Acronis

acronis.com

Acronis Cyber Protect 15

Actualización 6

Guía del usuario

REVISIÓN: 07/01/2025

Contenido

Declaración de derechos de autor

Es posible que se suministre código de terceros junto con el software o servicio. Los términos de la licencia de terceros se detallan en el archivo license.txt ubicado en el directorio raíz de instalación. La lista más reciente de códigos de terceros y los términos de la licencia asociada que se utiliza con el software o los servicios está disponible en todo momento en https://kb.acronis.com/content/7696

Tecnologías patentadas de Acronis

Las tecnologías que se usan en este producto están cubiertas y protegidas por uno o más Números de patente de los Estados Unidos: 7,047,380; 7,246,211; 7,275,139; 7,281,104; 7,318,135; 7,353,355; 7,366,859; 7,383,327; 7,475,282; 7,603,533; 7,636,824; 7,650,473; 7,721,138; 7,779,221; 7,831,789; 7,836,053; 7,886,120; 7,895,403; 7,934,064; 7,937,612; 7,941,510; 7,949,635; 7,953,948; 7,979,690; 8,005,797; 8,051,044; 8,069,320; 8,073,815; 8,074,035; 8,074,276; 8,145,607; 8,180,984; 8,225,133; 8,261,035; 8,296,264; 8,312,259; 8,347,137; 8,484,427; 8,645,748; 8,732,121; 8,850,060; 8,856,927; 8,996,830; 9,213,697; 9,400,886; 9,424,678; 9,436,558; 9,471,441; 9,501,234; y solicitudes de patentes pendientes.

Ediciones de Acronis Cyber Protect 15

Acronis Cyber Protect 15 está disponible en las siguientes ediciones:

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

Para obtener más información sobre las funciones que incluye cada edición, consulte Comparación de ediciones de Acronis Cyber Protect 15 que incluyen implementaciones en la nube.

Todas las ediciones de Acronis Cyber Protect 15 tienen licencias con el número y el tipo de cargas de trabajo protegidas (estación de trabajo, servidor, y servidor virtual). Las ediciones de Cyber Protect solo están disponibles con licencias de suscripción. Las ediciones de Cyber Backup están disponibles tanto por suscripción como con licencia perpetua. Para obtener más información sobre las opciones disponibles, consulte "Licencia" (p. 22).

Las claves de licencia sin caducidad de la versión 15 no pueden utilizarse con agentes de copia de seguridad de Acronis Cyber Backup 12.5. Sin embargo, estos agentes seguirán funcionando con sus claves de licencias antiguas, incluso cuando su servidor de gestión se actualice a la versión 15.

Las licencias de suscripción de copias de seguridad se pueden utilizar con agentes de la versión 12.5, incluso cuando los agentes se hayan actualizado a la versión 15. Las licencias de suscripción de Cyber Protect solo se pueden utilizar con agentes de la versión 15.

Los agentes de copia de seguridad de la versión 12.5 registrados en la versión 15 del servidor de gestión no pueden ejecutar operaciones de procesamiento de datos fuera del host, como la replicación y la validación de copia de seguridad, la limpieza o la conversión a una máquina virtual.

Nota
Las funciones varían según la edición. Puede que algunas de las funciones descritas en esta documentación no estén disponibles con su licencia. Para obtener más información sobre las funciones que incluye cada edición, consulte Comparación de ediciones de Acronis Cyber Protect 15 que incluyen implementaciones en la nube.

Funciones de Cyber Protect compatibles con el sistema operativo

Las funciones de Cyber Protect son compatibles con los siguientes sistemas operativos:

- Windows: Windows 7 y versiones posteriores, Windows Server 2008 R2 y versiones posteriores. La gestión del antivirus Windows Defender es compatible con Windows 8.1 y versiones posteriores.

- Linux: CentOS 7.x, CentOS 8.0, Virtuozzo 7.x, Acronis Cyber Infrastructure 3.x.
  Es posible que otras distribuciones y versiones de Linux sean compatibles con las funciones de Cyber Protect, pero aún no se han probado.
- macOS: 10.13.x y posteriores (solo se admite la protección antivirus y antimalware).

Importante
Las funciones de Cyber Protect solo están disponibles para equipos en los que está instalado un agente de protección. Para equipos virtuales protegidos sin agente, por ejemplo, por Agente para Hyper-V, Agente para VMware o Agente para Scale Computing, solo es compatible la copia de seguridad.

Funciones de Cyber Protect	Windows	Linux	macOS
Copia de seguridad forense	Sí	No	No
Protección continua de datos (CDP)			
CDP para archivos y carpetas	Sí	No	No
CDP para archivos cambiados mediante el seguimiento de aplicaciones	Sí	No	No
Autodetección e instalación remota			
Detección basada en la red	Sí	No	No
Detección basada en Active Directory	Sí	No	No
Detección con base en la plantilla (importación de equipos desde un archivo)	Sí	No	No
Inclusión manual de dispositivos	Sí	No	No
Protección antimalware de Acronis			
Detección de ransomware basada en el comportamiento de procesos (basada en IA)	Sí	No	No
Detección de procesos de criptominería	Sí	No	No
Protección contra malware en tiempo real	Sí	No	Sí
Recuperación automática de archivos afectados de la caché local	Sí	No	No
Autoprotección de los archivos de copias de seguridad de Acronis	Sí	No	No
Autoprotección del software Acronis	Sí	No	No

