Acronis

PRODUCTO #1
BAAS

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.

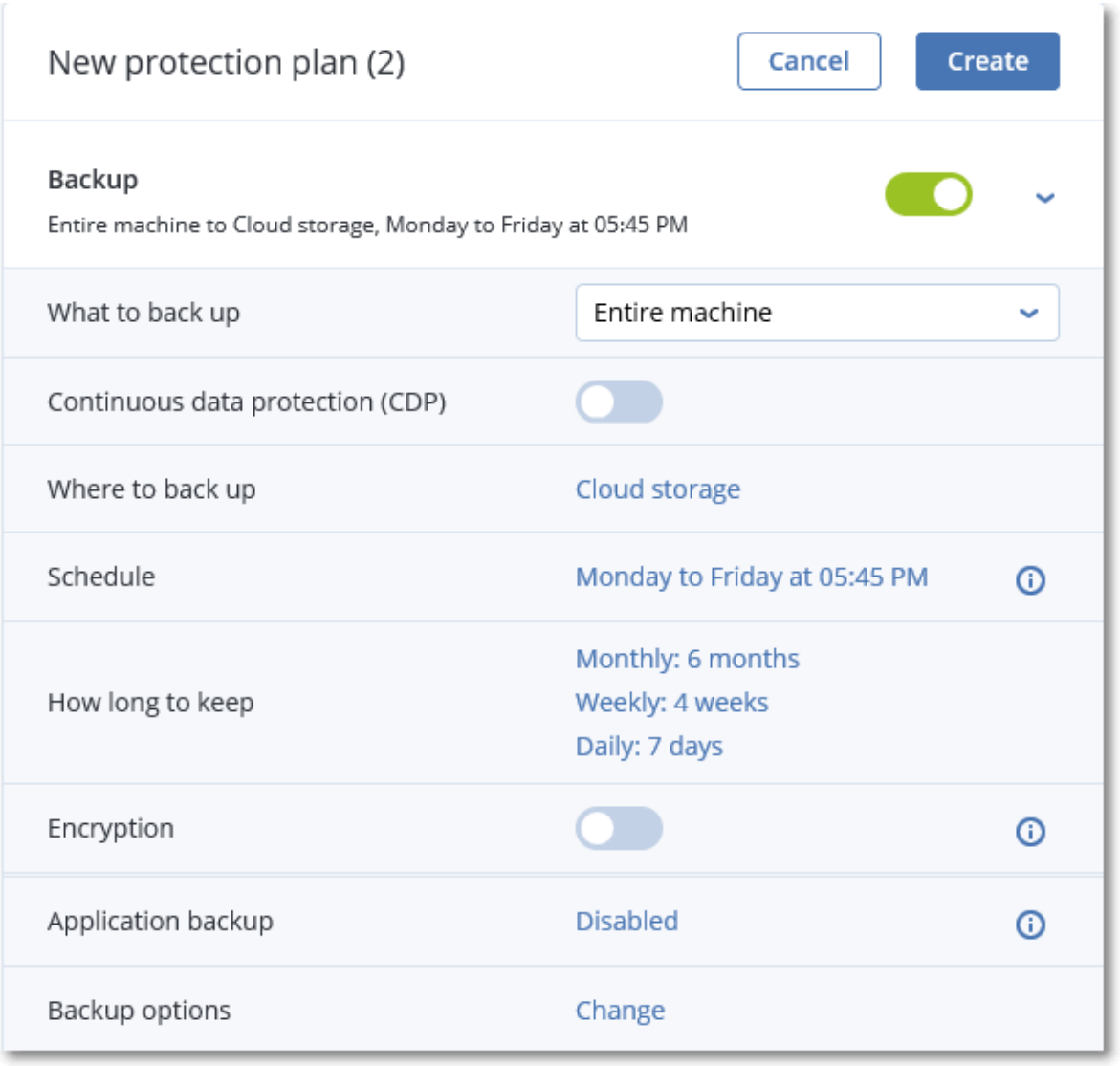
Copia de seguridad

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

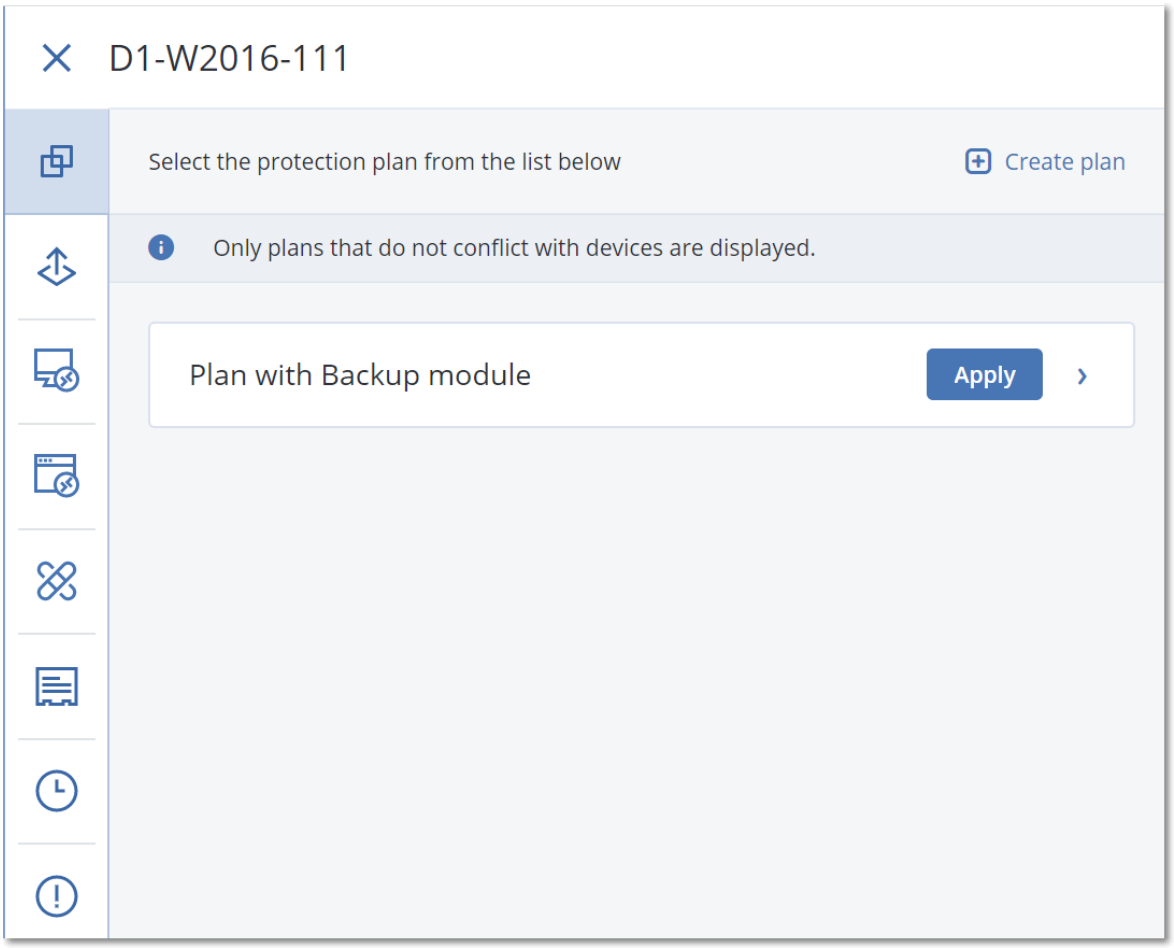
1. Seleccione los equipos que desea incluir en la copia de seguridad.
2. Haga clic en **Proteger**.
   Se mostrarán los planes de protección que están aplicados al equipo. Si no hay ningún plan de protección asignado al equipo todavía, verá el plan de protección predeterminado que se puede aplicar. Puede 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.

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. 437).

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. 503).

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. 440).

   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. 503).

