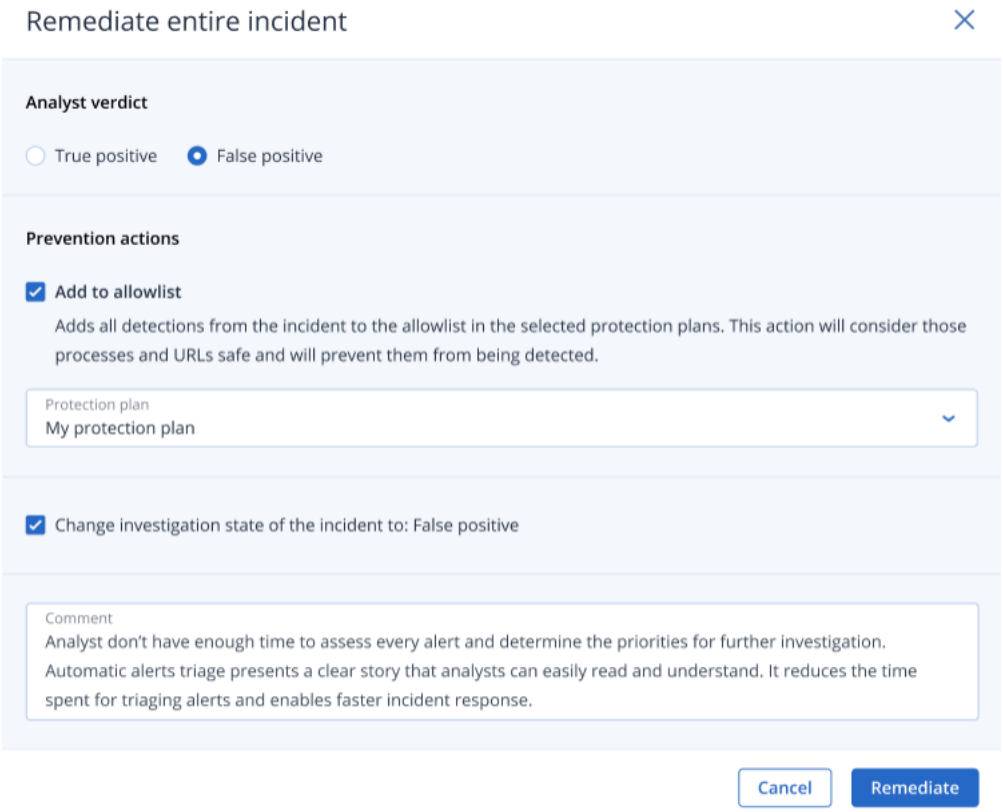
Solucionar un incidente con falso positivo

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.

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. 971).

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. 978).

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 (se aplican solo a cargas de trabajo) le permiten ejecutar una copia de seguridad forense o una conexión a escritorio remoto para una investigación más avanzada.
- **Investigar**: Las acciones de esta categoría (solo aplicables a las cargas de trabajo) permiten ejecutar una conexión a escritorio remoto para una investigación más avanzada.
- **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 la recuperación ante desastres.
- **Prevenir**: Las acciones de esta categoría le permiten prevenir futuras amenazas o falsos positivos al añadirlos a una lista de permitidos o una lista negra 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	Acciones de respuesta
Carga de trabajo	Solucionar	• Gestionar aislamiento de red • Reiniciar carga de trabajo
	Investigar	• Copia de seguridad forense • Conexión a escritorio remoto
	Investigar	• Conexión a escritorio remoto
	Recuperación	• Recuperación a partir de la

Nodo	Categoría	Acciones de respuesta
		copia de seguridad • Conmutación por error de la recuperación ante desastres
	Prevenir	• Parche
Proceso	Solucionar	• Detener proceso • Cuarentena
	Prevenir	• Agregar a la lista de permitidos • Agregar a la lista negra
Archivo	Solucionar	• Eliminar • Cuarentena
	Prevenir	• Agregar a la lista de permitidos • Agregar a la lista negra
Registro	Solucionar	• Eliminar
Red	Prevenir	• Agregar a la lista de permitidos • Agregar a la lista negra

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. 986).

- **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. 990).
- **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. 991).
- **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. 993).
- **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. 994).
- **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. 994).
- **Conmutación por error de la recuperación ante desastres**: Le permite ejecutar "Implementación de la recuperación ante desastres" (p. 774). 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 la recuperación ante desastres" (p. 995).

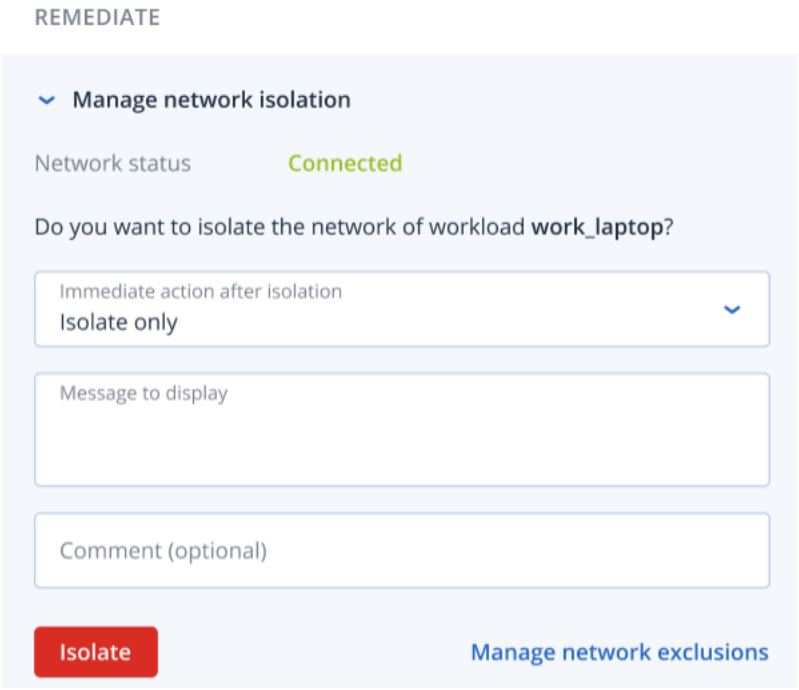
Gestione el aislamiento de red de una carga de trabajo

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 **Acciones de respuesta**.

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. 413).
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.

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. 971).

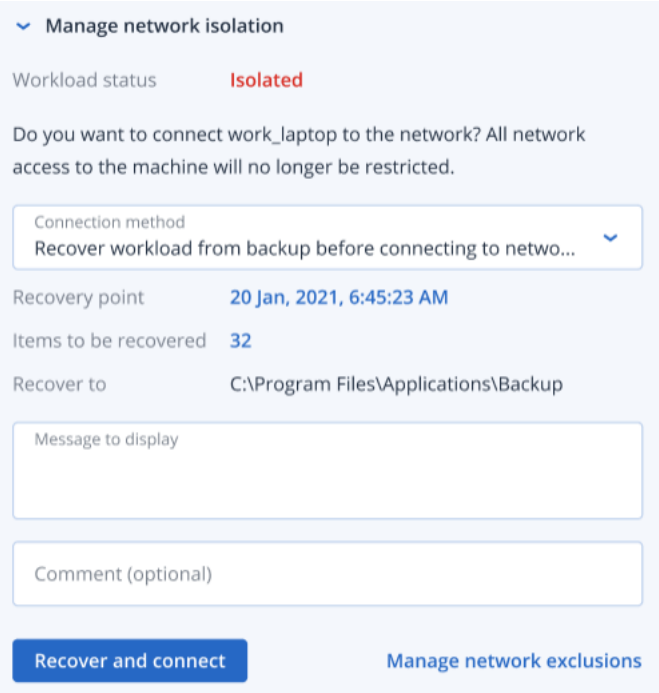
Nota
La carga de trabajo también se muestra como **Aislada** en el menú **Cargas de trabajo** de la consola de Cyber Protect. También puede aislar una o varias cargas de trabajo desde el menú **Cargas de trabajo > Cargas de trabajo con agentes**; seleccionar las cargas de trabajo correspondientes y, 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 **Acciones 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**.



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.

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 **Acciones 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 **Añadir** 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**.

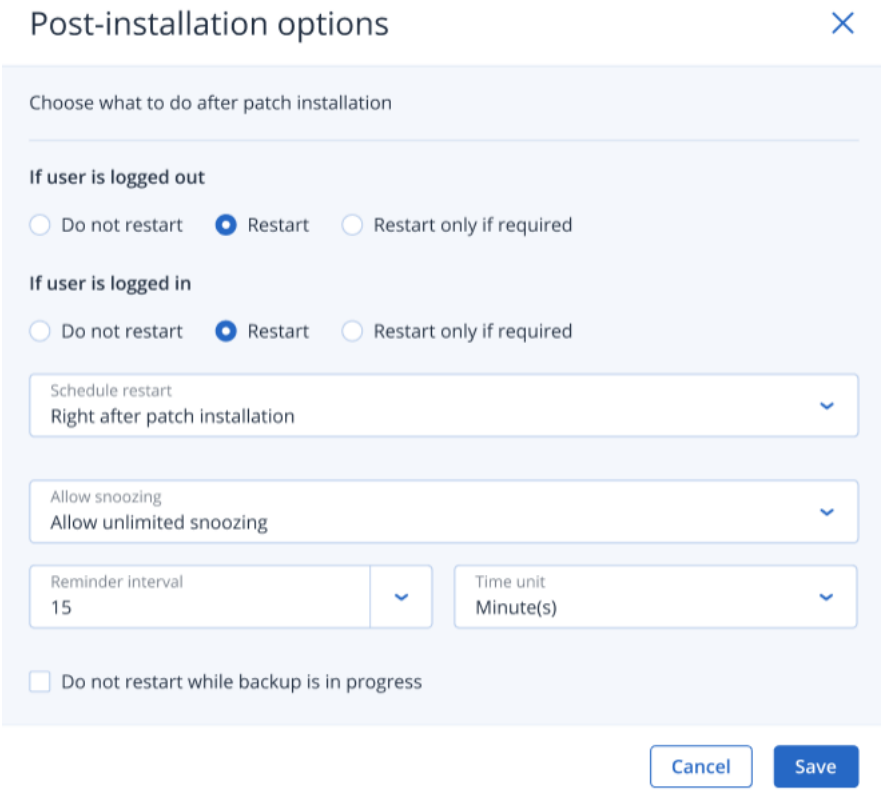
Aplicar parche a una carga de trabajo

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 característica solo está disponible si la carga de trabajo del partner tiene una suscripción a Advanced Management.

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 **Acciones de respuesta**.
3. En la sección **Solucionar** haga clic en **Aplicar parche**.
4. En el campo **Parches para instalar**, haga clic en **Seleccionar**. En el diálogo que se muestra, seleccione los parches que correspondan y haga clic en **Seleccionar**.

5. En el campo **Opciones posteriores a la instalación**, haga clic en el enlace que se muestra. Se mostrará el diálogo de las opciones posteriores a la instalación.



6. Seleccione la acción que se llevará a cabo después de instalar el parche:
   - **Si el usuario cerró la sesión**: Seleccione entre **No reiniciar**, **Reiniciar** o **Reiniciar solo si es necesario**.
   - **Si el usuario inició sesión**: Seleccione entre **No reiniciar**, **Reiniciar** o **Reiniciar solo si es necesario**.
     Cuando seleccione **Reiniciar**, también puede definir lo siguiente:
     - Programar el reinicio.
     - Permitir el aplazamiento, incluidos los intervalos definidos entre aplazamientos.
7. [Opcional] Seleccione la casilla de verificación **No reiniciar si la copia de seguridad está en curso** para asegurarse de que la carga de trabajo no se reinicia si una copia de seguridad está actualmente en curso.
8. Haga clic en **Guardar**.
9. En la pestaña **Acciones de respuesta**, haga clic en **Aplicar 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. 971).

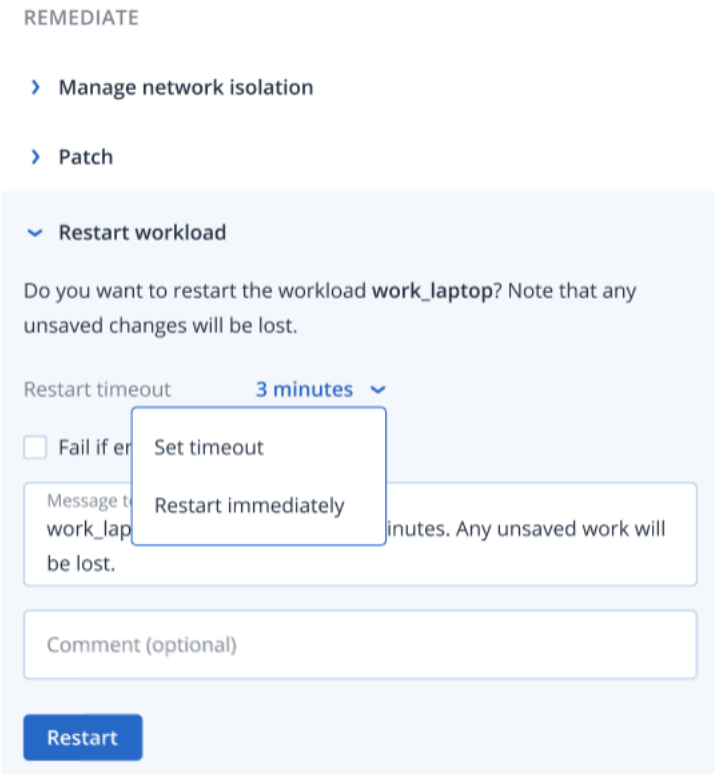
Reiniciar una carga de trabajo

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 **Acciones de respuesta**.
3. En la sección **Solucionar** haga clic en **Reiniciar carga de trabajo**.