Análisis estadístico para archivos ejecutables portátiles	Sí	No	Sí*
Protección de unidades externas (discos duros, unidades flash y tarjetas SD)	Sí	No	No
Protección de carpetas de red	Sí	No	No
Protección del servidor	Sí	No	No
Protección de Zoom, WebEx, Microsoft Teams y otras protecciones para trabajo remoto	Sí	No	No
Análisis antimalware bajo demanda	Sí	No	Sí
Analizar archivos del archivo comprimido	Sí	No	Sí
Exclusiones de archivos/carpetas	Sí	No	Sí**
Exclusiones de procesos	Sí	No	No
Lista blanca corporativa	Sí	No	Sí
Detección del comportamiento	Sí	No	No
Cuarentena	Sí	No	Sí
Filtrado de URL (http/https)	Sí	No	No
Gestión de Windows Defender Antivirus	Sí	No	No
Gestión de Microsoft Security Essentials	Sí	No	No
Evaluación de vulnerabilidades			
Evaluación de vulnerabilidades del sistema operativo y sus aplicaciones nativas	Sí	Sí***	No
Evaluación de vulnerabilidades para aplicaciones de terceros	Sí	No	No
Gestión de parches			
Aprobación automática de parches	Sí	No	No
Instalación manual de parches	Sí	No	No
Programación automática de instalación del parche	Sí	No	No
Instalación de parches a prueba de fallos: realización de una copia de seguridad del equipo antes de	Sí	No	No

instalar los parches como parte de un plan de protección			
Cancelación del reinicio de un equipo si se está ejecutando una copia de seguridad	Sí	No	No
Mapa de protección de datos			
Análisis de equipos para encontrar archivos no protegidos	Sí	No	No
Información general de ubicaciones no protegidas	Sí	No	No
Acción de protección en un mapa de protección de datos	Sí	No	No
Estado del disco			
Control del estado del disco duro y SSD basado en IA	Sí	No	No
Planes de protección inteligente basados en alertas del centro de operaciones de ciberprotección (CPOC) de Acronis			
Fuente de amenazas	Sí	No	No
Asistente de soluciones	Sí	No	No
Análisis de copia de seguridad			
Análisis de copias de seguridad cifradas	Sí	No	No
Análisis de copias de seguridad de disco en almacenamiento local, redes compartidas y Acronis Cloud Storage	Sí	No	No
Recuperación segura			
Análisis antimalware con la protección antivirus y antimalware de Acronis durante el proceso de recuperación	Sí	No	No
Escritorio remoto			
Conexión mediante cliente basado en HTML5	Sí	No	No
Conexión mediante cliente RDP de Windows	Sí	No	No
Borrado remoto	Sí****	No	No
Cyber Protect Monitor	Sí	No	Sí

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

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

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

**** El borrado remoto solo está disponible para equipos con Windows 10 o posterior.

Licencia

Para proteger una carga de trabajo con Acronis Cyber Protect, necesita una licencia. No se requiere una licencia para instalar Acronis Cyber Protect.

Tipos de licencia

Acronis Cyber Protect está disponible con licencias de suscripción. Dentro del período de validez, que comienza en la fecha de compra, están disponibles actualizaciones ilimitadas y soporte técnico sin cargos. Cuando el período de validez termine, los planes de protección existentes dejarán de funcionar y no se podrán crear planes de protección nuevos.

Hay disponibles renovaciones para las licencias perpetuas heredadas. Algunas características, como el despliegue en la nube o las copias de seguridad de la nube a la nube, no están disponibles con una licencia perpetua.

También está disponible una licencia de prueba que le ofrece acceso a todas las características del producto durante 30 días desde la activación de la licencia.

Para obtener más información sobre las diferentes opciones de licencia, consulte Acronis Cyber Protect 15: preguntas frecuentes sobre la licencia y la actualización o la reversión de la actualización en nuestra base de conocimientos. La política de licencias de Acronis está disponible en https://www.acronis.com/company/licensing.html.

Importante
La actualización 3 de Acronis Cyber Protect 15 presenta un nuevo modelo de licencia. Requiere el registro y la activación de la licencia en los servidores de gestión locales.

Cuenta de Acronis

Debe tener una cuenta de Acronis para utilizar Acronis Cyber Protect, gestionar sus licencias y su uso, acceder a las últimas compilaciones del producto y solicitar soporte técnico.

Todas las licencias y los servidores de administración se registran en esa cuenta. Al crear una cuenta de Acronis para un cliente empresarial, también se crea un perfil de empresa y un perfil de usuario administrador.

Con las credenciales de administrador, tiene acceso a las siguientes consolas:

- Portal del cliente de Acronis

  Nota
  Para los clientes, el portal de cliente de Acronis forma parte de la consola de la nube. Se redirige a estos clientes a la consola de la nube cuando inician sesión en su cuenta en https://account.acronis.com.

- Consola de Cyber Protect Cloud (consola de la nube)
- Consola de Cyber Protect (consola local de un servidor de administración in situ)

Para obtener más información, consulte "Consola local, consola de la nube y portal del cliente de Acronis" (p. 30).

Edición del perfil de la empresa

El perfil de la empresa contiene la información que proporcionó al crear la cuenta de Acronis.

Nota
Para los clientes, el portal de cliente de Acronis forma parte de la consola de la nube. Se redirige a estos clientes a la consola de la nube cuando inician sesión en su cuenta en https://account.acronis.com.

Pasos para editar el perfil de la empresa

Consola de la nube

1. Inicie sesión en la consola de Cyber Protect Cloud (https://cloud.acronis.com) como administrador.
2. Vaya a **Gestión empresarial** > **Perfil de la empresa**.
3. En la sección **Información de la empresa**, haga clic en **Editar**.
4. Edite la información de la empresa y haga clic en **Guardar**.