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. 442).

   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. 65).
- 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.

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. 458) y "Planificación por eventos" (p. 460).
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. 454).

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

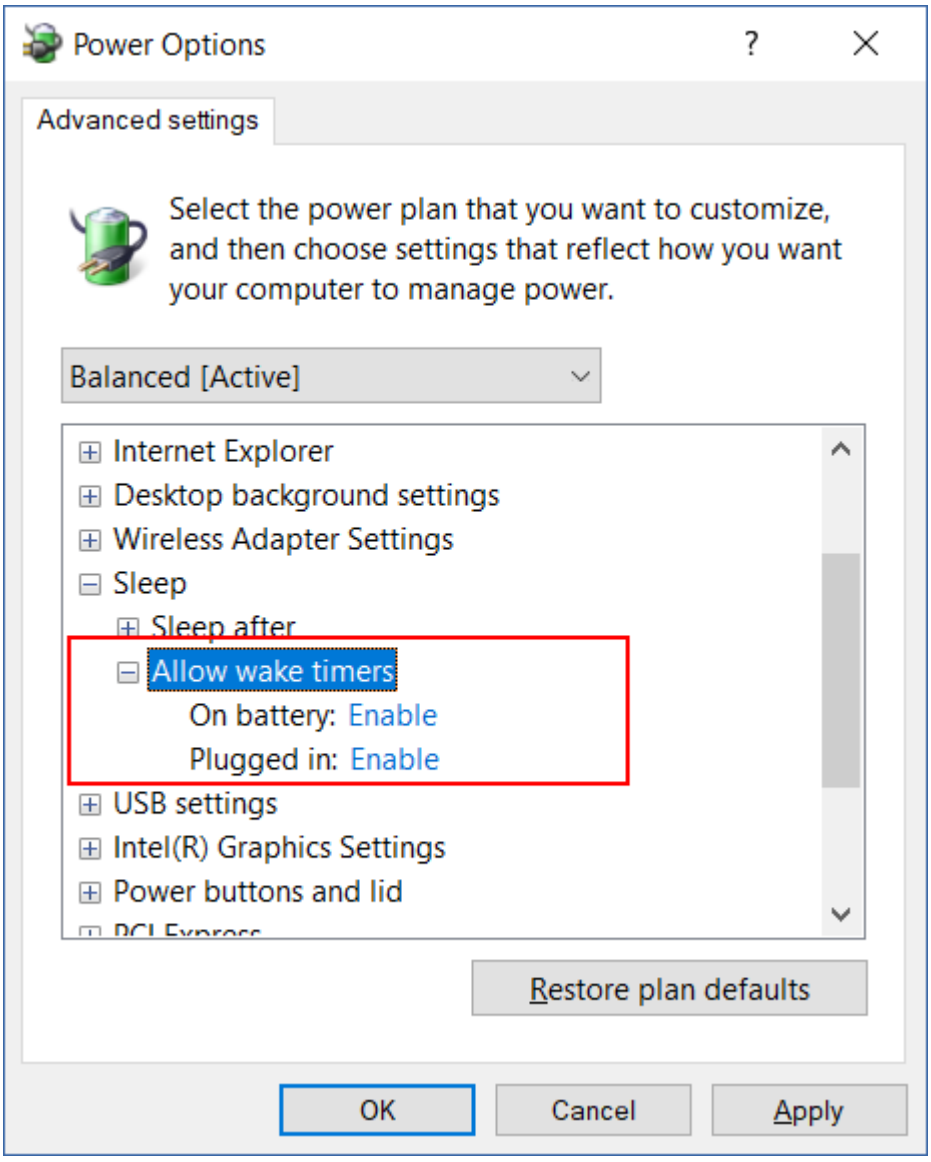
Opción	Descripción	Ejemplos
	seguridad consecutivas y el intervalo de tiempo en el que se ejecutan las copias de seguridad. Si configura el intervalo en minutos, puede seleccionar un intervalo sugerido entre 10 y 60 minutos o especificar uno personalizado, por ejemplo, 45 o 75 minutos.	a viernes. Ejecutar 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. 535).