4. En el campo **Reiniciar tiempo de espera**, 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.
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

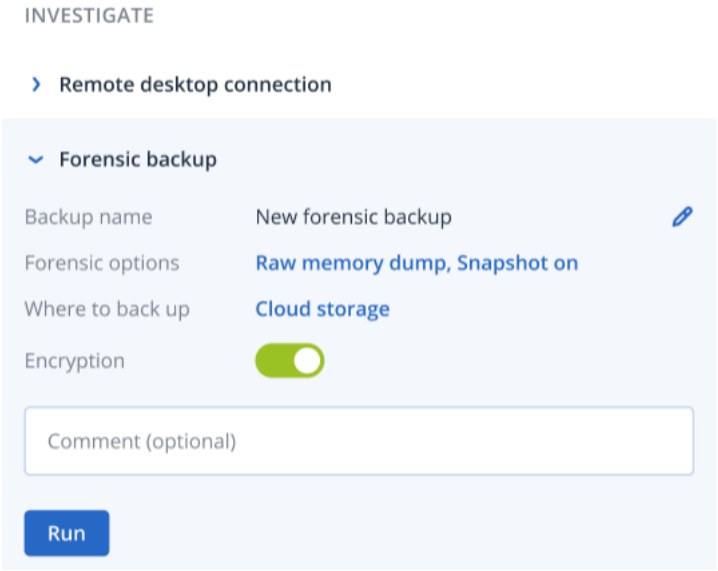
incidente. Para obtener más información, consulte "Entienda las acciones emprendidas para mitigar un incidente" (p. 971).

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 **Acciones 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.
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.

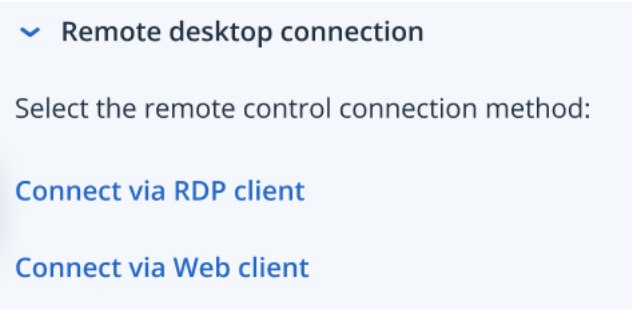
7. [Opcional] Haga clic en la opción **Cifrado** para habilitar el cifrado. En el cuadro que se muestra, introduzca la contraseña para la copia de seguridad cifrada y seleccione el algoritmo de cifrado correspondiente.
8. [Opcional] En el campo **Comentario**, añada un comentario. Este comentario puede 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. 971).

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 **Acciones 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.

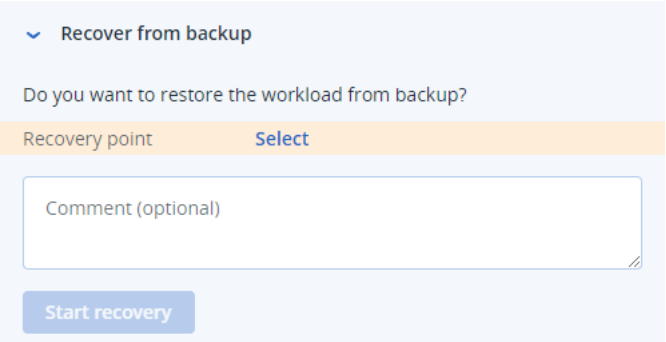
   Cuando se haya iniciado la conexión remota, puede ver esta acción en las pestañas **Actividades** del nodo individual y de todo el incidente. Para obtener más información, consulte "Entienda las acciones emprendidas para mitigar un incidente" (p. 971).

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 **Acciones 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**.

   Nota
   Si el punto de recuperación que selecciona está cifrado, se le pedirá la contraseña.

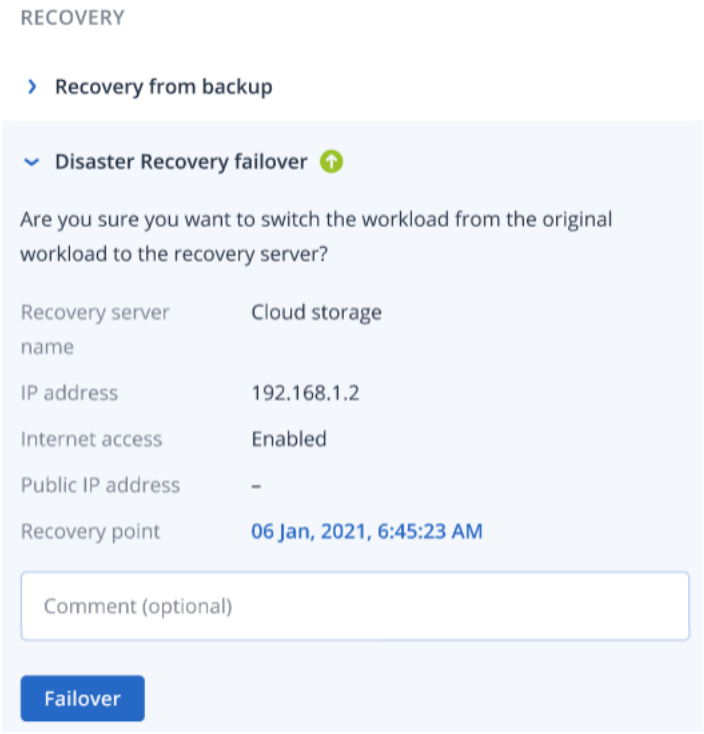
5. [Opcional] Seleccione la casilla de verificación **Reinicie la carga de trabajo automáticamente**. Esta opción solo aplica si ha seleccionado **Recuperar > Toda la carga de trabajo** en el paso 4.
6. [Opcional] En el campo **Comentario**, añada un comentario. Este comentario puede verse en la pestaña **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. 971).

Conmutación por error de la recuperación ante desastres

Como parte de su respuesta de recuperación a un ataque, con la EDR puede ejecutar "Implementación de la recuperación ante desastres" (p. 774), 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 la recuperación ante desastres

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 **Acciones de respuesta**.
3. En la sección **Recuperación**, haga clic en **Conmutación por error de la recuperación ante desastres**.



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 Recuperación ante desastres. 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. 971).

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:

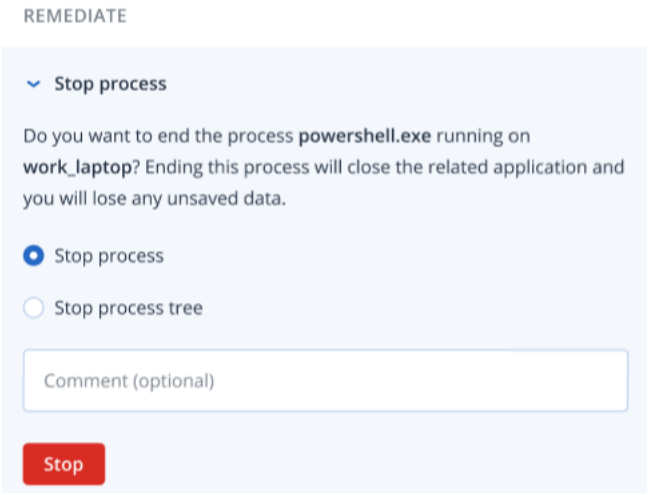
- Detener un proceso (consulte más adelante)
- Poner en cuarentena un proceso (consulte más adelante)
- Revertir los cambios realizados por un proceso (consulte más adelante)
- Agregar el proceso a la lista de permitidos o la lista negra de un plan de protección (consulte "Añade o elimina un proceso, archivo o red en la lista de bloqueados o permitidos del plan de protección" (p. 1002))

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 **Acciones de respuesta**.
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.

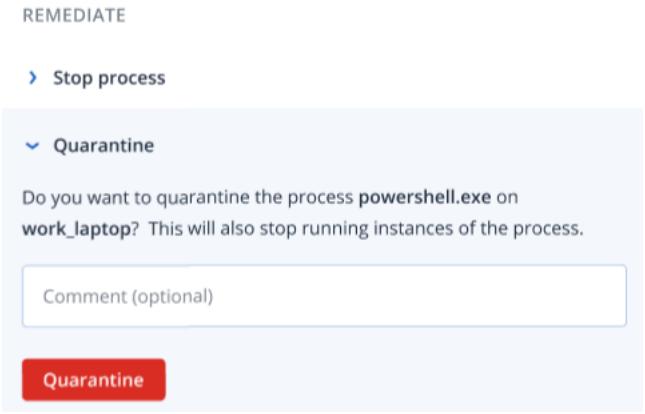
   También puede ver esta acción en las pestañas **Actividades** del nodo individual y de todo el incidente. Para obtener más información, consulte "Entienda las acciones emprendidas para mitigar un incidente" (p. 971).

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 **Acciones 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 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. 971).

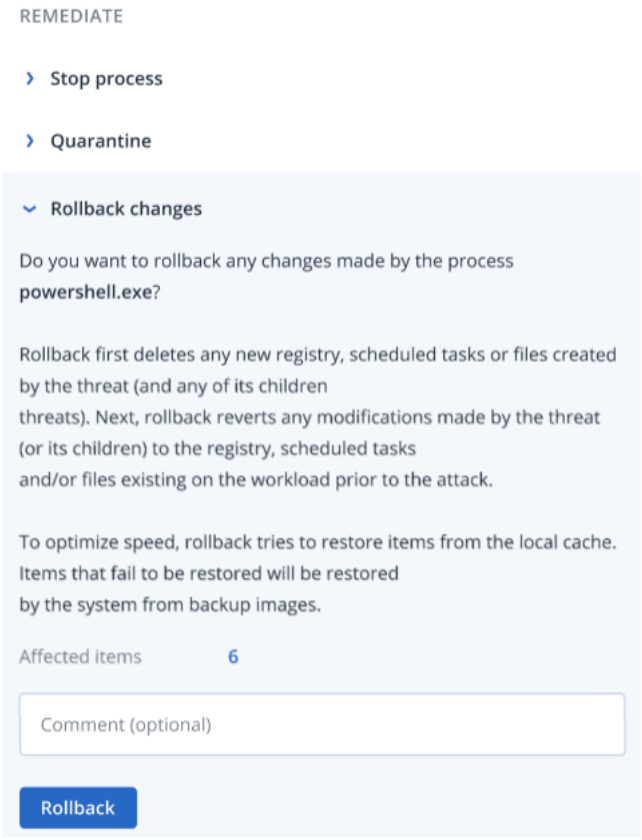
Cómo revertir cambios

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).

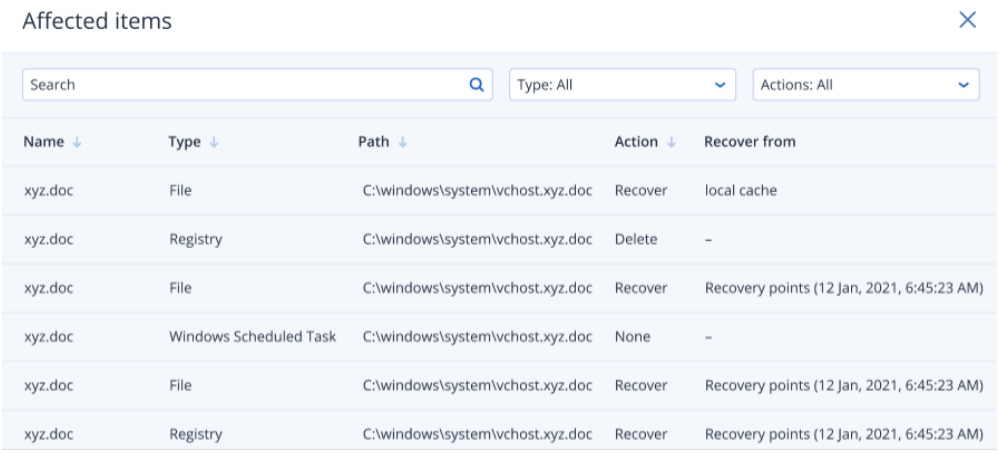
2. En la barra lateral que se muestra, haga clic en la pestaña **Acciones de respuesta**.

3. En la sección **Solucionar** haga clic en **Revertir cambios**.



Nota
El proceso de reversión solo recupera los elementos en la caché local. Se podrán revertir archivos de copia de seguridad en próximas versiones.

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:
   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. 971).

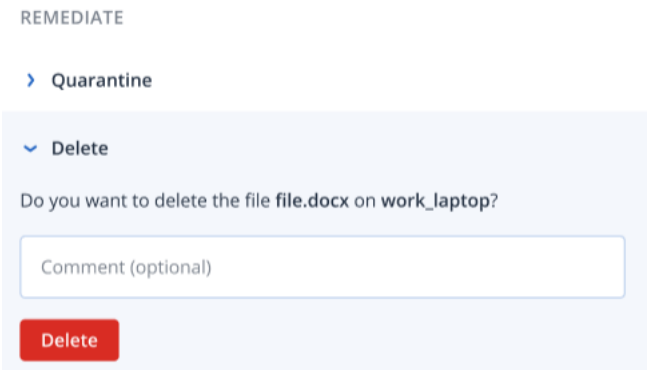
Defina las acciones de respuesta para un archivo sospechoso

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 negra 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. 1002))

Pasos para eliminar un archivo sospechoso

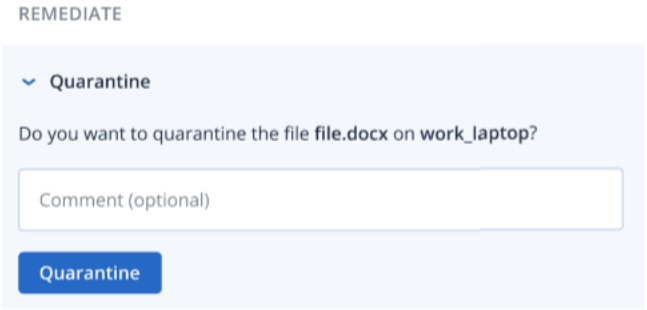
1. En la cyber kill chain, haga clic en el nodo del archivo que desee solucionar.
2. En la barra lateral que se muestra, haga clic en la pestaña **Acciones de respuesta**.
3. En la sección **Solucionar** haga clic en **Eliminar**.



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. 971).

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 **Acciones 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. 971).