Account.acronis.com

1. Inicie sesión en el portal de clientes de Acronis (https://account.acronis.com) con las credenciales de su cuenta de Acronis.
2. En el menú de navegación, haga clic en **Perfil**.
3. En la sección **Información general**, haga clic en **Editar**.
4. Edite la información del perfil y haga clic en **Guardar**.

Administración de los contactos de la empresa

De forma predeterminada, el administrador de la empresa que crea con su cuenta de Acronis es la persona de contacto que recibe información de facturación, técnica y relacionada con la empresa de Acronis.

Puede crear contactos de empresa adicionales y asignarles uno o más de los siguientes tipos de contacto:

- Facturación
- Técnico
- Empresa

Puede crear un contacto a partir de un perfil de usuario existente en Cyber Protect Cloud o un contacto que no esté asociado a un perfil de usuario.

Para obtener más información sobre cómo crear un perfil de usuario en Cyber Protect Cloud, consulte "Pasos para añadir administradores a su cuenta de Acronis" (p. 26).

Nota
Para los clientes, el portal de cliente de Acronis forma parte de la consola de la nube. Se redirige a estos clientes a la consola de la nube cuando inician sesión en su cuenta en https://account.acronis.com.

Pasos para añadir un contacto de la empresa

Consola de la nube

1. Inicie sesión en la consola de Cyber Protect Cloud (https://cloud.acronis.com) como administrador.
2. Vaya a **Gestión empresarial** > **Perfil de la empresa**.
3. En la sección **Contactos de empresa**, haga clic en **Añadir**.
4. [Para crear un contacto a partir de un perfil de usuario existente] Seleccione **Seleccionar una persona de contacto existente**.
   a. Seleccione un perfil de usuario de la lista desplegable.
      La lista desplegable muestra los perfiles de usuario en Cyber Protect Cloud. Estos perfiles de usuario son diferentes de los perfiles de usuario que crea en la consola local.
   b. Seleccione uno o más tipos de contacto.
5. [Para crear un contacto que no esté asociado a un perfil de usuario] Seleccione **Crear una nueva persona de contacto**.
   a. Especifique el nombre, el apellido y la dirección de correo electrónico de la persona de contacto.
   b. [Opcional] Especifique el número de teléfono y el cargo de la persona de contacto.
   c. Seleccione uno o más tipos de contacto.
6. Haga clic en **Agregar**.

Account.acronis.com

1. Inicie sesión en el portal de clientes de Acronis (https://account.acronis.com) con las credenciales de su cuenta de Acronis.
2. En el menú de navegación, haga clic en **Perfil**.
3. [Para añadir un contacto técnico] Vaya a **Contacto técnico** y haga clic en **Añadir contacto**
4. [Para agregar un contacto de facturación] Vaya a **Contacto de facturación** y haga clic en **Añadir contacto**.
5. Especifique el nombre, el apellido y la dirección de correo electrónico de la persona de contacto.

6. [Opcional] Especifique el número de teléfono y el cargo de la persona de contacto.
7. Haga clic en **Guardar**.

Como resultado, se enviará un correo electrónico de confirmación a la dirección de correo electrónico de la persona de contacto.

Una vez que se confirme la dirección de correo electrónico, se utilizará para la información técnica o de facturación relacionada con su cuenta de Acronis.

Pasos para editar un contacto de la empresa

Consola de la nube

1. Inicie sesión en la consola de Cyber Protect Cloud (https://cloud.acronis.com) como administrador.
2. Vaya a **Gestión empresarial** > **Perfil de la empresa**.
3. En la sección **Contactos de la empresa**, seleccione el contacto y haga clic en el icono de elipsis (...) > **Editar**.
4. Edite la información de contacto y haga clic en **Guardar**.

Account.acronis.com

1. Inicie sesión en el portal de clientes de Acronis (https://account.acronis.com) con las credenciales de su cuenta de Acronis.
2. En el menú de navegación, haga clic en **Perfil**.
3. [Para editar un contacto técnico] Vaya a **Contacto técnico** y haga clic en **Editar**.
4. [Para editar un contacto de facturación] Vaya a **Contacto de facturación** y haga clic en **Editar**.
5. Edite la información de contacto y haga clic en **Guardar**.

Pasos para eliminar un contacto de la empresa

Consola de la nube

1. Inicie sesión en la consola de Cyber Protect Cloud (https://cloud.acronis.com) como administrador.
2. Vaya a **Gestión empresarial** > **Perfil de la empresa**.
3. En la sección **Contactos de la empresa**, seleccione el contacto y haga clic en el icono de elipsis (...) > **Eliminar**.
4. Haga clic en **Continuar** para confirmar su decisión.

Como resultado, se elimina el contacto.

Nota
Cuando elimina un contacto, el perfil de usuario que está asociado al contacto en Cyber Protect Cloud no se elimina.

Account.acronis.com

1. Inicie sesión en el portal de clientes de Acronis (https://account.acronis.com) con las credenciales de su cuenta de Acronis.
2. En el menú de navegación, haga clic en **Perfil**.
3. [Para eliminar un contacto técnico] Vaya a **Contacto técnico** y haga clic en el icono de elipsis (...) > **Eliminar**.
4. [Para eliminar un contacto de facturación] Vaya a **Contacto de facturación** y haga clic en el icono de elipsis (...) > **Eliminar**.

Como resultado, se elimina el contacto.

Pasos para añadir administradores a su cuenta de Acronis

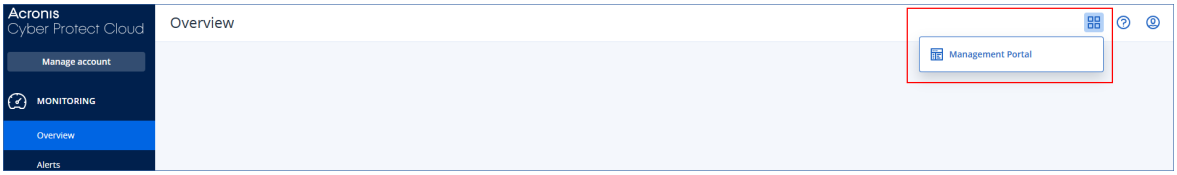
Se crea una cuenta de administrador de la empresa cuando registra su cuenta de Acronis.