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. 464).
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. 533)
   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.

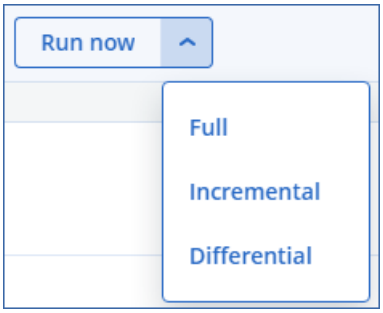
Si no se aplica ningún plan de protección a la carga de trabajo, aplique un plan existente o cree uno nuevo.

Para obtener más información sobre cómo crear un plan de protección, consulte "Creación de un plan de protección" (p. 230).

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. 474).

Dependiendo de la configuración del plan de protección, las reglas de retención se aplican a un archivo antes o después de una copia de seguridad.

Puede deshabilitar la eliminación automática de las copias de seguridad antiguas. Para ello, seleccione la opción **Conservar las copias de seguridad indefinidamente** al configurar las reglas de retención. Esto podría dar como resultado un mayor uso del almacenamiento y tendría que eliminar las copias de seguridad antiguas innecesarias de forma manual.

Consejos importantes

- Las reglas de retención son parte del plan de protección. Si revoca o elimina un plan, las reglas de retención de dicho plan ya no se aplicarán. Consulte "Eliminación de copias de seguridad" (p. 582) 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. 491).
- 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. 454).

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. 474).

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.

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. 1208).

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
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

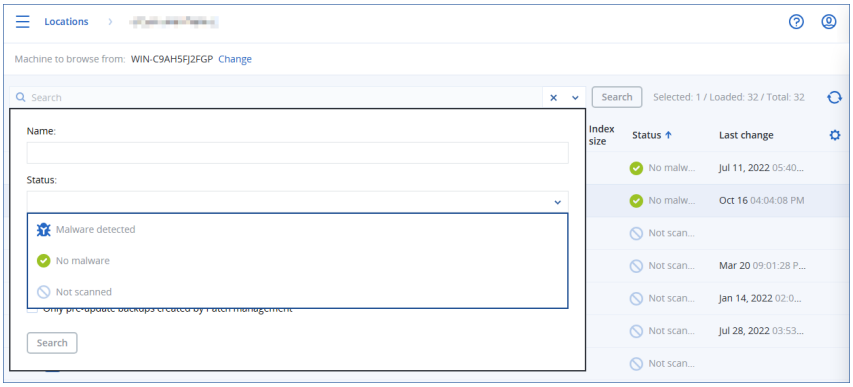
la copia de seguridad contiene archivos infectados.

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. 445).

Recuperar un equipo

Recuperación de equipos físicos

En esta sección se describe la recuperación de equipos físicos mediante la interfaz web.