Defina las acciones de respuesta para una entrada de registro sospechosa

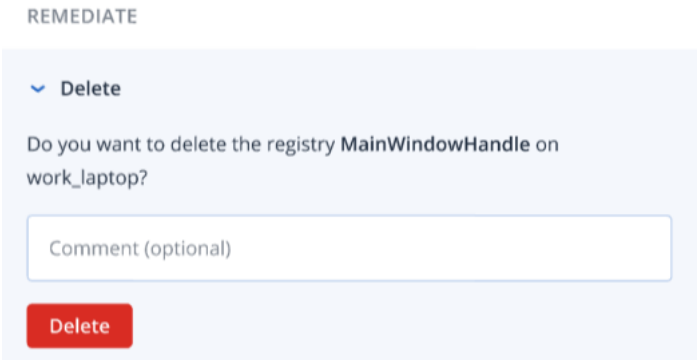
Como parte de su respuesta de solución a un ataque, puede eliminar las entradas de registro sospechosas.

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 **Acciones 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**.
   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. 971).

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.

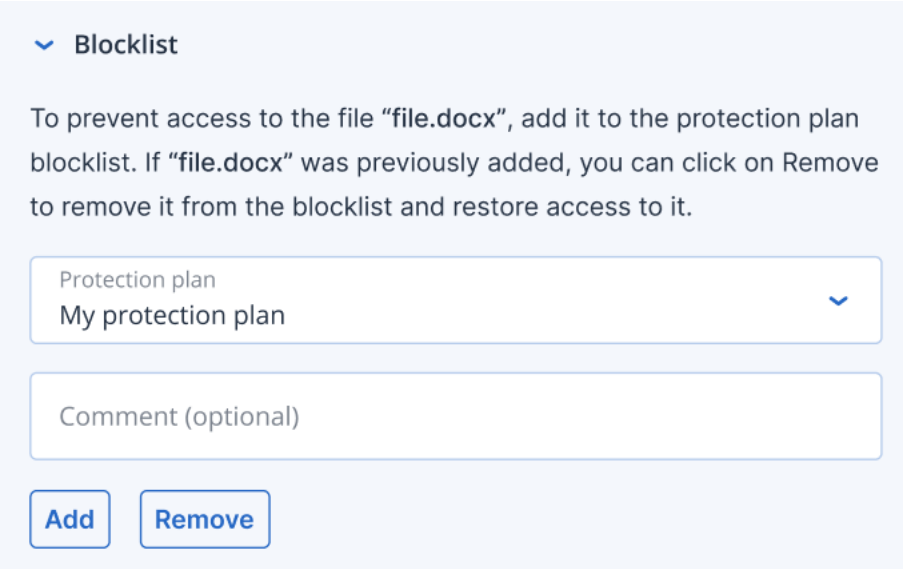
También puede eliminar un nodo de la lista de permitidos o bloqueados para permitir o prevenir cualquier acceso futuro al nodo.

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

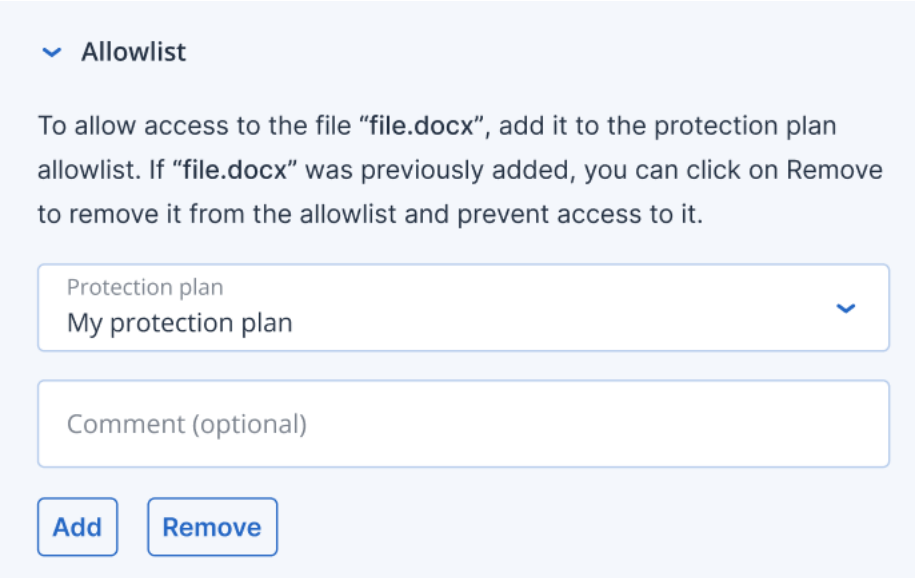
1. En la cyber kill chain, haga clic en el proceso, archivo o nodo de red que desee remediar.
2. En la barra lateral que se muestra, haga clic en la pestaña **Acciones de respuesta**.
3. En la sección **Prevenir**, haga clic en el icono de flecha junto a **Lista de bloqueados**.



4. Seleccione los planes de protección correspondientes a los que desee aplicar esta acción.
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. 971).

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 **Acciones 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. 971).

Habilitar el modo de supervisión para Endpoint Detection and Response (EDR)

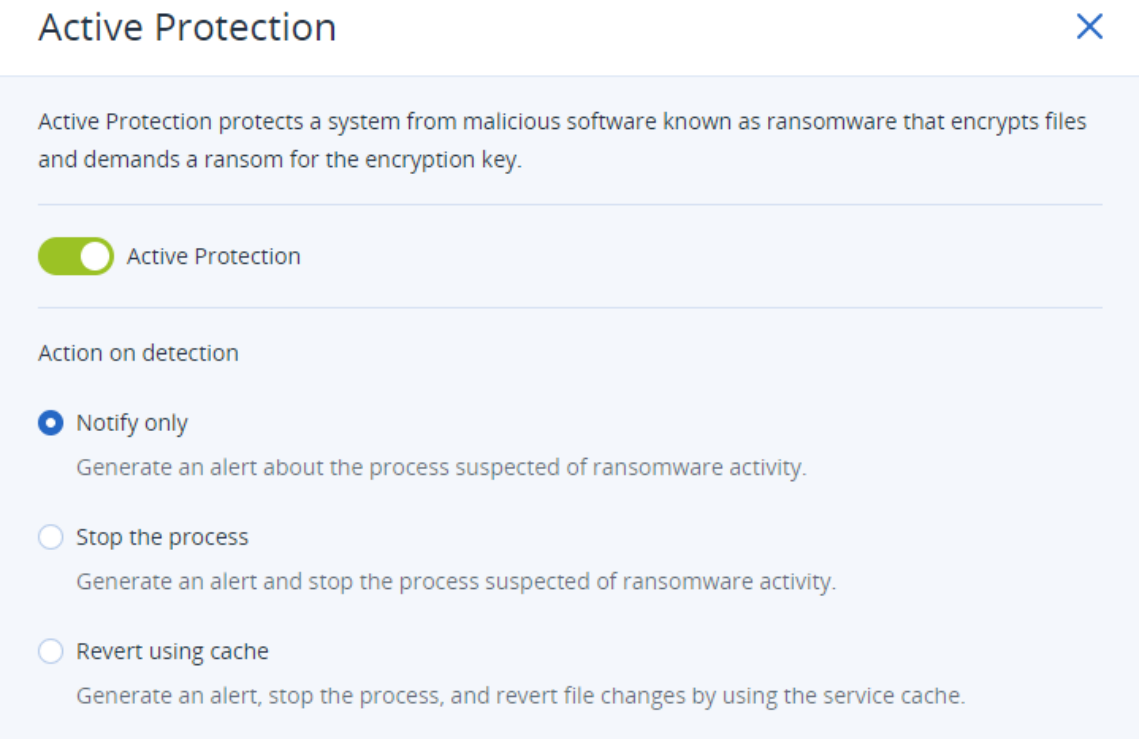
El modo de supervisión de Cyber Protection permite usar la EDR en un entorno de producción. A su vez, esto permite verificar si hay falsos positivos y hacer las exclusiones necesarias antes de desplegar completamente la EDR.

En modo de supervisión, nada se bloquea ni se detiene y se crean incidentes, pero no se inician respuestas.

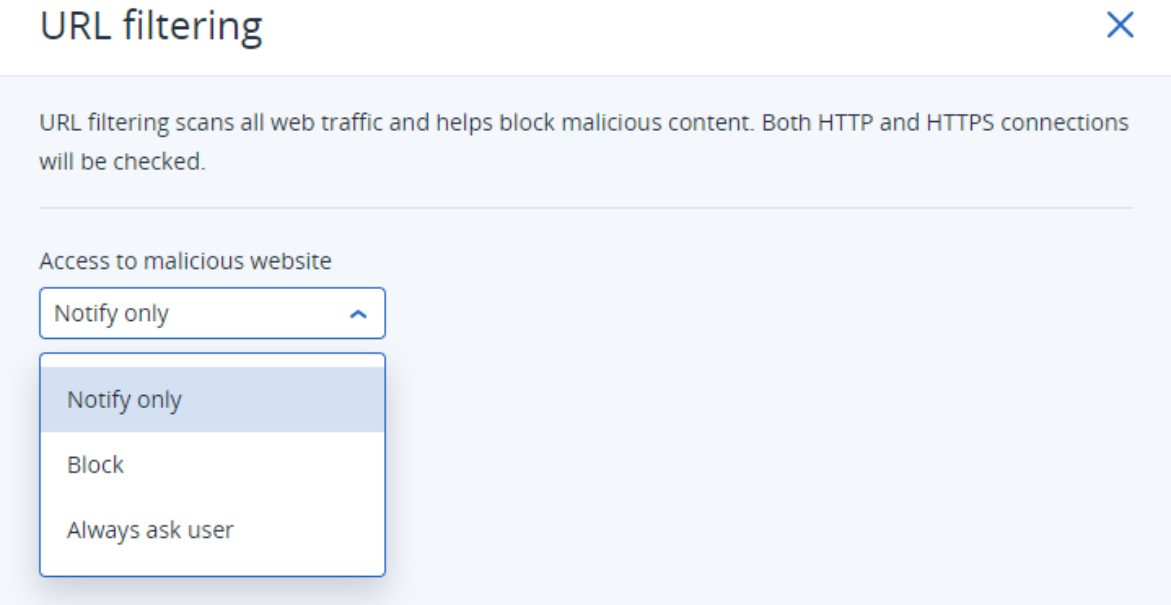
Para habilitar el modo de supervisión para EDR

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. 952).

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. 871).



   - 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. 876).
   - 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. 877).
   - 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. 879).
   - 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. 880).
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. 895).



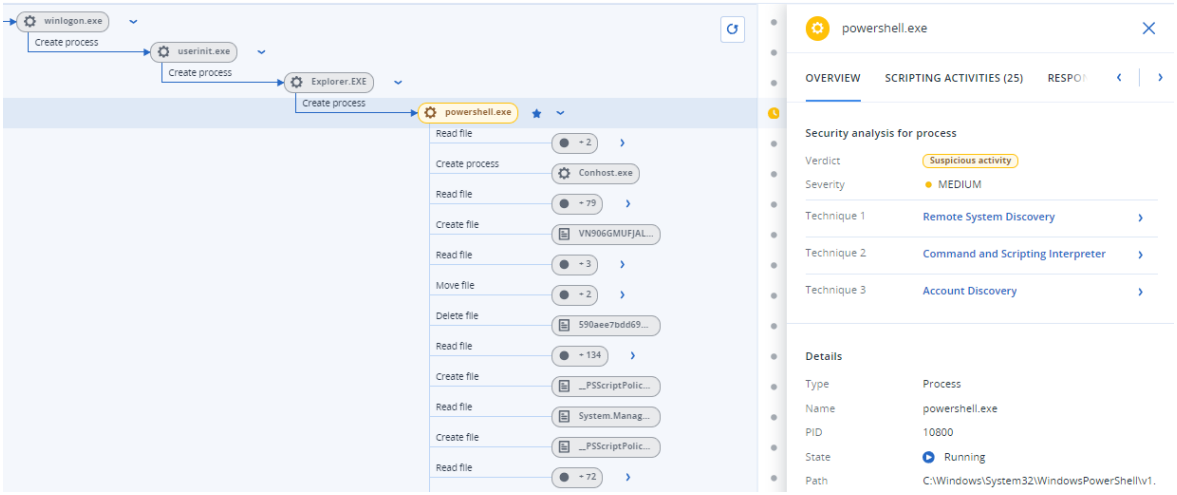
Cómo probar si Endpoint Detection and Response (EDR) funciona correctamente

Para garantizar que la EDR se implementa y funciona, puede ejecutar un número de comandos que desencadenan las detecciones de la EDR.

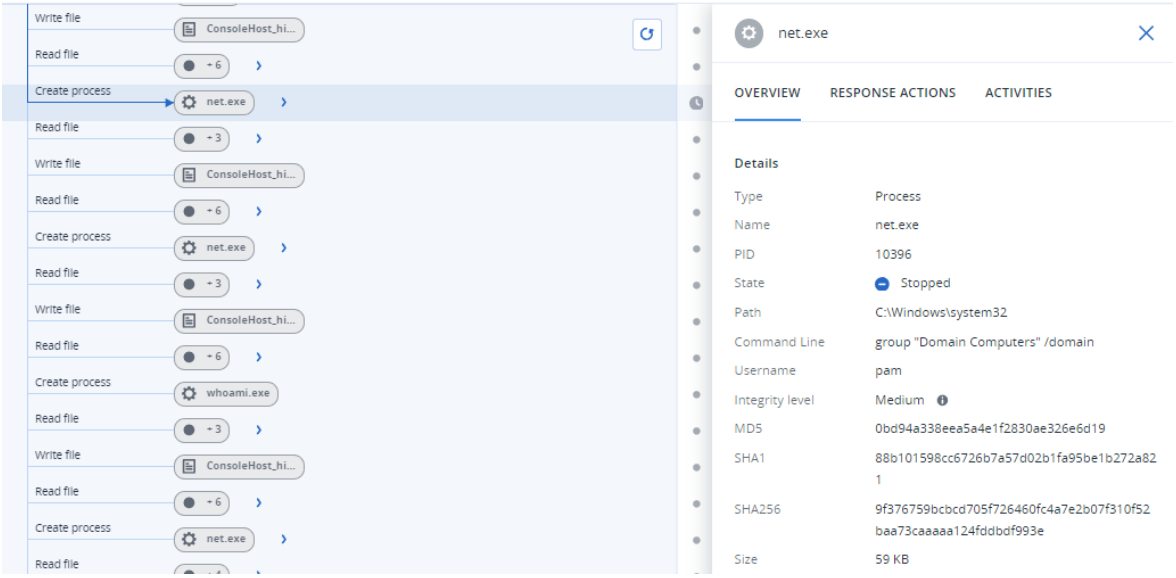
Nota
Cuando se implemente la EDR, debería ver incidentes inmediatamente si ocurre cualquier actividad sospechosa. Los pasos indicados a continuación le permiten comprobar si la EDR funciona si no se desencadenan incidentes nuevos durante varios días.