Puede crear cuentas de administrador adicionales. Estos administradores pueden acceder a la consola de la nube pero no pueden acceder al portal de cliente de Acronis en https://account.acronis.com .

Nota
Para los clientes, el portal de cliente de Acronis forma parte de la consola de la nube. Se redirige a estos clientes a la consola de la nube cuando inician sesión en su cuenta en https://account.acronis.com.

Pasos para crear una cuenta de administrador adicional

1. Inicie sesión en la consola de Cyber Protect Cloud (https://cloud.acronis.com) como administrador.
2. En la esquina superior derecha, haga clic en el icono del conmutador de la consola y, a continuación, haga clic en **Portal de administración**.



3. En el portal de administración, vaya a **Gestión empresarial** > **Usuarios**.
4. Haga clic en **Nuevo** > **Usuario**.
5. Especifique la dirección de correo electrónico del nuevo administrador.
   Esta dirección de correo electrónico será el inicio de sesión del administrador.
6. [Opcional] Para configurar un inicio de sesión y una dirección de correo electrónico diferentes, seleccione **Usar un inicio de sesión diferente al correo electrónico** y, a continuación, especifique una dirección de correo electrónico y un inicio de sesión.
7. Especifique el nombre y el apellido del administrador.
8. En **Servicios y roles**, seleccione un rol de administrador para la nueva cuenta.
   Las siguientes opciones están disponibles.

Rol	Servicio
Administrador de la compañía	Rol en toda la cuenta. Este rol incluye el rol de administrador en el portal de administración y en el servicio de protección.
Administrador Administrador de solo lectura	Portal de administración
Administrador Administrador de solo lectura Usuario* Restaurar operador*	Protección

* No es un rol de administrador.

9. Haga clic en **Crear**.

Como resultado, se crea la cuenta del administrador y se envía un correo electrónico de activación a la dirección de correo electrónico que especificó para esa cuenta.

La cuenta aparece en el **portal de administración**, en la pestaña **Gestión empresarial** > **Usuarios**.

Cómo eliminar su cuenta de Acronis

Advertencia.
Esta operación es irreversible. Después de eliminar la cuenta, el perfil de su empresa, los números de serie de los productos registrados y los datos que se almacenan en Acronis Cloud se perderán de forma permanente.

Nota
Para los clientes, el portal de cliente de Acronis forma parte de la consola de la nube. Se redirige a estos clientes a la consola de la nube cuando inician sesión en su cuenta en https://account.acronis.com.

Para eliminar su cuenta de Acronis

Consola de la nube

1. Inicie sesión en la consola de Cyber Protect Cloud (https://cloud.acronis.com) como administrador.
2. Vaya a **Gestión empresarial** > **Perfil de la empresa**.
3. En la sección **Eliminar cuenta**, haga clic en **Eliminar cuenta**.
4. En el asistente de confirmación, lea el aviso y haga clic en **Siguiente**.
5. Seleccione la casilla de verificación **Acepto que se perderán todos los datos y deseo eliminar mi cuenta** y, a continuación, haga clic en **Siguiente**.
6. En el menú desplegable, seleccione el motivo por el que desea eliminar su perfil.

7. [Opcional] Deje un comentario adicional.
8. Haga clic en **Confirmar**.
9. En la ventana de confirmación, haga clic en **Listo**.
   Se enviará un correo electrónico de confirmación a su dirección de correo electrónico. Debe confirmar la eliminación en un plazo de 24 horas.
10. Haga clic en **Confirmar eliminación** en el correo electrónico de confirmación.

Como resultado, su cuenta de Acronis se eliminará. Una vez completada la eliminación, se enviará una notificación a su dirección de correo electrónico.

Account.acronis.com

1. Inicie sesión en el portal de clientes de Acronis (https://account.acronis.com) con las credenciales de su cuenta de Acronis.
2. En el menú de navegación, haga clic en **Perfil**.
3. En la sección **Eliminar cuenta**, haga clic en **Eliminar cuenta**.
4. En el asistente de confirmación, lea el aviso y después haga clic en **Continuar con la eliminación**.
5. En el menú desplegable, seleccione el motivo por el que desea eliminar su perfil.
6. [Opcional] Deje un comentario adicional.
7. Especifique su contraseña y después seleccione la casilla de verificación **Sí, acepto que se perderán todos los datos y deseo eliminar mi cuenta**.
8. Haga clic en **Confirmar eliminación**.
9. En la ventana de confirmación, seleccione la casilla de verificación **Confirmo que quiero eliminar mi cuenta** y después haga clic en **Eliminar**.

El proceso de eliminación puede tardar hasta 24 horas. Cuando se complete la eliminación, se enviará una notificación a su dirección de correo electrónico.

Licencia de Acronis Cyber Protect 15, actualización 3 y posteriores

En Acronis Cyber Protect 15, actualización 3 y posteriores, no hay claves de licencia añadidas a la consola local del servidor de administración (`https://<IP>:<port>`).

En su lugar, añada las licencias a su cuenta en el portal de cliente de Acronis (https://account.acronis.com) y, a continuación, gestione las licencias en la consola de la nube de Acronis Cyber Protect(https://cloud.acronis.com).

La gestión de licencias de servidores de gestión offline requiere operaciones en las consolas locales y de la nube.