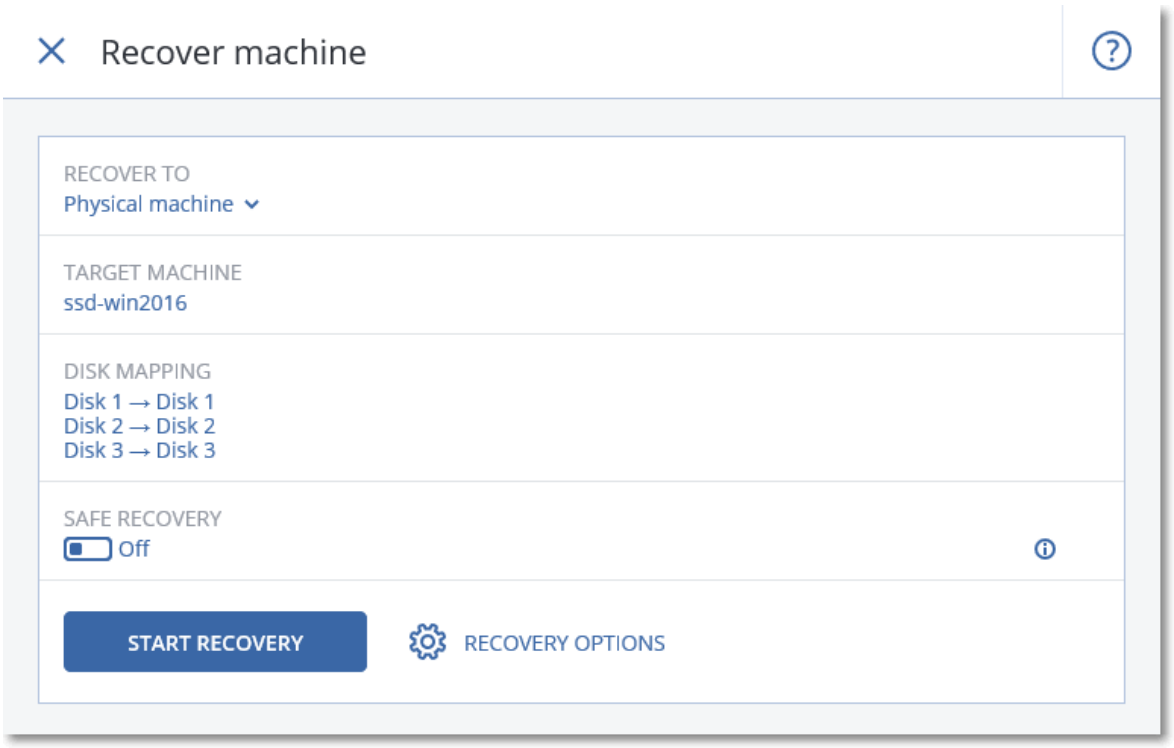
Use dispositivos de inicio en vez de interfaz web si necesita recuperar:

- 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.

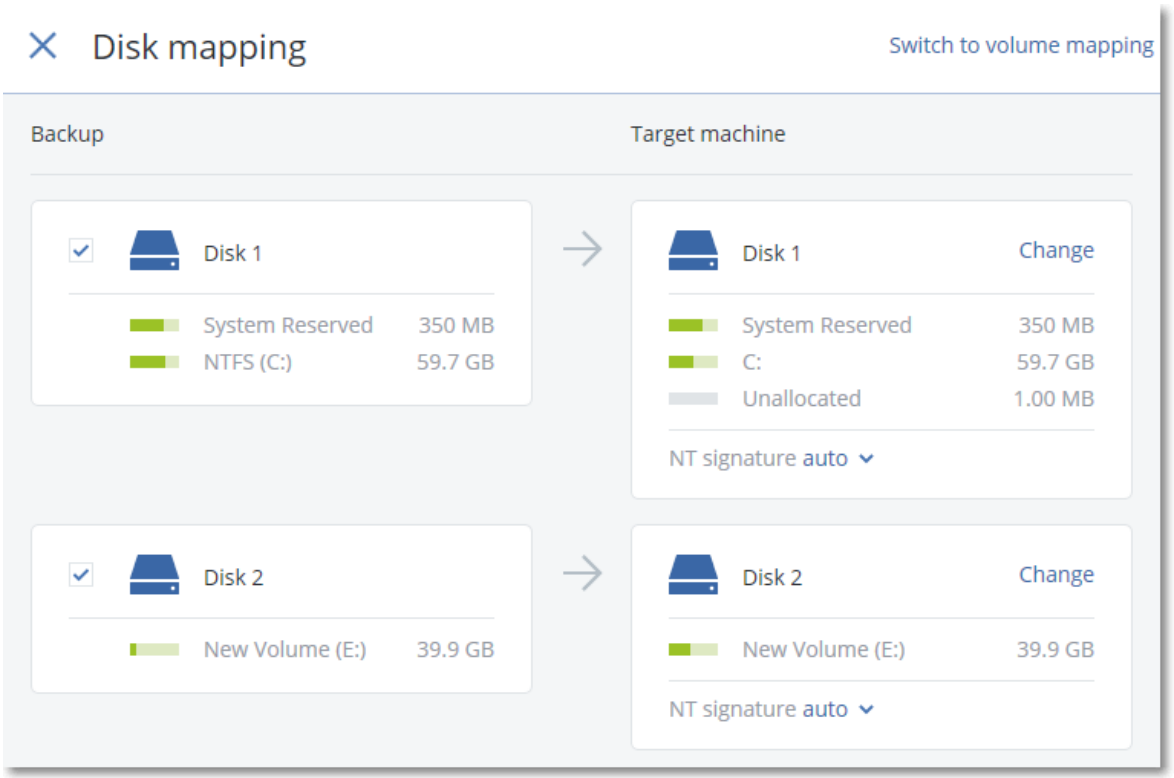
Nota
No puede recuperar copias de seguridad a nivel de disco de equipos Mac basados en Intel en equipos Mac que usen procesadores Apple Silicon, ni viceversa. Puede recuperar archivos y carpetas.

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. 543).
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.