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.
   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.



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. 962). También puede escribir un comentario para el incidente para indicar que fue

un incidente de la prueba.

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" (p. 1010).
- macOS. Para obtener más información, consulte "Productos de Apple y de terceros compatibles" (p. 1011).
- Equipos Linux (CentOS 7/Virtuozzo/Acronis Cyber Infrastructure). Para obtener más información, consulte "Productos de Linux compatibles" (p. 1012).

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" (p. 1010).

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**.

Productos de Microsoft y de terceros compatibles

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

Sistema operativo Windows

- Windows 7 (Enterprise, Professional y Ultimate)
- Windows 8
- Windows 8.1
- Windows 10
- Windows 11

Sistema operativo Windows Server

- 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 relacionados con el sistema operativo Windows

- Internet Explorer
- Microsoft EDGE
- Windows Media Player
- .NET Framework
- Visual Studio y aplicaciones
- Componentes del sistema operativo

Aplicaciones del servidor

- Microsoft SQL Server 2008 R2
- Microsoft SQL Server 2012
- Microsoft SQL Server 2014
- Microsoft SQL Server 2016
- Microsoft SQL Server 2017
- Microsoft SQL Server 2019
- Microsoft Exchange Server 2013
- Microsoft Exchange Server 2016
- Microsoft Exchange Server 2019
- Microsoft SharePoint Server 2016
- Microsoft SharePoint Server 2019

Productos de terceros compatibles con Windows

El trabajo remoto se extiende cada vez más por el mundo, por lo que es importante que los clientes VPN y las herramientas de colaboración y comunicación estén siempre actualizados, así como que se analicen en busca de posibles vulnerabilidades. El servicio Cyber Protection permite realizar evaluación de vulnerabilidades y gestión de parches para tales aplicaciones.

Herramientas de colaboración y comunicación, clientes VPN

- Microsoft Teams
- Zoom
- Skype
- Slack
- Webex
- NordVPN
- TeamViewer

Para obtener más información sobre los productos de terceros compatibles para Windows, consulte Lista de productos de terceros compatibles con gestión de parches (62853).

Productos de Apple y de terceros compatibles

Los siguientes productos de Apple y de terceros para macOS son compatibles con la evaluación de vulnerabilidades:

Productos de Apple compatibles

macOS

- 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
- Skype
- Thunderbird
- VLC media player

Productos de Linux compatibles

Distribuciones Linux y versiones de este sistema operativo que son compatibles con la evaluación de vulnerabilidades:

- 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 cuando esté planificado 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:

- Equipos Windows:
  - **Productos de Microsoft**
  - **Productos de terceros compatibles con Windows**: para obtener más información sobre los productos de terceros compatibles para Windows, consulte Lista de productos de terceros compatibles con gestión de parches (62853).

- 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: • **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

Campo	Descripción
	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 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**

Campo	Descripción
	• **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.

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 **Productos de Microsoft**, **productos de terceros para Windows** 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. 1012).
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**.

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. 1012).

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. 1012).
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.

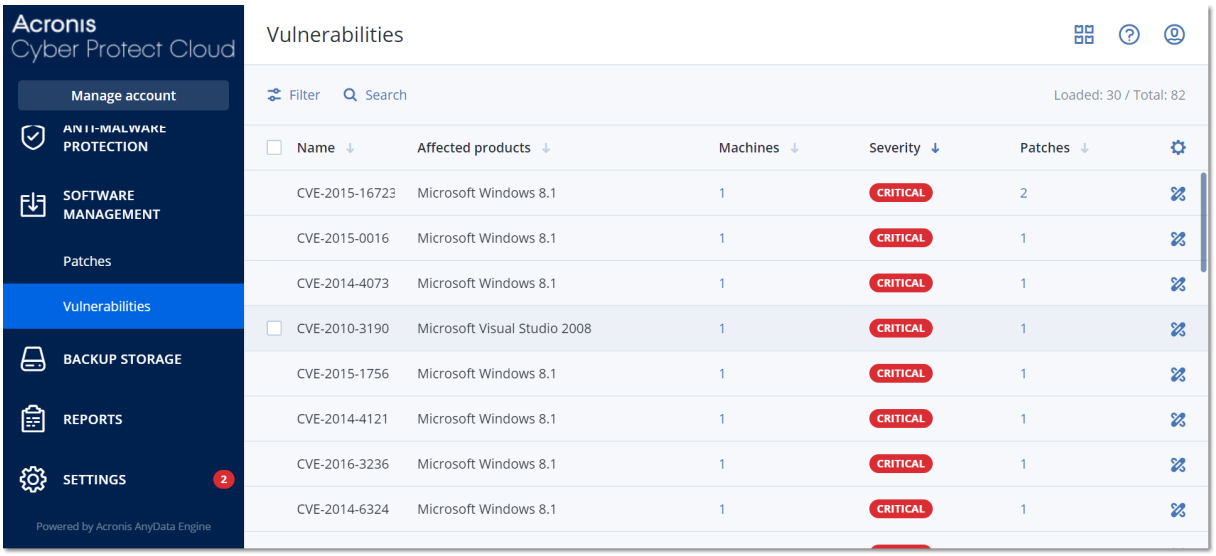
Para comprobar los resultados de la evaluación de vulnerabilidades, consulte los widgets de **Supervisión** > **Información general** > **Vulnerabilidades/Vulnerabilidades existentes**.

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.



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.
   a. Seleccione si quiere que el equipo se reinicie después de instalar los parches.

Opción	Descripción
No	Los equipos no se reiniciarán automáticamente después de instalar los parches.
Si es necesario	Los equipos se reiniciarán únicamente si es necesario para aplicar los parches.
Sí	Los equipos se reiniciarán automáticamente después de instalar los parches. También puede especificar cuándo tendrá lugar el reinicio.

   b. [Opcional] Si quiere programar el reinicio del equipo mientras se está realizando una copia de seguridad del equipo, seleccione **No reiniciar hasta que finalice la copia de seguridad**.
6. Haga clic en **Instalar parches**.

Como resultado, los parches seleccionados se instalan en los equipos indicados.

Gestión de parches

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

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 actualizaciones de Windows, la función de gestión de parches requiere que las actualizaciones de Windows estén habilitadas en la carga de trabajo.

Cyber Protection presenta 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 en 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, 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. 1012).
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. 1019)
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. 1027). También puede aprobar los parches manualmente cambiando su estado de aprobación a **Aprobado**. Para obtener más información, consulte "Aprobar parches manualmente" (p. 1032).
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. 1032).

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. 223).

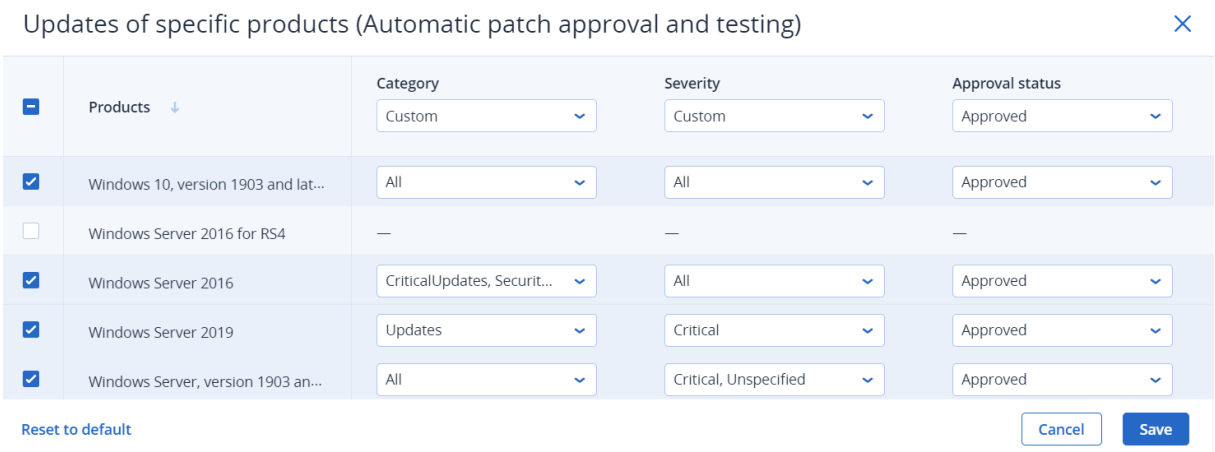
Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

Productos de Microsoft

Para instalar las actualizaciones de Microsoft en los equipos seleccionados, habilite la opción **Actualizar productos de Microsoft**.

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.



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.

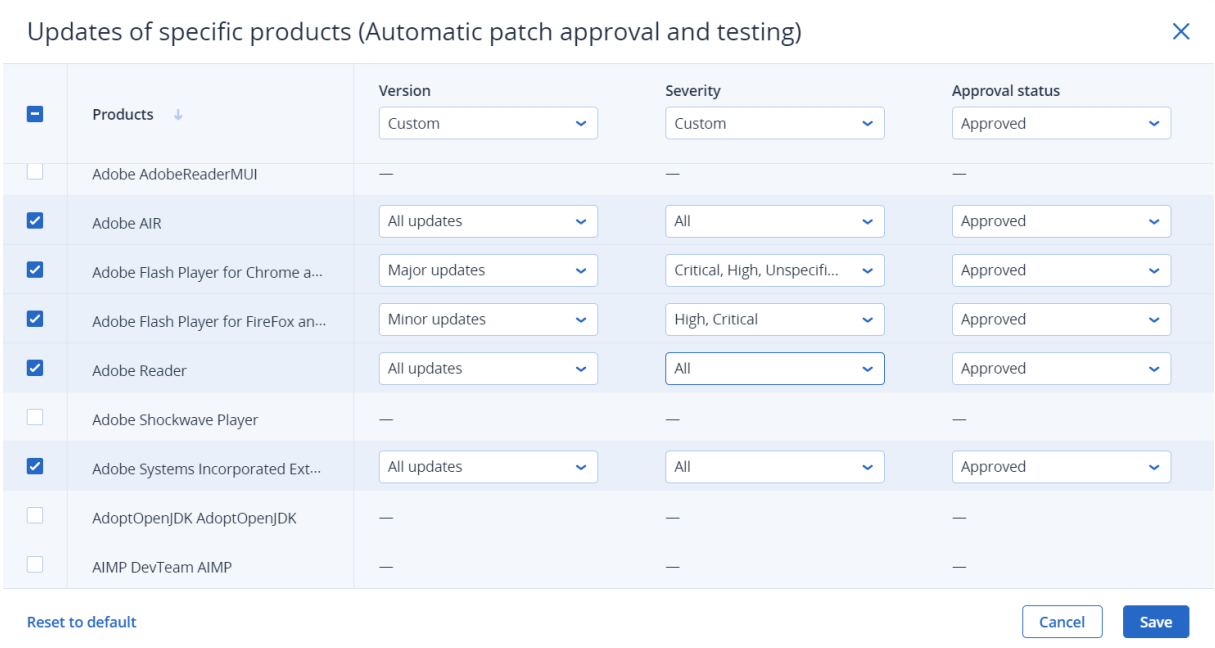
Productos de terceros a Windows

Para instalar las actualizaciones de terceros para Windows en los equipos seleccionados, habilite la opción **Productos de terceros para Windows**.

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	Seleccione esta casilla de verificación si desea instalar las últimas actualizaciones solo para las aplicaciones en las que se hayan detectado vulnerabilidades. *

* Esta opción requiere la versión 23.11.36772 del agente Cyber Protect o posterior.



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.

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.

Campo	Descripción
	• **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 periodo de mantenimiento para parches	El campo se muestra si, en **Planificar la ejecución de tareas con los 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	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**.

Campo	Descripción
sistema operativo iniciará una tarea	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.
Reiniciar después de la actualización	Defina si reiniciar automáticamente el equipo una vez que se complete la instalación de las actualizaciones. Los valores disponibles son los siguientes: • **Nunca**: los equipos no se reiniciarán nunca después de las actualizaciones. • **Si es necesario**: el reinicio tendrá lugar únicamente si es necesario para aplicar las actualizaciones. • **Siempre**: siempre se reiniciará el equipo tras las actualizaciones. Puede especificar cuándo tendrá lugar el reinicio.
No reiniciar hasta que la copia de seguridad haya	Si selecciona esta opción, se retrasará el reinicio del equipo hasta que finalice la copia de seguridad en caso de que se esté ejecutando un proceso de copia de seguridad.

Campo	Descripción
finalizado	

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**.

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.

Campo	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.
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. • **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 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. 1028).

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. 1031).

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.
   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. 1028).
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. 1029).
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, consulte "Configurar el plan de protección Instalación de parches en entornos de producción" (p. 1030).
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. 1031).
5. Ejecute el plan Instalación de parches en entornos de producción.