Para obtener más información sobre la consola local y la de la nube, consulte "Consola local, consola de la nube y portal del cliente de Acronis" (p. 30).

Pasos para empezar a utilizar el servidor de gestión con Acronis Cyber Protect 15, actualización 3 y posteriores

1. Añada una o más licencias a su cuenta en el portal de cliente de Acronis (https://account.acronis.com).
   Las licencias que adquiera en línea se añaden automáticamente a esta cuenta.
2. [Para el modo de despliegue local] Active su servidor de gestión.
3. Asigne una licencia al servidor de gestión.

Tipos de servidores de gestión

Según el modo de despliegue, puede utilizar los siguientes tipos de servidores de gestión:

- Servidor de gestión de la nube
- Servidor de gestión local
  - Servidor de gestión en línea
  - Servidor de gestión offline

Puede tener más de un servidor de gestión en su cuenta de Acronis. También puede usar un modelo de despliegue combinado con un servidor de gestión de la nube y un servidor de gestión local.

Si utiliza varios servidores de administración, puede dividir la cuota de licencia entre ellos. Para obtener más información, consulte "Transferencia de la cuota de licencia a otro servidor de gestión" (p. 45).

Servidor de gestión local

Con el despliegue in situ, puede instalar tanto el servidor de administración como los agentes de protección de su red. Puede tener un servidor de administración offline que no esté conectado a Internet o un servidor de administración en línea con acceso a Internet.

Los servidores de administración in situ requieren activación. Para obtener más información, consulte "Activación de un servidor de gestión" (p. 36).

Servidor de gestión local en línea

Puede activar un servidor de administración en línea mediante Internet. Para ello, inicie sesión en su cuenta de Acronis al acceder a la consola local por primera vez.

Nota

En la consola local de un servidor de administración in situ en línea, se muestran dos cuentas diferentes: la cuenta de Acronis, que se utiliza para sincronizar la información de las licencias, y la cuenta de la consola, que se utiliza para acceder a la propia consola local.

Servidor de gestión local offline

Puede activar un servidor de administración offline y sincronizar la información de licencias con su cuenta de Acronis de forma manual, mediante un archivo.

Servidor de gestión de la nube

Con el despliegue en la nube, no instale ni mantenga un servidor de gestión en su red. Utiliza un servidor de gestión que ya está desplegado en un centro de datos de Acronis y solo necesita instalar agentes de protección para sus cargas de trabajo.

El servidor de gestión de la nube no necesita activación. Siempre está en línea, y la información de licencias se sincroniza automáticamente entre el servidor y su cuenta de Acronis.

Consola local, consola de la nube y portal del cliente de Acronis

Con las credenciales de administrador de su cuenta de Acronis, puede acceder a las siguientes consolas:

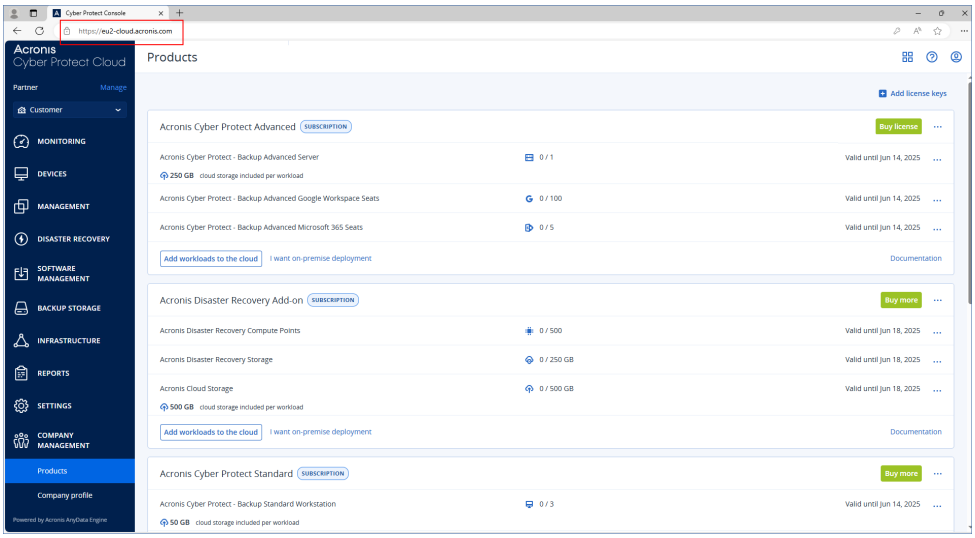
- Portal del cliente de Acronis
- Consola de Cyber Protect Cloud (consola de la nube)
- Consola de Cyber Protect (consola local de un servidor de administración in situ)

Portal del cliente de Acronis

El portal del cliente de Acronis está disponible en https://account.acronis.com .

Para los clientes, el portal de cliente de Acronis forma parte de la consola de la nube. Se redirige a estos clientes a la consola de la nube cuando inician sesión en su cuenta en https://account.acronis.com.