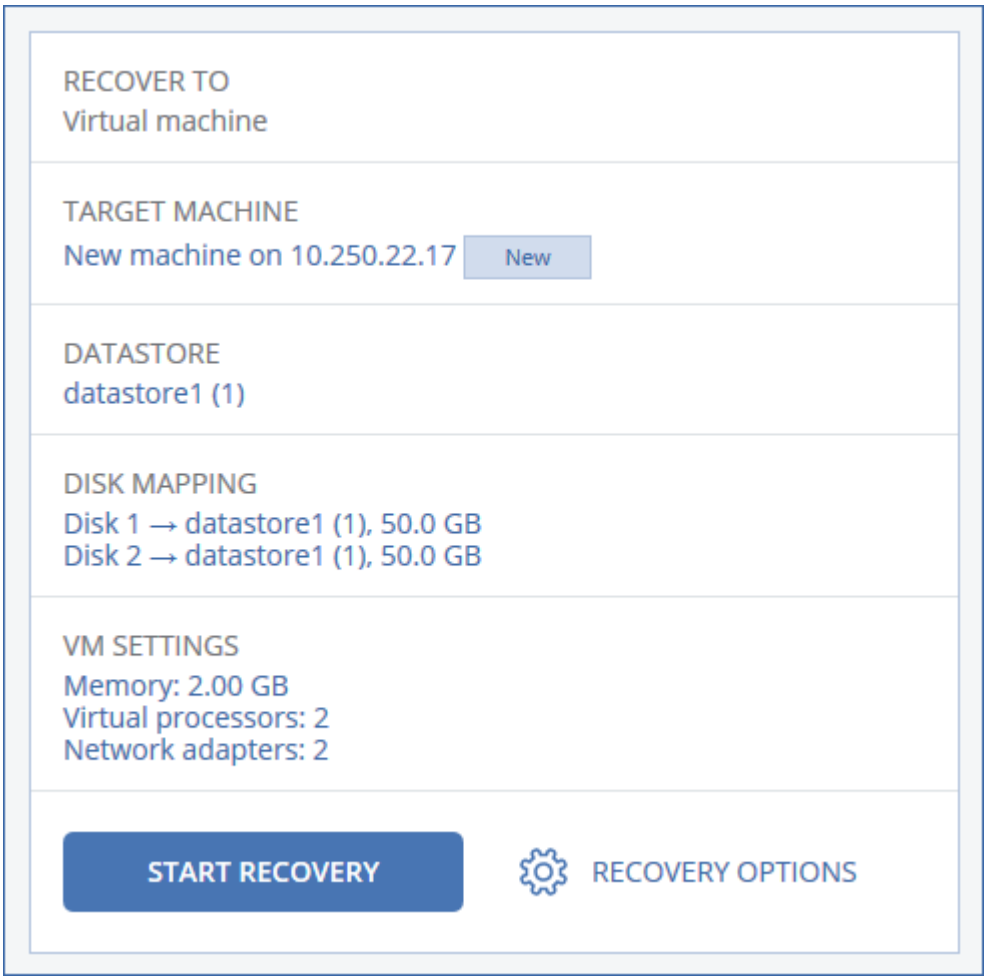
      Nota
      Debe haber al menos un agente para el hipervisor instalado y registrado en el Servidor de gestión de Acronis.

   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. 543).
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. 1208).

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".

      Tenga en cuenta que al seleccionar **Microsoft Azure** como destino, puede seleccionar la suscripción, la región y el grupo de recursos de Azure correspondientes.

   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.

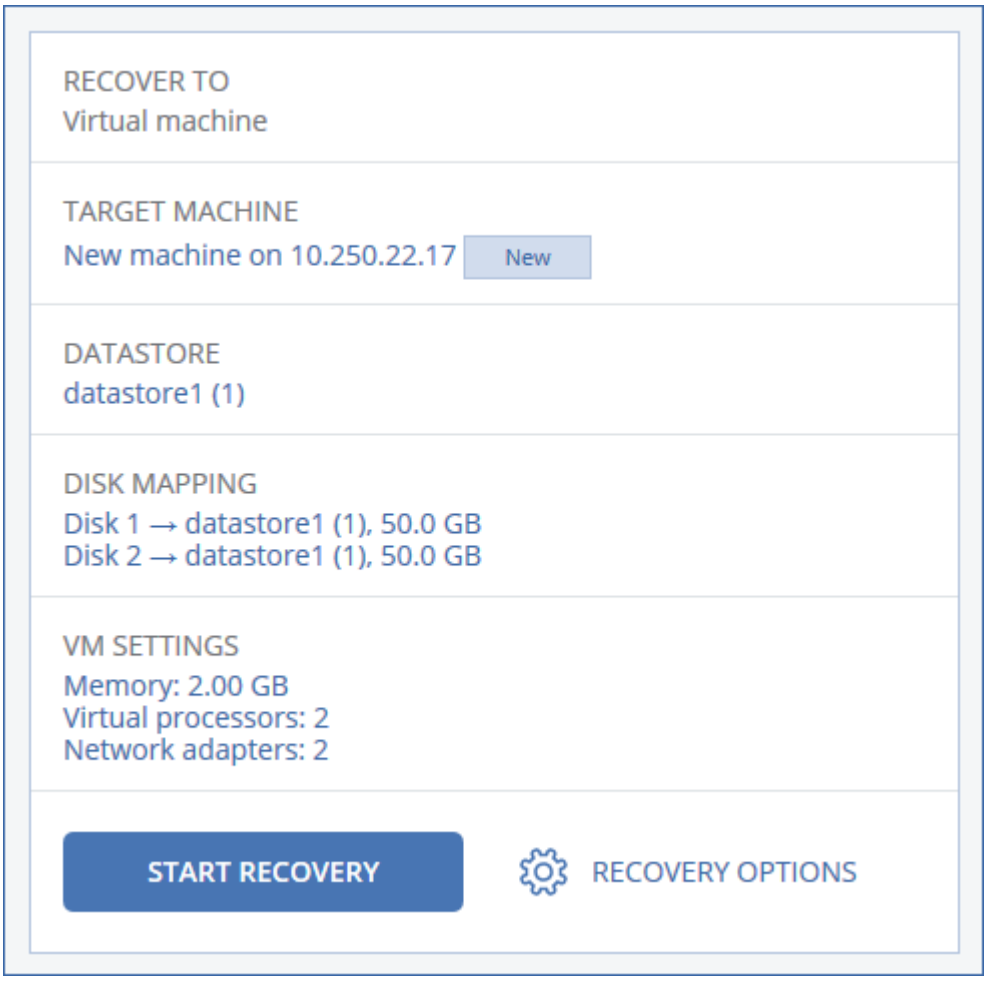
Para la Virtuozzo Hybrid Infrastructure, solo puede seleccionar la directiva de almacenamiento de los discos de destino. Para hacerlo, seleccione el disco de destino deseado y, a continuación, haga clic en **Cambiar**. En la ficha que se abre, haga clic en el icono de engranaje, seleccione la directiva de almacenamiento y, a continuación, haga clic en **Listo**.