Configurar el plan de protección Instalación de parches en entornos de prueba

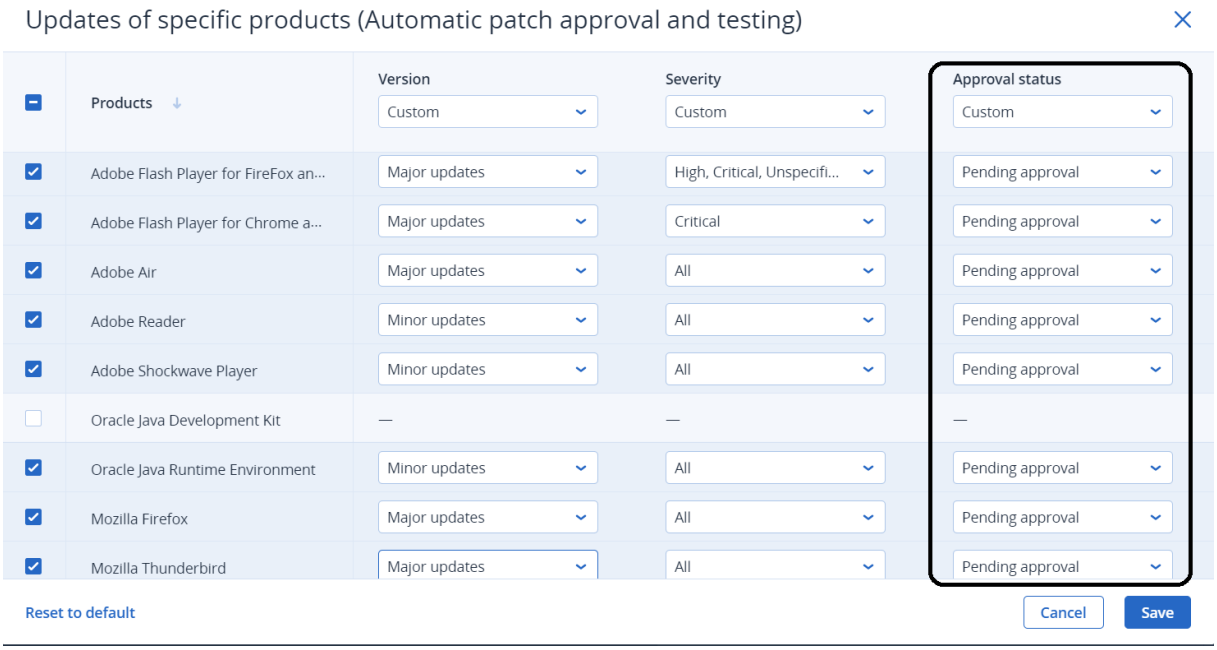
Puede configurar un plan de protección con ajustes de instalación de parches para sus equipos en el entorno de prueba.

Pasos para configurar el plan de protección Instalación de parches en entornos de prueba

1. En la consola de Cyber Protect, vaya a **Administración** > **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. 1019).

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.



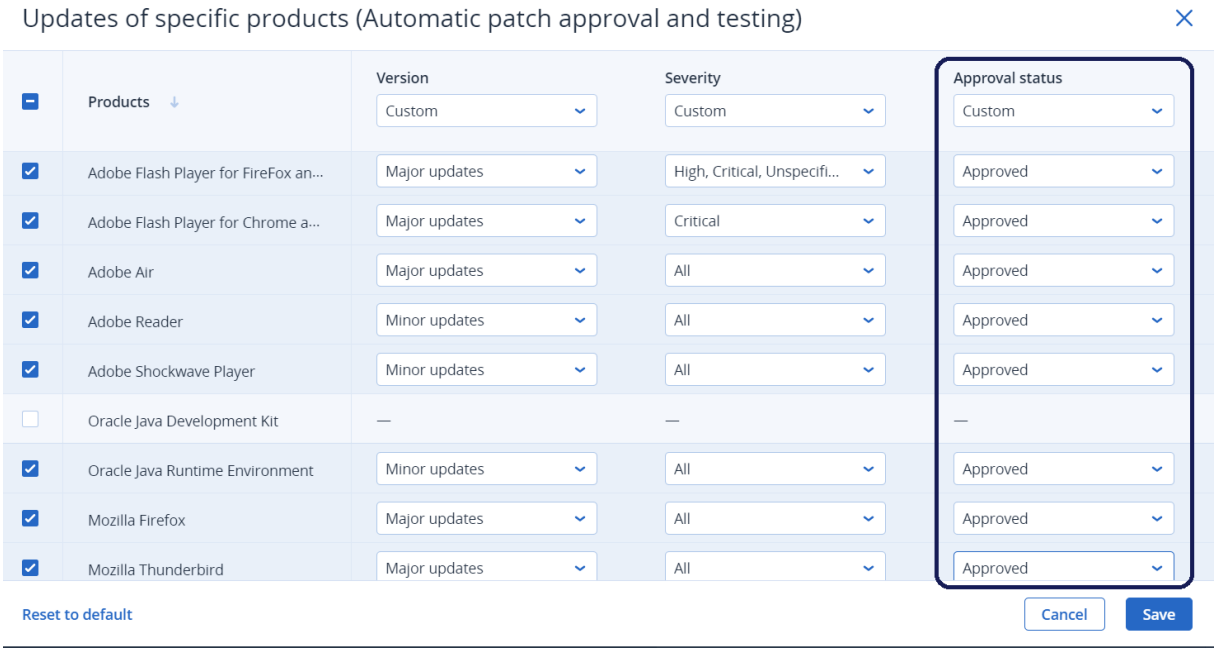
Configurar el plan de protección Instalación de parches en entornos de producción

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 **Administración** > **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. 1019).

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.



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. 1028).

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. 1030).
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. 1032).

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**.

Pasos para instalar un parche manualmente

Desde Parches

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.
   a. Seleccione si quiere que el equipo se reinicie después de instalar los parches.

Opción	Descripción
No	Los equipos no se reiniciarán automáticamente después de instalar los parches.
Si es necesario	Los equipos se reiniciarán únicamente si es necesario para aplicar los parches.
Sí	Los equipos se reiniciarán automáticamente después de instalar los parches. También puede especificar cuándo tendrá lugar el reinicio.

   b. [Opcional] Si quiere programar el reinicio del equipo mientras se está realizando una copia de seguridad del equipo, seleccione **No reiniciar hasta que finalice la copia de seguridad**.
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. 1016).

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.
   a. Seleccione si quiere que el equipo se reinicie después de instalar los parches.

Opción	Descripción
No	Los equipos no se reiniciarán automáticamente después de instalar los parches.
Si es necesario	Los equipos se reiniciarán únicamente si es necesario para aplicar los parches.
Sí	Los equipos se reiniciarán automáticamente después de instalar los parches. También puede especificar cuándo tendrá lugar el reinicio.

   b. [Opcional] Si quiere programar el reinicio del equipo mientras se está realizando una copia de seguridad del equipo, seleccione **No reiniciar hasta que finalice la copia de seguridad**.
6. Haga clic en **Instalar parches**.

Gestión del inventario de software y hardware

Inventario de software

La función de inventario de software está disponible para los dispositivos que tengan el paquete Advanced habilitado o que cuenten con una licencia de Cyber Protect (heredada). La función le permite visualizar todas las aplicaciones de software instaladas en 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 el análisis de 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.

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.

Pasos para habilitar el análisis de inventario de software

1. En la consola de Cyber Protect, vaya a **Configuración**.
2. Haga clic en **Protección**.
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**.

Pasos para deshabilitar el análisis de inventario de software

1. En la consola de Cyber Protect, vaya a **Configuración**.
2. Haga clic en **Protección**.
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**.

Ejecución manual de un análisis de inventario de software

Puede ejecutar manualmente un análisis de inventario de software desde la pantalla **Inventario de software**, o bien desde la pestaña **Software** de la pantalla **Inventario**.

Requisitos previos

- El dispositivo debe tener un sistema operativo Windows o macOS.
- El dispositivo tiene la licencia de Cyber Protect (heredada) necesaria o tiene un paquete Advanced Management activado.

Pasos para ejecutar 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 campo desplegable **Agrupar por:**, seleccione **Dispositivos**.
4. Busque el dispositivo que desee analizar y haga clic en **Analizar ahora**.

Pasos para ejecutar un análisis de inventario de software desde la pestaña Software de la pantalla Inventario

1. En la consola de Cyber Protect, vaya a **Dispositivos**.
2. Haga clic en el dispositivo que desee analizar, y haga clic en **Inventario**.
3. En la pestaña **Software**, haga clic en **Analizar ahora**.

Búsqueda en el inventario de software

Puede visualizar y buscar los datos de todas las aplicaciones de software que están disponibles en todos los dispositivos de la empresa.

Requisitos previos

- Los dispositivos deben tener un sistema operativo Windows o macOS.
- Los dispositivos tienen la licencia de Cyber Protect (heredada) necesaria o tienen un paquete Advanced Management activado.
- El análisis de inventario de software de los dispositivos se ha realizado correctamente.

Pasos para visualizar todas las aplicaciones de software disponibles en los dispositivos con Windows y macOS de la empresa

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.
Rango	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.
Usuario	Usuario que ha instalado 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 **Filtrar**.
   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.

Filtro	Descripción
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.
Rango	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**.

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 el campo desplegable, seleccione el número 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, así como 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 de Cyber Protect (heredada) necesaria o tiene un paquete Advanced Management activado.
- El análisis de inventario de software del dispositivo se ha realizado correctamente.

Pasos para visualizar el inventario de software de un solo 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 campo desplegable **Agrupar por:**, seleccione **Dispositivos**.
4. Busque el dispositivo que desee inspeccionar mediante una de las opciones siguientes.
   - Buscar el dispositivo mediante la opción **Filtrar**:
     a. Haga clic en **Filtrar**.
     b. En el campo **Nombre de dispositivo**, seleccione el nombre del dispositivo que desea ver.
     c. Haga clic en **Aplicar**.
   - Buscar el dispositivo mediante la opción de **Buscar** dinámicamente:
     a. Haga clic en **Buscar**.
     b. Escriba el nombre completo del dispositivo o parte del mismo.

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 desee ver, y haga clic en **Inventario**.
3. Haga clic en la pestaña **Software**.

Inventario de hardware

La función de inventario de hardware le permite visualizar todos los componentes de hardware 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. 32).

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 activos de hardware de la organización
- buscar en el inventario de hardware de todos los dispositivos de su organización
- comparar los componentes de hardware de los diversos dispositivos de la empresa
- ver información detallada acerca de un componente de hardware.

Habilitar 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.

Pasos para habilitar el análisis de inventario de hardware

1. En la consola de Cyber Protect, vaya a **Configuración**.
2. Haga clic en **Protección**.
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**.

Pasos para deshabilitar el análisis de inventario de hardware

1. En la consola de Cyber Protect, vaya a **Configuración**.
2. Haga clic en **Protección**.
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**.

Ejecución manual de un análisis de inventario de hardware

Puede ejecutar manualmente un análisis de inventario de hardware para un solo dispositivo, así como visualizar 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

- (Para todos los dispositivos) El dispositivo tiene un sistema operativo Windows o macOS.
- (Para todos los dispositivos) Los dispositivos tienen una licencia que admite la función de inventario de hardware. Tenga en cuenta que la función de inventario de hardware para las máquinas virtuales no es compatible con las ediciones de Cyber Protect (heredadas).
- (Para todos los dispositivos) Un agente de protección está instalado en el dispositivo.
- (Para máquinas virtuales) La máquina se ejecuta en una de las plataformas de virtualización compatibles. Para obtener más información, consulte "Inventario de hardware" (p. 1038).

Pasos para ejecutar un análisis de inventario de hardware en un solo dispositivo

1. En la consola de Cyber Protect, vaya a **Dispositivos**.
2. Haga clic en el dispositivo que desee analizar, y haga clic en **Inventario**.
3. En la pestaña **Hardware**, haga clic en **Analizar ahora**.

Búsqueda en el inventario de hardware

Puede visualizar y buscar los datos de todos los componentes de hardware que están disponibles en todos los dispositivos de la empresa.

Requisitos previos

- (Para todos los dispositivos) Los dispositivos deben tener un sistema operativo Windows o macOS.
- (Para todos los dispositivos) Los dispositivos deben tener una licencia compatible con la característica del inventario de hardware. Tenga en cuenta que la característica del inventario de hardware para las máquinas virtuales no es compatible con las ediciones heredadas de Cyber Protect.
- (Para todos los dispositivos) Un agente de protección está instalado en el dispositivo.
- (Para todos los dispositivos) El análisis de inventario de hardware de los dispositivos se ha realizado correctamente.
- (Para máquinas virtuales) La máquina se ejecuta en una de las plataformas de virtualización compatibles. Para obtener más información, consulte "Inventario de hardware" (p. 1038).

Pasos para visualizar todos los componentes de hardware disponibles en los dispositivos con Windows y macOS de la empresa

1. En la consola de Cyber Protect, vaya a **Dispositivos**.
2. En el campo desplegable **Vista:**, seleccione **Hardware**.

Nota
La 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**. • El estado **No compatible** se muestra para aquellas cargas de trabajo que no son compatibles con la funcionalidad de inventario de hardware, como equipos virtuales, dispositivos móviles o dispositivos con Linux. • **Actualizar agente** se muestra cuando el dispositivo tiene instalada una versión desactualizada del agente. Al hacer clic en esta acción, se le redirigirá a la página Configuración > Agentes, donde el administrador puede actualizar el agente. • **Actualizar cuota**. Al hacer clic aquí, se abrirá un cuadro de diálogo donde el administrador puede cambiar la licencia actual por otra disponible para licencias de 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.

Columna	Descripción
Número de serie de la placa base	El número de serie de la placa base.
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.

3. Para añadir columnas a la tabla, haga clic en el icono de opciones de la columna y seleccione aquellas columnas que desee incluir en la tabla.
4. 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. 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

- (Para todos los dispositivos) El dispositivo tiene un sistema operativo Windows o macOS.
- (Para todos los dispositivos) Los dispositivos deben tener una licencia compatible con la característica del inventario de hardware. Tenga en cuenta que la característica del inventario de hardware para las máquinas virtuales no es compatible con las ediciones heredadas de Cyber Protect.
- (Para todos los dispositivos) Un agente de protección está instalado en el dispositivo.
- (Para todos los dispositivos) El análisis de inventario de hardware del dispositivo se ha realizado correctamente.
- (Para máquinas virtuales) La máquina se ejecuta en una de las plataformas de virtualización compatibles. Para obtener más información, consulte "Inventario de hardware" (p. 1038).