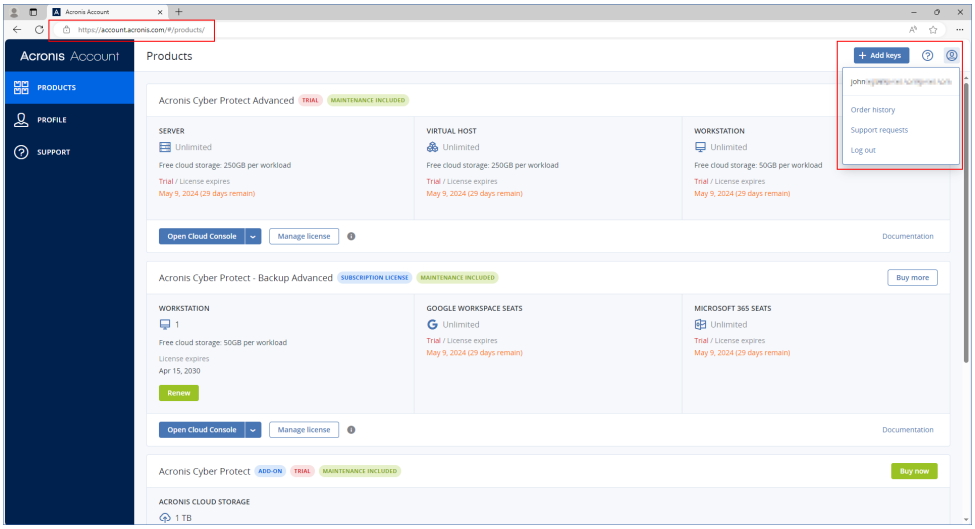
Consola de la nube



En la pestaña **Gestión empresarial** > **Productos** de la consola de la nube, puede comprobar la fecha de vencimiento de una suscripción, añadir nuevas claves de licencia, registrar renovaciones de licencia y descargar los archivos de instalación del producto.

En la pestaña **Gestión empresarial** > **Perfil de la empresa** de la consola de la nube, puede editar la información del perfil de la empresa, gestionar los contactos de la empresa y eliminar su cuenta.

Account.acronis.com

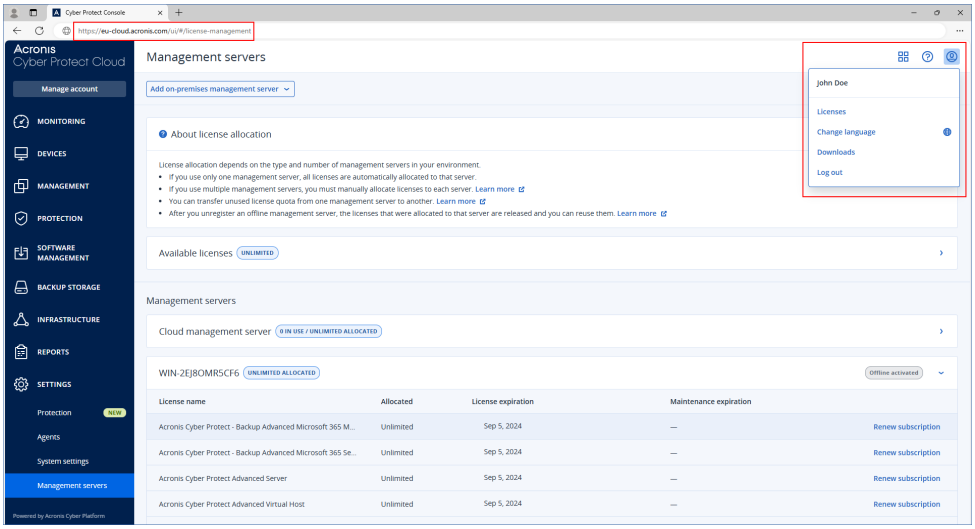


En el portal de clientes de Acronis, puede comprobar la fecha de vencimiento de una suscripción, añadir nuevas claves de licencia y registrar renovaciones de licencia. También puede ponerse en contacto con el equipo de soporte, descargar los archivos de instalación del producto y acceder a la documentación del producto.

Consola de la nube

La consola de la nube está disponible en https://cloud.acronis.com.

Cuando inicie sesión en su cuenta, la URL cambiará y mostrará el centro de datos exacto al que pertenece su cuenta. Por ejemplo, https://eu-cloud.acronis.com o https://jp-cloud.acronis.com.

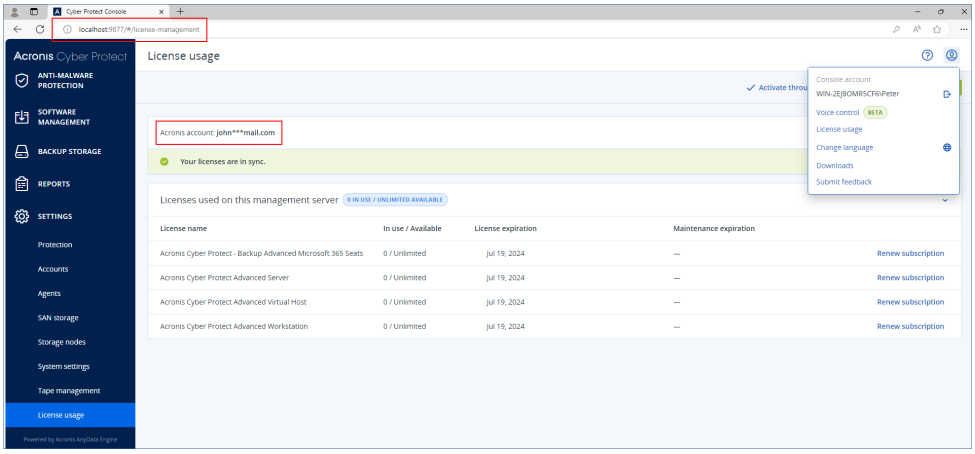


La consola de la nube es la ubicación principal desde la que gestiona sus licencias. En la pestaña **Configuración** > **Uso de licencia**, podrá asignar licencias y cuotas de licencia disponibles a un servidor de administración específico, reasignar cuotas de licencia a otro servidor de administración o completar el registro de un servidor de administración offline.

Consola local de un servidor de administración in situ

La consola local está disponible en `https://<IP>:<port>`.

`IP` es la dirección de su servidor de administración y `port` es el puerto en el que está disponible la consola de Cyber Protect. De manera predeterminada, este puerto es el 9877.