La sección de asignación también permite elegir discos individuales para la recuperación.

Para Microsoft Azure puede cambiar el tipo de almacenamiento de cada disco de destino al seleccionar el tipo de almacenamiento correspondiente (almacenamiento con redundancia local [LRS] o almacenamiento con redundancia de zona [ZRS]).

- [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.

  [Disponible para Microsoft Azure] Para cambiar el tipo y la zona de disponibilidad, el tamaño de la memoria y las conexiones de red (incluidas las subredes y los grupos de seguridad) de la máquina virtual, haga clic en **Configuración de máquina virtual**.
- [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. 543).

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**.

Recuperación con reinicio

La recuperación con reinicio es compatible con los equipos de Windows y Linux.

Puede elegir si reiniciar el equipo automáticamente o asignarle el estado de **Interacción requerida**. El sistema operativo recuperado se pone en línea automáticamente.

Es necesario reiniciar al recuperar lo siguiente:

- Un sistema operativo

  Por ejemplo, cuando recupera un equipo entero o el volumen del sistema de un equipo.
- Volúmenes cifrados

  Por ejemplo, cuando recupera volúmenes cifrados con BitLocker o cifrados con CheckPoint.

Importante
Los volúmenes no cifrados de los que se haya hecho una copia de seguridad se recuperan como no cifrados.

Un entorno de recuperación se prepara automáticamente en el equipo recuperado. Cuando el entorno está listo, el equipo se reinicia y luego se abre el entorno de recuperación. Cuando se completa la recuperación, se inicia el sistema operativo.

Entorno de recuperación

La recuperación con reinicio utiliza un entorno de recuperación de Linux.

Nota
La recuperación de un equipo con volumen de sistema cifrado requiere al menos un volumen no cifrado en el mismo equipo.

Requisitos de espacio en disco

El entorno de recuperación requiere espacio en disco para archivos temporales. Los requisitos varían dependiendo del equipo recuperado.

La tabla siguiente resume las opciones disponibles.

Modo de arranque	Equipo con volumen de sistema no cifrado	Equipo con volumen de sistema cifrado
BIOS	200 MB en el volumen del sistema	400 MB en un volumen sin cifrar
UEFI	200 MB en la partición del sistema EFI (ESP)	Uno de los siguientes: • 400 MB en la partición del sistema EFI (ESP) • 200 MB en la partición del sistema EFI (ESP) y 200 MB en una partición no cifrada que es accesible durante el proceso de arranque

Limitaciones

- Antes de la recuperación debe bloquear todos los volúmenes cifrados ajenos al sistema cifrados. Puede bloquear un volumen abriendo un archivo que reside en él. Si el volumen no está bloqueado, la recuperación continuará sin reiniciar, y el sistema operativo puede que no reconozca el volumen.

  No necesita bloquear un volumen de sistema cifrado.

Solución de problemas

Si una recuperación falla y el error `No se puede obtener el archivo de la partición` se muestra después de reiniciar, desactive el arranque seguro. Para obtener más información, consulte Cómo desactivar el arranque seguro en la documentación de Microsoft.

Recuperar discos usando dispositivos de arranque

Para obtener información sobre cómo crear dispositivos de inicio, consulte "Creación de un dispositivo de arranque físico" (p. 777).

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. 795).

   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. 1208).

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. 504).

   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. 560).
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. 565).

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

     Por ejemplo, al recuperar archivos de una máquina virtual de Microsoft Azure, la carpeta de red debe ser accesible para el agente para Azure desplegado en la máquina virtual.
10. Haga clic en **Iniciar recuperación**.
11. Seleccione una de las opciones de sobreescritura de archivos:
    - **Sobrescribir archivos existentes**
    - **Sobrescribir un archivo existente si es más antiguo**
    - **No sobrescribir archivos existentes**