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 **Filtrar**:
     a. Haga clic en **Filtrar**.
     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.

Componente de hardware	Información que se muestra
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, versión del BIOS, dispositivo de arranque, configuración regional del sistema y zona horaria del sistema.

Conexión a cargas de trabajo para asistencia o escritorio remotos

La funcionalidad de escritorio remoto y asistencia remota es una forma cómoda de conectarse a las cargas de trabajo de su organización para controlarlas o recibir asistencia de forma remota. A partir de diciembre de 2022, la funcionalidad es compatible con los protocolos NEAR, RDP y el uso compartido de pantalla de Apple. Para obtener más información, consulte "Protocolos de conexión remota" (p. 1050).

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.

Para obtener más información acerca de las características que forman parte de los paquetes de Standard y Advanced Management, consulte "Funciones de asistencia y escritorio remotos" (p. 1047).

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.

Para obtener más información acerca de las características que forman parte de la protección estándar y Advanced Management, consulte "Funciones de asistencia y escritorio remotos" (p. 1047).

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.

Por ejemplo, puede crear un plan de administración remota que solo tenga habilitado el protocolo RDP y aplicarlo a varias cargas de trabajo. De esa forma, podrá conectarse de forma remota a esas cargas de trabajo sin activar la licencia de Advanced Management por carga de trabajo y sin pagar costes adicionales.

Por otro lado, puede crear otro plan de administración remota que tenga activados los protocolos NEAR y el uso compartido de pantalla de Apple. En este caso, se activará la licencia de Advanced Management por carga de trabajo y se le cobrará por cada carga de trabajo a la que se aplique este plan de administración remota.

Para obtener más información acerca de los planes de administración remota y trabajar con ellos, consulte "Planes de administración remota" (p. 1054).

Nota

La funcionalidad de asistencia y escritorio remotos requiere:

- una sola instalación de Cliente de Connect en la carga de trabajo (host) gestionada. El sistema le sugerirá que descargue el cliente cuando intente ejecutar una acción remota (control remoto o asistencia remota) en una carga de trabajo de destino por primera vez. De forma alternativa, puede descargar Cliente de Connect desde la ventana **Descargas** en la consola de Protección. Para obtener más información acerca de los ajustes que puede configurar, consulte "Configuración de los ajustes de Cliente de Connect" (p. 1086).
- 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. 85).
- 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 "Plataformas compatibles" (p. 1049).

Funciones de asistencia y escritorio remotos

La siguiente tabla le ofrece más información acerca de los cambios de las funciones compatibles de asistencia y escritorio remotos que se incorporaron en diciembre de 2022.

Característica	Protección estándar antes de diciembre de 2022	Advanced Management antes de diciembre de 2022	Protección estándar después de diciembre de 2022	Advanced Management después de diciembre de 2022
Asistencia remota a través de RDP para Windows	Sí	No	No	No
Compartir una conexión remota con usuarios	No	Sí	No	No
Conexiones remotas				
Acciones remotas	No	No	Sí	Sí
Selección de una sesión para conectarse a Windows, macOS o Linux	No	No	No	Sí
Conexión directa mediante RDP y el uso compartido de pantalla de Apple	No	No	No	Sí
Control de varias ventanas	No	No	No	Sí
Modos de conexión: control, solo visualización y cortina	No	No	No	Sí
Compatibilidad con credenciales comunes para conexiones remotas	No	No	Sí	Sí
Conexiones simultáneas por técnico				
a través de RDP	Sí	Sí	Sí	Sí
a través de NEAR	No	No	No	Sí
Transferencia y uso compartido de archivos				
de Windows a Windows,	No	No	No	Sí

Característica	Protección estándar antes de diciembre de 2022	Advanced Management antes de diciembre de 2022	Protección estándar después de diciembre de 2022	Advanced Management después de diciembre de 2022
macOS o Linux				
de macOS a Windows, macOS o Linux	No	No	No	Sí
de Linux a Windows, macOS o Linux	No	No	No	Sí
Conexión mediante la aplicación Asistencia rápida				
de Windows a Windows, macOS o Linux	No	No	No	Sí
de macOS a Windows, macOS o Linux	No	No	No	Sí
de Linux a Windows, macOS o Linux	No	No	No	Sí
Conexiones remotas mediante protocolos				
Conexión remota a través de NEAR				
de Windows a Windows, macOS o Linux	No	No	No	Sí
de macOS a Windows, macOS o Linux	No	No	No	Sí
de Linux a Windows, macOS o Linux	No	No	No	Sí
Conexión remota a través de RDP (cliente de escritorio)				
de Windows a Windows	Sí	Sí	Sí	Sí
de macOS a Windows	Sí	Sí	Sí	Sí
de Linux a Windows	No	No	Sí	Sí
Conexión remota a través de RDP (cliente web)				
de Windows a Windows	Sí	Sí	Sí	Sí
de macOS a Windows	Sí	Sí	Sí	Sí
de Linux a Windows	No	No	Sí	Sí

Característica	Protección estándar antes de diciembre de 2022	Advanced Management antes de diciembre de 2022	Protección estándar después de diciembre de 2022	Advanced Management después de diciembre de 2022
Conexión remota a través del uso compartido de pantalla de Apple				
de Windows, macOS o Linux a macOS	No	No	No	Sí
Administración de sesiones				
Grabación de sesiones	No	No	No	Sí
Informes y supervisión				
Historial de sesiones y búsqueda	No	No	No	Sí
Transmisión de captura de pantalla	No	No	No	Sí

Plataformas compatibles

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 y 8.1

Componente del escritorio remoto	Plataformas compatibles
	Fedora 30 Ubuntu 18.4 LTS (Bionic Beaver) -19.04 (Disco 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 y 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.

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. 1051).

- ### 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. 1050).

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.

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. 86).

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.

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

Conexión directa	Opción de conexión directa	Acción remota compatible	Disponible para
			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

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 configuración que puede configurar en el plan de administración remota depende del paquete de servicios que se aplica al inquilino. Para acceder a toda la configuración, active el paquete de Advanced Management. Para obtener más información acerca de las características que forman parte de los paquetes de Standard y Advanced Management, consulte "Funciones de asistencia y escritorio remotos" (p. 1047).

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 cuota de servicio que está asignada al inquilino. Si usa la funcionalidad estándar, solo puede configurar conexiones a través de RDP.

Requisitos previos

La autenticación de doble factor está habilitada en su cuenta de usuario.

Pasos para crear un plan de administración remota

Desde planes de administración remota

1. En la consola de Cyber Protect, vaya a **Administración** > **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 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 y 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 y 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 creación de sesión del sistema** están desactivadas, solo podrá conectarse a sesiones de administrador	Windows y macOS

Configuración	Descripción	Disponible para
	activas en las cargas de trabajo remotas de 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 y Linux

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 cargas 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	Windows, macOS y Linux

Configuración	Descripción	Disponible el
	trabajo locales y remotas.	
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 y Linux

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
Use la codificación H.264 de hardware	NEAR es compatible con tres	Windows y macOS

Configuración	Descripción	Disponible el
	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.	

9. Si desea que la información sobre los usuarios que iniciaron sesión por última vez en las cargas de trabajo esté disponible en la información de la carga de trabajo, haga clic en **Caja de herramientas**, seleccione **Mostrar últimos usuarios que iniciaron sesión** y, a continuación, haga clic en **Listo**.

   Para obtener más información sobre los usuarios que iniciaron sesión por última vez, consulte "Buscar el último usuario que ha iniciado sesión" (p. 411).
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 **Añadir**.
    c. Si hay problemas de compatibilidad que desea resolver, siga el procedimiento descrito en "Resolución de problemas de compatibilidad con planes de administración remota" (p. 1067).

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 y 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 y 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 creación de sesión del**	Windows y macOS

Configuración	Descripción	Disponible para
	sistema están desactivadas, solo podrá conectarse a sesiones de administrador activas en las cargas de trabajo remotas de 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 y Linux

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 cargas 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 y 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 y Linux

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**.

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

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 y macOS

11. Si desea que la información sobre los usuarios que iniciaron sesión por última vez en las cargas de trabajo esté disponible en la información de la carga de trabajo, haga clic en **Caja de herramientas**, seleccione **Mostrar últimos usuarios que iniciaron sesión** y, a continuación, haga clic en **Listo**.

    Para obtener más información sobre los usuarios que iniciaron sesión por última vez, consulte "Buscar el último usuario que ha iniciado sesión" (p. 411).
12. Haga clic en **Crear**.

Adición de una carga de trabajo a un plan de administración remota

Según sus necesidades, puede añadir cargas de trabajo a un plan de administración remota después de crearlo.

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 **Administración** > **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 **Administración** > **Planes de administración remota**.
2. Haga clic en el plan de administración remota.
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**.

Operaciones adicionales con planes de administración remota existentes

Desde la pantalla **Plan de administración remota**, puede realizar las operaciones adicionales siguientes con los planes de administración remota: ver detalles, editar, ver actividades, ver alertas, cambiar nombre, habilitar, deshabilitar, clonar, exportar 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 **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 **Más acciones** del plan de administración remota.
2. Haga clic en **Editar**.

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 **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

1. En la pantalla **Planes de administración remota**, haga clic en el icono **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 **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 **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 **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 **Más acciones** del plan de administración remota.
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 **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.

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 **Más acciones** del plan de administración remota.
2. Haga clic en **Eliminar**.
3. Seleccione **Confirmo** y, a continuación, haga clic en **Eliminar**.

Problemas de compatibilidad con planes de administración remota

En algunos casos, aplicar un plan de administración remota en una carga de trabajo podría causar problemas de compatibilidad. Es posible que observe los siguientes problemas de compatibilidad:

- Planes en conflicto: este problema aparece cuando otro plan de administración remota ya se ha aplicado a la carga de trabajo, ya que solo se puede aplicar un plan de administración remota a una carga de trabajo.
- El sistema operativo es incompatible: este problema aparece cuando el sistema operativo de la carga de trabajo no es compatible.
- Agente no compatible: este problema aparece cuando la versión del agente de protección de la carga de trabajo está obsoleta y no es compatible con la funcionalidad de escritorio remoto.
- Cuota insuficiente: este problema aparece cuando no hay una cuota de servicio suficiente en el inquilino para asignarla a las cargas de trabajo seleccionadas.

Si se aplica el plan de administración remota a un máximo de 150 cargas de trabajo seleccionadas de forma individual, se le pedirá que resuelva los conflictos existentes antes de guardar el plan.

Para resolver un conflicto, elimine la causa raíz o las cargas de trabajo afectadas desde el plan. Para obtener más información, consulte "Resolución de problemas de compatibilidad con planes de administración remota" (p. 1067). Si guarda el plan sin resolver los conflictos, se deshabilitará automáticamente para las cargas de trabajo no compatibles y se mostrarán alertas.

Si se aplica el plan de administración remota a más de 150 cargas de trabajo o grupos de dispositivos, primero se guardará y, después, se comprobará la compatibilidad. El plan se deshabilitará automáticamente para las cargas de trabajo incompatibles y se mostrarán las alertas.

Resolución de problemas de compatibilidad con planes de administración remota

Según la causa de los problemas de compatibilidad, puede ejecutar diferentes acciones para resolverlos como parte del proceso de creación de un nuevo plan de administración remota.

Nota
Al resolver un problema de compatibilidad mediante la eliminación de cargas de trabajo de un plan, no puede eliminar las cargas de trabajo que son parte de un grupo de dispositivos.

Pasos para resolver problemas de compatibilidad

1. Haga clic en **Revise los problemas**.
2. [Pasos para resolver problemas de compatibilidad con los planes de administración remota existentes mediante la eliminación de cargas de trabajo desde el nuevo plan]
   a. En la pestaña **Planes en conflicto**, 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. [Pasos para resolver problemas de compatibilidad con los planes de administración remota mediante la deshabilitación de los planes que ya se han aplicado a las cargas de trabajo]
   a. Haga clic en **Deshabilitar los planes aplicados**.
   b. Haga clic en **Deshabilitar** y, a continuación, haga clic en **Cerrar**.
4. [Para resolver problemas de compatibilidad con sistemas operativos no compatibles]
   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**.
5. [Para resolver problemas de compatibilidad con agentes no compatibles mediante la eliminación de cargas de trabajo desde el plan]
   a. En la pestaña **Agentes no compatibles**, 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**.

6. [Para resolver problemas de compatibilidad con agentes no compatibles mediante la actualización de la versión del agente] Haga clic en **Ir a la lista de agentes**.

   Nota
   Esta opción solamente está disponible para los administradores de clientes.

7. [Para resolver problemas de compatibilidad con una cuota insuficiente mediante la eliminación de cargas de trabajo desde el plan]
   a. En la pestaña **Cuota insuficiente**, 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**.
8. [Para resolver problemas de compatibilidad con una cuota insuficiente mediante el aumento de la cuota del cliente]

   Nota
   Esta opción solamente está disponible para los administradores de partner.

   a. En la pestaña **Cuota insuficiente**, haga clic en **Ir al portal de administración**.
   b. Aumentar la cuota de servicio para el cliente.

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

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.

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 **Añadir credenciales**.
4. En el **Almacén de credenciales**, seleccione las credenciales de la lista y haga clic en **Seleccionar credenciales**.

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 control, solo visualización o en modo 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

- 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.
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.

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

- Un plan de administración remota con el protocolo de conexión correspondiente habilitado se aplica a la carga de trabajo gestionada.
- La cuota de servicio requerida se asigna a la carga de trabajo. (La cuota de servicio se adquiere automáticamente cuando aplica un plan de administración remota a la carga de trabajo).
- [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 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	**Controlar**: 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	**Controlar**: En este modo, podrá ver y ejecutar operaciones en la carga de trabajo remota.	Escritorio remoto

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 **Deshabilitarlo una vez finalizada 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	**Controlar**: 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. 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**.
7. 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. 1069).

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.

8. 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).
   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. 1083).

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.