En la consola local, puede comprobar las licencias asignadas, su cuota, uso y la fecha de finalización.

Utilice la consola local, junto con la consola de la nube, cuando active un servidor de administración offline o le asigne licencias.

Gestión de licencias

Se requiere una licencia de Acronis Cyber Protect para cada carga de trabajo protegida. No es necesaria una licencia para instalar Acronis Cyber Protect.

Las licencias que compra se añaden a su cuenta en el portal de cliente de Acronis (https://account.acronis.com).

Para los clientes, el portal de cliente de Acronis forma parte de la consola de la nube. Se redirige a estos clientes a la consola de la nube cuando inician sesión en su cuenta en https://account.acronis.com.

Puede asignar las licencias a uno o más servidores de gestión en su entorno. Luego, el servidor de administración distribuye la cuota de licencia a las cargas de trabajo que están registradas en ese servidor.

Se asigna automáticamente una licencia cuando se aplica un plan de protección a una carga de trabajo por primera vez. Si hay más de una licencia disponible, se asigna automáticamente la más adecuada. Por ejemplo, a una carga de trabajo se le podría asignar una licencia Acronis Cyber Protect Advanced - Server, mientras que otra carga de trabajo podría tomar una Acronis Cyber Protect Standard. La asignación automática depende del tipo de carga de trabajo, sistema operativo y nivel de protección requerido.

La siguiente tabla resume las operaciones disponibles y muestra dónde ejecutarlas.

Operación	Ubicación
Añadir licencias a su cuenta	Puede añadir licencias en el Portal de cliente de Acronis. Las licencias que adquiera online se añaden automáticamente ahí.
Activar un servidor de gestión	Puede activar un servidor de administración registrándolo en su cuenta. Active los servidores de administración en línea en su consola local (`https://<IP>:<port>`). Para ello, inicie sesión en su cuenta de Acronis. Para esta operación, debe utilizar ambas consolas, la de la nube y la local. Para acceder a la consola de la nube, necesita un segundo equipo conectado a Internet.
Asignar licencias a un servidor de gestión Modificar una asignación de licencia existente	En los servidores de administración en línea, puede asignar licencias con la consola de la nube (https://cloud.acronis.com). Las licencias asignadas se sincronizan automáticamente con el servidor de administración. En los servidores de administración offline, puede asignar licencias con un archivo de activación. Para llevar a cabo este proceso, debe utilizar la consola local del servidor de administración (`https://<IP>:<port>`) y la consola de la nube (https://cloud.acronis.com).
Asignar licencias a cargas de	Esta operación es automática, pero puede cambiar manualmente la asignación.

Operación	Ubicación
trabajo	
Cancelar el registro de un servidor de gestión de su cuenta	Puede cancelar el registro de los servidores de administración en línea con la consola de la nube (https://cloud.acronis.com). Puede cancelar el registro de los servidores de administración offline con un archivo de desactivación. Para este proceso debe utilizar la consola local del servidor de administración offline (`https://<IP>:<port>`) y la consola de la nube (https://cloud.acronis.com). Para cancelar el registro de un servidor de administración offline al que no tiene acceso, debe utilizar solo la consola de la nube.

Pasos para añadir licencias a su cuenta de Acronis

Solo puede utilizar las licencias que se han añadido a su cuenta de Acronis.

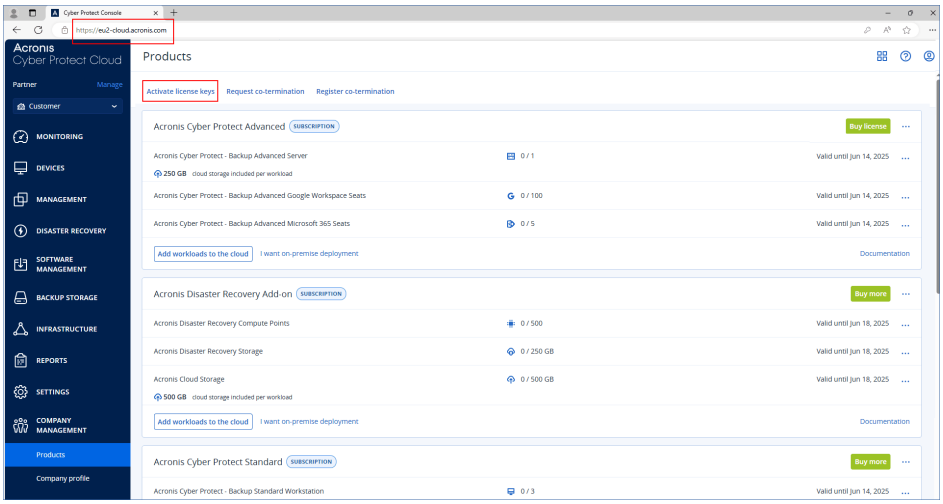
Las licencias que compra en línea se añaden automáticamente a su cuenta. Las licencias que compra offline deben añadirse manualmente a su cuenta.

Nota
Para los clientes, el portal de cliente de Acronis forma parte de la consola de la nube. Se redirige a estos clientes a la consola de la nube cuando inician sesión en su cuenta en https://account.acronis.com.

Pasos para añadir una licencia a su cuenta de Acronis

Consola de la nube

1. Inicie sesión en la consola de Cyber Protect Cloud (https://cloud.acronis.com) como administrador.
   O bien, inicie sesión en su cuenta en https://account.acronis.com. Se redireccionará a la consola de la nube.
2. Vaya a **Gestión empresarial** > **Productos**.