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

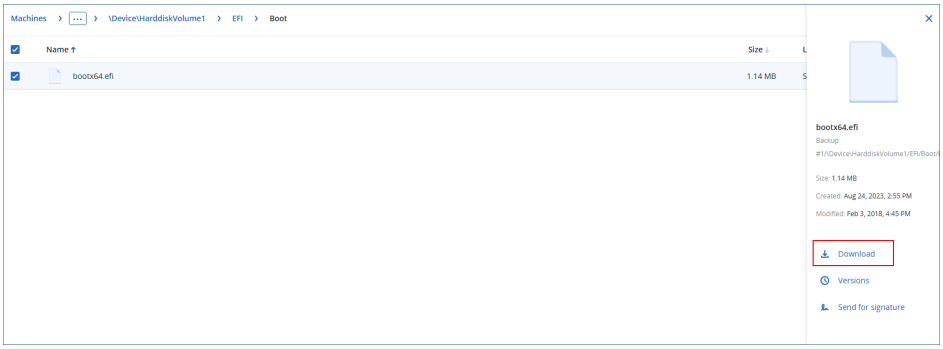
1. En la consola de Cyber Protection, seleccione la carga de trabajo requerida y haga clic en **Recuperación**.
2. [Si hay varias ubicaciones de copia de seguridad disponibles] Seleccione la ubicación de la copia de seguridad y haga clic en **Otras formas de recuperar**.
3. Haga clic en **Descargar archivos**.

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. 795).

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. 1208).

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. 571), 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. 1208).

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. 777).

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 arranque**	**Windows**	**Linux**	**macOS**	**Dispositivo de arranque**	**ESXi, Hyper-V, Scale Computing, oVirt y**	**Azure**	**Windows**

								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. 244).

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 el agente para VMware, agente para Azure, agente para Hyper-V, agente para Virtuozzo, agente para Scale Computing HC3 o agente para oVirt realizan la recuperación en una máquina virtual.

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

Puede validar una copia de seguridad para verificar que puede recuperar los datos. Para obtener más información sobre esta operación, consulte "Validación" (p. 242).

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. 576).
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. 239).

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. 576).
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.

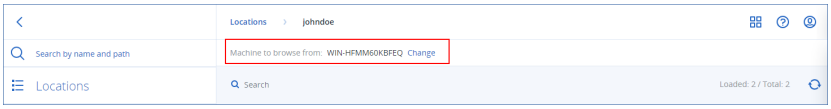
Eliminación de copias de seguridad fuera de la consola de Cyber Protect

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.

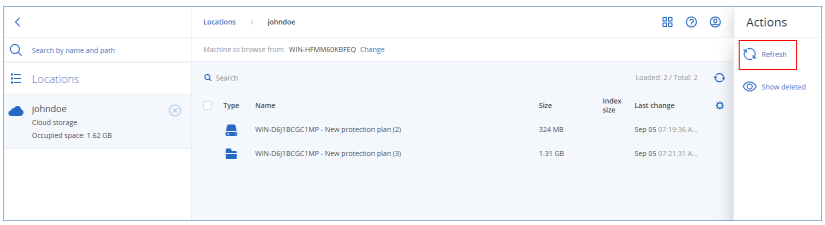
Prerrequisito

- 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. 586) y "¿Se muestran los atascos en las cargas de trabajo, los agentes y las ubicaciones de copia de seguridad?" (p. 588).

¿Qué es un atasco?

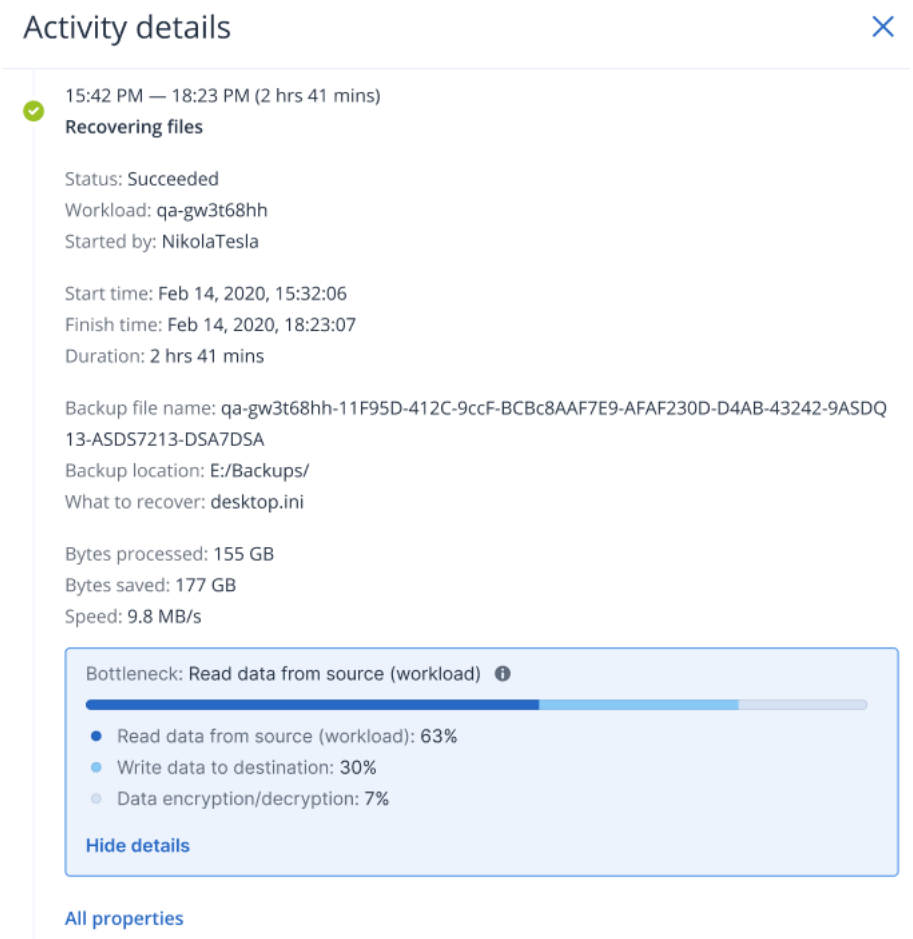
Los atascos suelen estar causados por un componente lento de la cadena de procesamiento, es decir, un componente al que tienen que esperar el resto de componentes.