Requisitos previos

- La cuota de servicio estándar se asigna a la carga de trabajo.
- Un plan de administración remota con RDP habilitado se aplica a la carga de trabajo administrada.
- 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. Introduzca el nombre de usuario y la contraseña para acceder a la carga de trabajo y haga clic en **Conectar**.

> **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. 1069).

Transferir archivos

Puede transferir fácilmente archivos entre la carga de trabajo local y una carga de trabajo gestionada.

Requisitos previos

- Un plan de administración remota con el protocolo NEAR y la transferencia de archivos habilitados se aplica a la carga de trabajo.
- La cuota de Advanced Management se aplica a la carga de trabajo.
- 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. 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, haga clic en **Permitir**.
- Si Cliente de Connect ya está instalado, en la ventana emergente de confirmación que aparece, haga clic en **Abrir Cliente de Connect**.

5. 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 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.

6. 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**.

7. [Opcional] Si desea eliminar las tareas completadas del panel de **Tareas**, haga clic en **Borrar completadas**.
8. Cuando se completen todas las transferencias, cierre la ventana.

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 cuota de servicio estándar se aplica a la carga de trabajo.
- 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**.
4. 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**.

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**.
   - 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**.
   - 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

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. Seleccione el usuario del que desea cerrar sesión y, a continuación, haga clic en **Cerrar sesión**.

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

- Un plan de administración remota con la función de transmisión de captura de pantalla habilitada se aplica a la carga de trabajo.
- La versión del agente de protección está actualizada y es compatible con la función de transmisión de capturas de pantalla.
- La cuota de servicio de Advanced Management se aplica a la carga de trabajo.
- La carga de trabajo está en línea.
- La autenticación de doble factor está habilitada en su cuenta de usuario en Acronis Cyber Protect Cloud.

Supervisión de una carga de trabajo mediante la transmisión de captura de pantalla

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. Seleccione la sesión de usuario.
4. Seleccione la pantalla.
5. Seleccione la tasa de actualización para hacer una nueva captura de pantalla del escritorio.
6. Seleccione la calidad de la imagen.
7. Para descargar la captura de pantalla, haga clic en el icono de descarga.

Captura de pantalla de una carga de trabajo

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**.
   La pantalla **Transmisión de captura de pantalla** se abrirá con la carga de trabajo preseleccionada. Según la configuración del plan de administración remota que se aplica a la

carga de trabajo, verá la captura de pantalla o la verá después de que el usuario de la carga de trabajo remota apruebe la solicitud.

Observar varias cargas de trabajo gestionadas de manera simultánea

Puede observar los escritorios de varias cargas de trabajo remotas de manera simultánea en una sola ventana.

Nota
El número de escritorios que puede ver de manera simultánea en la ventana depende del tamaño de su monitor.

Requisitos previos

- NEAR o el Uso compartido de la pantalla están habilitados en los planes de administración remota que se aplican a las cargas de trabajo.
- La cuota de servicio de Advanced Management se aplica a la carga de trabajo.
- 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. 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**.
5. 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

Opción de autenticación	Descripción
	carga de trabajo remota lo permita.

6. 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**.
7. 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.

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:

- El paquete de Advanced Management está activado para 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

- El paquete de Advanced Management 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

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. 1083).

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

- El paquete de Advanced Management 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.

   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. 1083).

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

- El paquete de Advanced Management 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.
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**

Icono	Descripción
	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.
	**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. 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 hayan 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 esta opción esté activada, el cliente sincronizará automáticamente su portapapeles local y el portapapeles del equipo remoto. Disponible para conexiones NEAR y a través del uso compartido de pantalla de Apple
Enviar portapapeles **Obtener portapapeles**	**Enviar portapapeles** reemplaza el contenido del portapapeles del equipo remoto con el contenido del portapapeles local. **Obtener portapapeles** transfiere el contenido del portapapeles del equipo remoto al portapapeles local.
Teclado inteligente/Teclas Raw/Teclas Raw con todos los accesos directos	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 **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

Opción	Descripción
Preferencias	Configure los ajustes de Cliente de Connect. Para obtener más información, consulte "Configuración de los ajustes de Cliente de Connect" (p. 1086).

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

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 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	Seleccione el intervalo de tiempo de inactividad después del cual

Opción	Descripción
inactiva	cerrar la ventana del Visor.

4. Configure los ajustes en la pestaña **Teclado**.

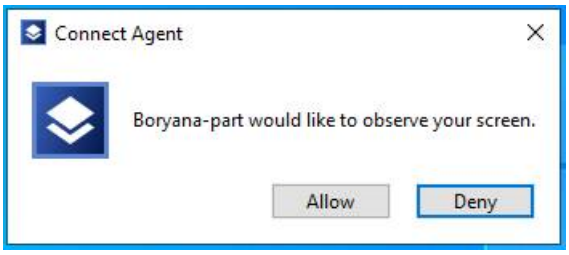
Opción	Descripción
Asignaciones de modificadores	Cambie el comportamiento de las claves del modificador con un menú emergente. Estos ajustes se almacenan de forma independiente para las conexiones NEAR, RDP y el uso compartido de pantalla de Apple.
Modo de entrada	Para cada tipo de conexión (seleccionada en el encabezado del panel), seleccione el modo de entrada predeterminado del teclado.

5. Haga clic en **Aceptar**.

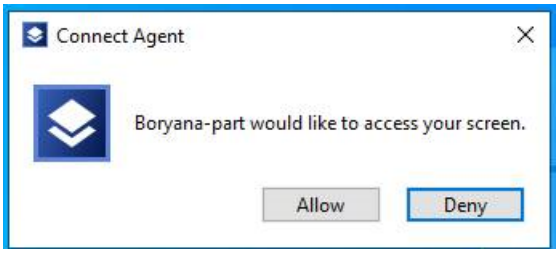
Los notificadores del escritorio remoto

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.

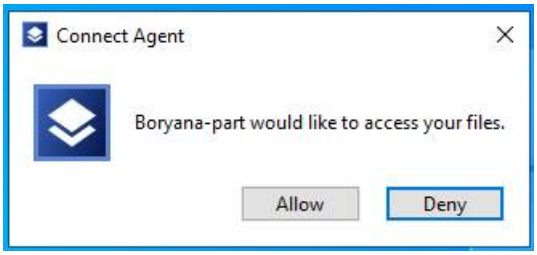


- cuando intenta conectarse a la carga de trabajo de forma remota pidiendo permiso para controlar. El usuario que ha iniciado sesión en la carga de trabajo remota de forma local puede permitir o denegar la solicitud.



- 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

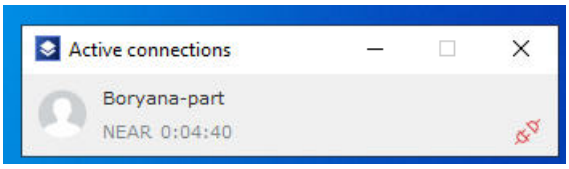
carga de trabajo remota de forma local puede permitir o denegar la solicitud.



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**.



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. 1125). Para obtener más información acerca de los monitores disponibles que puede configurar en los planes de supervisión, consulte "Monitores configurables" (p. 1091).

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. 1091).

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. 1136).

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)

Monitores configurables

La funcionalidad de supervisión es compatible con los siguientes monitores, divididos en seis categorías: hardware, rendimiento, software, sistema, seguridad y personalizado.

Monitor	Descripción	Sistemas operativos compatibles	Frecuencia de la recopilación de datos	Soporte para la supervisión basada en anomalías	Disponibilidad en la protección estándar o en Advanced Management
Hardware					
Espacio de disco	Supervisa el espacio libre en una unidad específica de la carga de trabajo.	Windows macOS	1 minuto	Sí	Protección estándar
Temperatura de CPU	Supervisa la temperatura de la CPU.	Windows macOS	30 seg	Sí	Advanced Management
Temperatura de GPU	Supervisa la temperatura de la GPU.	Windows macOS	30 seg	Sí	Advanced Management
Cambios del hardware	Supervisa los cambios de hardware, como añadir, eliminar o sustituir hardware en una carga de trabajo	Windows macOS	24 horas	No	Protección estándar
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	Advanced Management
Uso de la memoria	Supervisa el uso de la memoria total (por todas las ranuras de memoria de la carga de	Windows macOS	30 seg	Sí	Advanced Management

Monitor	Descripción	Sistemas operativos compatibles	Frecuencia de la recopilación de datos	Soporte para la supervisión basada en anomalías	Disponibilidad en la protección estándar o en Advanced Management
	trabajo).				
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	Advanced Management
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	Advanced Management
Uso de la CPU por proceso	Supervisa el uso que hace determinado proceso de la CPU.	Windows macOS	30 seg	No	Advanced Management
Uso de la memoria por proceso	Supervisa el uso de la memoria del proceso seleccionado.	Windows macOS	30 seg	No	Advanced Management
Velocidad de transferencia del disco por proceso	Supervisa la velocidad de lectura y escritura del proceso seleccionado.	Windows macOS	30 seg	No	Advanced Management
Uso de la red por proceso	Supervisa el tráfico de entrada y salida del proceso	Windows macOS	30 seg	No	Advanced Management

Monitor	Descripción	Sistemas operativos compatibles	Frecuencia de la recopilación de datos	Soporte para la supervisión basada en anomalías	Disponibilidad en la protección estándar o en Advanced Management
	seleccionado.				
Software					
Estado del servicio de Windows	Supervisa el estado del servicio de Windows seleccionado (En ejecución o detenido).	Windows	30 seg	No	Advanced Management
Estado del proceso	Supervisa el estado del proceso seleccionado (En ejecución o detenido).	Windows macOS	30 seg	No	Advanced Management
Software instalado	Supervisa la instalación, actualización o eliminación de aplicaciones de software.	Windows macOS	24 horas	No	Advanced Management
Sistema					
Último reinicio del sistema	Supervisa cuándo se ha reiniciado la carga de trabajo.	Windows macOS	1 hora	No	Protección estándar
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	Advanced Management

Monitor	Descripción	Sistemas operativos compatibles	Frecuencia de la recopilación de datos	Soporte para la supervisión basada en anomalías	Disponibilidad en la protección estándar o en Advanced Management
Tamaño de archivos y carpetas	Supervisa el tamaño total de los archivos o carpetas seleccionados.	Windows macOS	10 min	No	Protección estándar
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	Advanced Management
Estado del firewall	Supervisa el estado del cortafuegos integrado o de terceros que está instalado en la carga de trabajo.	Windows macOS	5 min	No	Advanced Management
Estado de software antimalware	Supervisa el estado del software antimalware integrado o de terceros que está instalado en la carga de trabajo.	Windows macOS	5 min	No	Advanced Management
Error al iniciar sesión	Supervisa los intentos de inicio de sesión sin éxito de la	Windows	1 hora	No	Advanced Management

Monitor	Descripción	Sistemas operativos compatibles	Frecuencia de la recopilación de datos	Soporte para la supervisión basada en anomalías	Disponibilidad en la protección estándar o en Advanced Management
	carga de trabajo.				
Estado de AutoRun	Supervisa si la función AutoRun está activada en el soporte de almacenamiento extraíble.	Windows	1 hora	No	Advanced Management
Personalizado					
Personalizado	Supervisa los objetos personalizados mediante la ejecución de secuencias de comandos.	Windows macOS	personalizado	No	Advanced Management

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. • **Cualquier unidad**
Operador	El operador es una función condicional que define cómo definir el

Configuración	Descripción
	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 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. • **Cualquier unidad**
Modelo de periodo de formación	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.

Configuración	Descripción
	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: • **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	
Modelo de periodo de formación	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. 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.

Configuración	Descripción
	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 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	
Modelo de periodo de	El periodo durante el cual el sistema formará a los modelos de aprendizaje automático según los datos que recopilen los agentes y

Configuración	Descripción
formación	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.
Duración de la anomalía	El sistema solo generará una alerta cuando detecte una anomalía si el comportamiento anómalo persiste en el periodo especificado.

Configuración	Descripción
	Escriba un valor entero en el intervalo 1-60 (min). El valor predeterminado es 15.

Configuración del monitor de cambios de hardware

Los cambios de 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. • **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

Configuración	Descripción
	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. Escriba un valor entero en el intervalo 1-60 (min). El valor predeterminado es 5.
Supervisión basada en anomalías	
Modelo de periodo de formación	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

Configuración	Descripción
	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	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.

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 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.
Supervisión basada en anomalías	
Modelo de periodo de formación	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

Configuración	Descripción
	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 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:

Configuración	Descripción
	• **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.
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	Descripción
Supervisión basada en anomalías	
Modelo de periodo de formación	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: • **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.

Configuración	Descripción
	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.
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.

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 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 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	
Modelo de periodo de formación	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

Configuración	Descripción
	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: 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.

Configuración	Descripción
	• **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.

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. 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** • **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	El sistema solo generará una alerta cuando detecte un problema si el valor del parámetro está fuera de la norma durante el periodo especificado.

Configuración	Descripción
velocidad de escritura	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 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. Los valores disponibles son los siguientes:

Configuración	Descripción
	• **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.

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.
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

Configuración	Descripción
	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.

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**

Configuración	Descripción
	• **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 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.

Configuración	Descripción
	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 • `?`: 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. No es obligatorio especificar una ubicación concreta para los filtros de exclusión. Los archivos introducidos sin una ubicación específica se excluirán en las carpetas supervisadas.
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

Configuración	Descripción
	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 actualización de Windows 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.

Configuración de la supervisión del estado del firewall

El estado del cortafuegos supervisa el firewall 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 firewall integrado en el SO (firewall de Windows Defender o firewall de macOS) está deshabilitado y no se ejecuta ningún firewall de terceros.
- El firewall de Windows Defender está deshabilitado para las redes públicas.
- El firewall de Windows Defender está deshabilitado para las redes privadas.
- El firewall 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.

Configuración	Descripción
	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.

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

Sistema operativo	Software antimalware admitido
	• 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 **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.
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

Configuración	Descripción
	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. 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: • **Sin definir** • **AllSigned** • **Bypass**: Este es el valor predeterminado. • **RemoteSigned** • **Restringido** • **Sin restringir** 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 la configuración que puede configurar en el plan de supervisión depende del paquete de servicios que se aplica al inquilino. Para acceder a toda la configuración, active el paquete de Advanced Management.

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 **Administración** > **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**.
3. En la ventana **Crear plan de supervisión**, según si el paquete de Advanced Management está activado para su inquilino, haga lo siguiente:
   - Si su inquilino utiliza la protección estándar, 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 de Advanced Management está habilitado para su cliente, 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.

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 **Añadir**.

Nota
La configuración del monitor se rellenará automáticamente con los valores predeterminados. Puede añadir hasta tres monitores del mismo tipo y hasta 30 monitores en total 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. 1091) y "Configuración de alertas de supervisión" (p. 1137).

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 **Añadir**.
   c. Si hay problemas de compatibilidad que desea resolver, siga el procedimiento descrito en "Resolución de problemas de compatibilidad con planes de supervisión" (p. 1135).
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.
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 tres monitores del mismo tipo y hasta 30 monitores en total 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. 1091) y "Configuración de alertas de supervisión" (p. 1137).

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.

Pasos para añadir una carga de trabajo a un plan de supervisión

Desde Planes de supervisión

1. En la consola de Protección, vaya a **Administración** > **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.

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 **Administración** > **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 **Añadir** 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 operación. 4. Especifique la directiva de ejecución de PowerShell. 5. Ejecutar una secuencia de comandos. Para llevar a cabo esta medida, necesita una licencia del paquete de Advanced Management para la carga de trabajo (si todavía no está asignada). El sistema ejecutará la secuencia de comandos remota seleccionada con los parámetros especificados cuando se	Windows y macOS

Acción de respuesta automática	Descripción	SO compatibles
	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 supervisión del estado de la actualización de Windows.	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

Otras operaciones con planes de supervisión

Desde la pantalla **Planes de supervisión**, puede realizar las operaciones adicionales siguientes con los planes de supervisión: ver detalles, editar, ver actividades, ver alertas, cambiar nombre, habilitar, deshabilitar, clonar, exportar y eliminar.

Ver detalles

Pasos para consultar los detalles de un plan de supervisión

1. En la pantalla **Planes de supervisión**, haga clic en el icono **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 **Planes de supervisión**, haga clic en el icono **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:
   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. 1091) y "Configuración de alertas de supervisión" (p. 1137).

   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 **Planes de supervisión**, haga clic en el icono **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 **Planes de supervisión**, haga clic en el icono **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 **Planes de supervisión**, haga clic en el icono **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

- 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 **Planes de supervisión**, haga clic en el icono **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 **Planes de supervisión**, haga clic en el icono **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 **Planes de supervisión**, haga clic en el icono **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 **Planes de supervisión**, haga clic en el icono **Más acciones** del plan de supervisión.
2. Haga clic en **Exportar**.
   La configuración del plan se exporta en formato JSON al equipo local.

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 **Planes de supervisión**, haga clic en el icono **Más acciones** del plan de supervisión.
2. Haga clic en **Eliminar**.
3. Seleccione **Confirmo** y, a continuación, haga clic en **Eliminar**.

Problemas de compatibilidad con planes de supervisión

En algunos casos, aplicar un plan de supervisión en una carga de trabajo podría causar problemas de compatibilidad. Es posible que observe los siguientes problemas de compatibilidad:

- El sistema operativo es incompatible: este problema aparece cuando el sistema operativo de la carga de trabajo no es compatible.

- Agente no compatible: este problema aparece cuando la versión del agente de protección de la carga de trabajo está obsoleta y no es compatible con la funcionalidad de supervisión.
- Cuota insuficiente: este problema aparece cuando no hay una cuota de servicio suficiente en el inquilino para asignarla a las cargas de trabajo seleccionadas.

Si se aplica el plan de supervisión a un máximo de 150 cargas de trabajo seleccionadas de forma individual, se le pedirá que resuelva los conflictos existentes antes de guardar el plan. Para resolver un conflicto, elimine la causa raíz o las cargas de trabajo afectadas desde el plan. Para obtener más información, consulte "Resolución de problemas de compatibilidad con planes de supervisión" (p. 1135). Si guarda el plan sin resolver los conflictos, se deshabilitará automáticamente para las cargas de trabajo no compatibles y se mostrarán alertas.

Si se aplica el plan de supervisión a más de 150 cargas de trabajo o grupos de dispositivos, primero se guardará y, después, se comprobará la compatibilidad. El plan se deshabilitará automáticamente para las cargas de trabajo incompatibles y se mostrarán las alertas.

Resolución de problemas de compatibilidad con planes de supervisión

Según la causa de los problemas de compatibilidad, puede ejecutar diferentes acciones para resolverlos como parte del proceso de creación de un nuevo plan de supervisión.

Pasos para resolver problemas de compatibilidad

1. Haga clic en **Revise los problemas**.
2. [Opcional] Para resolver problemas de compatibilidad con sistemas operativos mediante la eliminación de cargas de trabajo desde el 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. [Opcional] Para resolver problemas de compatibilidad con sistemas operativos mediante la deshabilitación de un monitor del 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. [Opcional] Para resolver problemas de compatibilidad con agentes no compatibles mediante la eliminación de cargas de trabajo desde el plan:
   a. En la pestaña **Agentes no compatibles**, 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**.

5. [Opcional] Para resolver problemas de compatibilidad con agentes no compatibles mediante la actualización de la versión del agente, haga clic en **Ir a la lista de agentes**.

   Nota
   Esta opción solamente está disponible para los administradores de clientes.

6. [Opcional] Para resolver problemas de compatibilidad con una cuota insuficiente mediante la eliminación de cargas de trabajo desde el plan:
   a. En la pestaña **Cuota insuficiente**, 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**.
7. [Opcional] Para resolver problemas de compatibilidad con una cuota insuficiente mediante el aumento de la cuota del cliente:
   a. En la pestaña **Cuota insuficiente**, haga clic en **Ir al portal de administración**.
   b. Aumentar la cuota de servicio para el cliente.

      Nota
      Esta opción solamente está disponible para los administradores de partner.

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. 1145).

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 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. 1138).

   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.

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.

Variable	Descripción	Disponible para supervisión
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.
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

Variable	Descripción	Disponible para supervisión
		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
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 del firewall	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 uso del espacio de disco	Abre una ventana con el gráfico **Uso del 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.	Windows y 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	Windows y macOS

Medida de respuesta manual	Descripción	SO compatibles
	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 llevar a cabo esta acción, necesita una licencia del paquete de Advanced Management para la carga de trabajo (si todavía no está asignada).	
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
Abrir inventario de hardware	Se le redirigirá a la pestaña **Inventario de hardware** para la carga de trabajo actual.	Windows y 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 y 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 y 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 y 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 y macOS
Examinar los 10 principales procesos que han cargado la	Abre una ventana con los 10 principales procesos que han cargado el adaptador de	Windows y macOS

Medida de respuesta manual	Descripción	SO compatibles
red	interfaz de red (La instantánea del sistema en el momento de la generación de la alerta).	
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 y macOS
Reiniciar carga de trabajo	Abre una ventana de confirmación. Reinicia la carga de trabajo después de la confirmación.	Windows y macOS
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 y 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

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 **Acción 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 auditoría 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 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 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	El nombre del monitor

Información mostrada	Descripción
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. 1147).

Widgets de supervisión

En el widget de supervisión, puede ver la siguiente información acerca de la supervisión.

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.

Detalle	Descripción
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.  **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.

Herramientas de Cyber Protection adicionales

Modo de cumplimiento normativo

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
- 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
- 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 la contraseña de cifrado con la herramienta **Acropsh**, consulte "Cifrado" (p. 461).
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 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. 470).

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. 461).

Recuperación de copias de seguridad para 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

Con el almacenamiento inmutable, puede acceder a copias de seguridad eliminadas durante un periodo 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 se eliminan 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.

A los inquilinos eliminados no se les cobra por ningún almacenamiento, incluido el almacenamiento inmutable.

Modos de almacenamiento inmutables

Para los inquilinos cliente, el almacenamiento inmutable está disponible en los siguientes modos:

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 para 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.

Para configurar los parámetros del almacenamiento inmutable es necesario que esté habilitada la autenticación de doble factor para el inquilino al que pertenece la cuenta de administrador.

Pasos para habilitar el almacenamiento inmutable

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 confirme su elección, si se le solicita.

   En el modo de Administración, puede habilitar o deshabilitar el almacenamiento inmutable y cambiar el período de retención. Puede cambiar del modo de Administración a modo de Cumplimiento.

   Advertencia.
   Cambiar a modo de Cumplimiento es irreversible. Después de seleccionar el modo de Cumplimiento, no puede desactivar el almacenamiento inmutable ni cambiar su modo o período de retención.

7. Haga clic en **Guardar**.
8. Para establecer un soporte de archivo comprimido como el almacenamiento inmutable, cree una nueva copia de seguridad en ese archivo comprimido.

   Para crear una nueva copia de seguridad, ejecute el plan de protección de forma manual o planificada.

   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

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.
La deshabilitación del almacenamiento inmutable no tiene efecto inmediato. Durante un período de gracia de 14 días, el almacenamiento inmutable seguirá activo y podrá acceder a las copias de seguridad eliminadas en función de su periodo de retención original. Cuando finaliza el período de gracia, todas las copias de seguridad en el almacenamiento inmutable se eliminan 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.

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

1. En la pestaña **Almacenamiento de la copia de seguridad**, seleccione el almacenamiento en la nube que contenga la copia de seguridad eliminada.
2. [Solo para archivos eliminados] Para ver los archivos eliminados, haga clic en **Mostrar elementos eliminados**.
3. Seleccione el archivo que contiene la copia de seguridad que desea recuperar.
4. Haga clic en **Mostrar copias de seguridad** y en **Mostrar elementos eliminados**.
5. Seleccione la copia de seguridad que desea recuperar.
6. Continúe con la operación de recuperación como se describe en "Recuperación" (p. 518).

Almacenamiento redundante geográficamente

El almacenamiento con redundancia geográfica garantiza la durabilidad de los datos copiándolos de forma asíncrona en una ubicación secundaria que esté geográficamente distante de la ubicación primaria. Gracias a la redundancia geográfica, podrá acceder a sus datos aunque la ubicación primaria no esté disponible.

Importante
Los datos replicados ocupan el mismo espacio de almacenamiento que los datos originales.

Habilitar y deshabilitar el almacenamiento con redundancia geográfica

Requisitos previos

- El almacenamiento con redundancia geográfica no estará disponible en la consola de Cyber Protect hasta que un administrador de partners lo habilite en el portal de administración o a través de la API.
- Solo los administradores pueden habilitar o deshabilitar el almacenamiento con redundancia geográfica en la consola de Cyber Protect. Asegúrese de que tiene derechos de administrador.

Pasos para habilitar el almacenamiento con redundancia geográfica

1. [Solo si se ha habilitado el almacenamiento con redundancia geográfica a través de la API] En la alerta de la parte superior "La redundancia geográfica está disponible para todos los datos en la nube", haga clic en **Habilitar el almacenamiento en la nube con redundancia geográfica**.
2. En la consola de Cyber Protect, vaya a **Configuración** > **Configuración del sistema**.
3. Desplácese por 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**.
   De ese modo, los datos se replicarán en una ubicación secundaria y seguirán estando disponibles aunque falle la ubicación primaria.

Pasos para deshabilitar el almacenamiento con redundancia geográfica

Advertencia.
Los datos replicados se eliminan un día después de deshabilitar la redundancia geográfica.

1. En la consola de Cyber Protect, vaya a **Configuración** > **Configuración del sistema**.
2. Desplácese por la lista de opciones de copia de seguridad y haga clic en **Almacenamiento en la nube con redundancia geográfica**.
3. Deshabilite el conmutador **Almacenamiento en la nube con redundancia geográfica**.
4. Para confirmar el cambio, escriba **Deshabilitar** y, a continuación, haga clic en **Deshabilitar**.

Estado de georreplicación

La redundancia geográfica implica que los datos se repliquen en una ubicación secundaria. El estado de georreplicación muestra las fases de este proceso. Se pueden dar los siguientes estados:

- **Sincronizados**: los datos se han replicado en la ubicación secundaria.
- **Sincronizando**: los datos se están replicando en la ubicación secundaria. 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 aplicación en la consola de Cyber Protect

1. En la consola de Cyber Protect, vaya a **Almacenamiento de la copia de seguridad**.
2. Seleccione la ubicación y el conjunto de copias de seguridad.
3. Haga clic en **Detalles** y compruebe el estado en **Estado de georreplicación**.

Limitaciones

- Actualmente, las ubicaciones secundarias para los datos replicados solo están disponibles en Estados Unidos y Canadá.

- Para obtener información sobre las limitaciones del servicio de recuperación ante desastres al utilizar la redundancia geográfica, consulte el documento "Recuperación ante desastres".

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)

[Recuperación ante desastres] 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)

[Recuperación ante desastres] 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

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

[Recuperación ante desastres] 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

[Recuperación ante desastres] Una dirección IP necesaria para que los servidores en la nube estén disponibles desde Internet.

Dispositivo VPN

[Recuperación ante desastres] 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

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)

[Recuperación ante desastres] 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.

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)

[Recuperación ante desastres] 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

[Recuperación ante desastres] Red virtual aislada que se usa para probar el proceso de conmutación por error.

Red productiva

[Recuperación ante desastres] 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

[Recuperación ante desastres] Situación planificada que consiste en pasos configurables que automatizan las acciones de recuperación ante desastres.

S

Servidor de recuperación

[Recuperación ante desastres] 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

[Recuperación ante desastres] Referencia general a un servidor principal o de recuperación.

Servidor principal

[Recuperación ante desastres] 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)

[Recuperación ante desastres] Sitio remoto alojado en la nube, usado para la ejecución de infraestructuras de recuperación en caso de desastres.

Sitio local

[Recuperación ante desastres] La infraestructura local implementada en las instalaciones de su 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.

Índice

D

E

F

G

H

I

L

M

N

S

T

U

V

W