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.

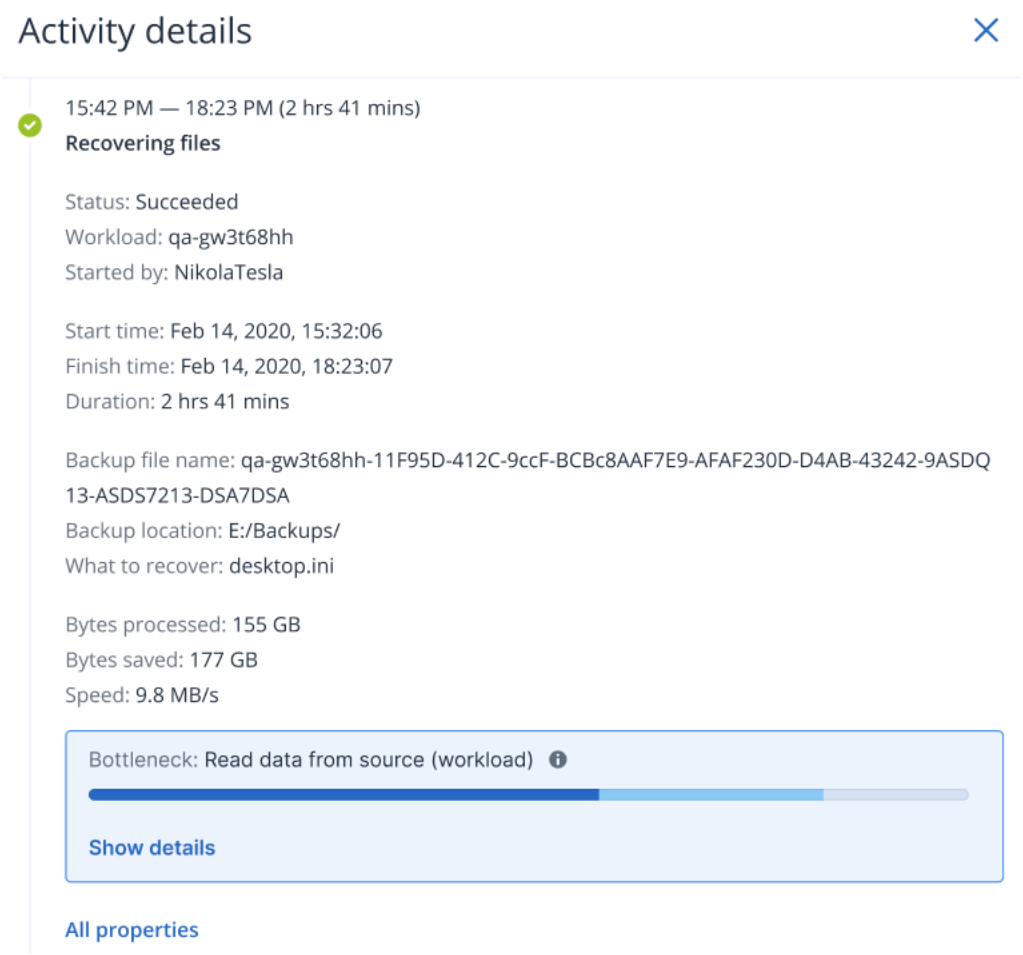
Visualización de detalles de atasco

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.

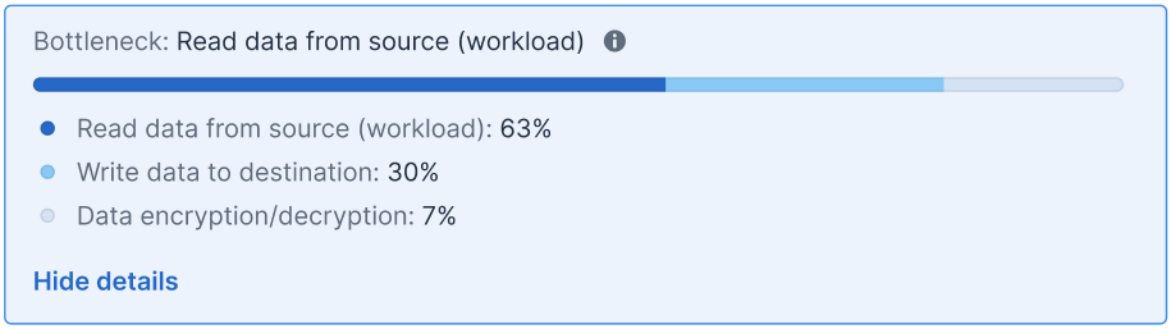
Para obtener más información sobre la definición y los conceptos básicos de los tipos de atascos, consulte "Descripción de la detección de atascos" (p. 584).

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