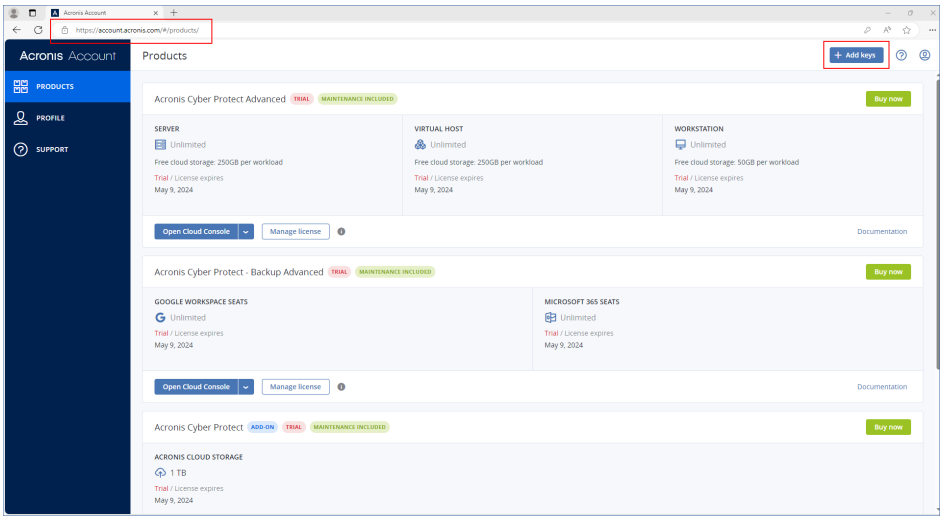


3. Haga clic en **Activar claves de licencia**.
4. [Para añadir claves de licencia individuales] Haga clic en **Introducir claves de licencia**.
   a. Introduzca una o más claves de licencia, una por línea.
   b. Haga clic en **Agregar**.
5. [Para añadir un archivo con varias claves de licencia] Haga clic en **Cargar archivo de clave de licencia**.
   a. Haga clic en **Examinar** y seleccione el archivo TXT que contiene las claves de licencia.
   b. Haga clic en **Agregar**.

Las licencias se han añadido ahora a su cuenta y puede gestionar su uso en la pestaña **Configuración**> **Uso de licencias**.

Account.acronis.com

1. Inicie sesión en el Acronisportal de clientes (https://account.acronis.com) con las credenciales de su cuenta de Acronis.
2. En el menú de navegación, haga clic en **Productos**.
3. Haga clic en **Añadir claves**.



4. Ingrese una o más claves de licencia, una por línea, y, a continuación, haga clic en **Añadir**.

> **Nota**
> Puede introducir hasta 100 claves de licencia a la vez.

Las licencias se han añadido ahora a su cuenta y puede gestionar su uso en la pestaña **Configuración** > **Uso de licencias** de la consola de la nube (https://cloud.acronis.com).

> **Importante**
> Antes de cambiar a la actualización 3 de Acronis Cyber Protect 15, exporte las licencias sin caducidad almacenadas localmente a un archivo y, a continuación, añádalas a la cuenta de Acronis.
>
> Vaya a `https://<IP>:<port>/api/account_server/v2/licensing/legacy/license_keys` para comprobar las claves de licencia que introdujo de manera local en un servidor de administración.
>
> `IP` es la dirección de su servidor de administración y `port` es el puerto en el que está disponible la consola de Cyber Protect. De manera predeterminada, este puerto es el 9877.

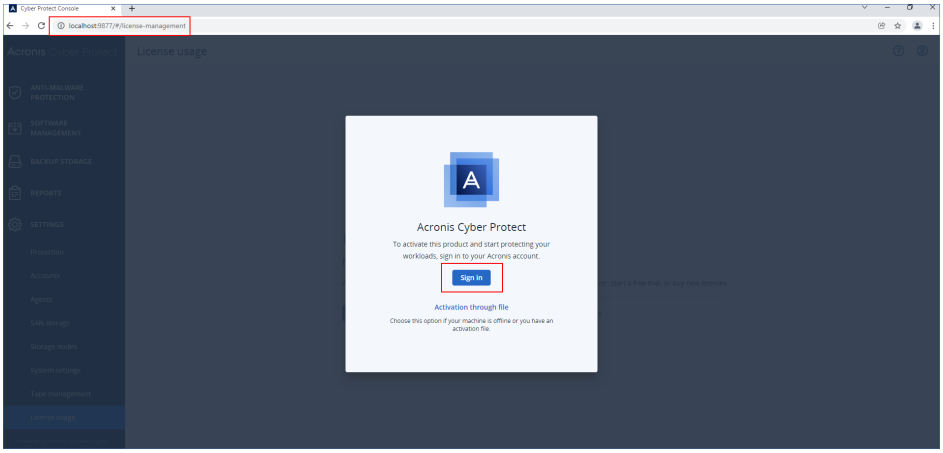
Activación de un servidor de gestión

Debe activar un servidor de administración registrándolo en su cuenta Acronis.

Pasos para activar un servidor de administración en línea

1. Después de instalar el servidor de administración de Acronis Cyber Protect, abra la consola local (`https://<IP>:<port>`).

   `IP` es la dirección de su servidor de administración y `port` es el puerto en el que está disponible la consola de Cyber Protect. De manera predeterminada, este puerto es el 9877.
2. En el cuadro de diálogo que se abra, haga clic en **Iniciar sesión**.



3. Inicie sesión en su cuenta de Acronis.

Como resultado, el servidor de gestión se registrará y activará automáticamente.

Para comenzar a proteger sus cargas de trabajo, asigne una o más licencias a este servidor. Para obtener más información, consulte "Asignación de licencias a un servidor de gestión" (p. 39).

Nota

Los servidores de gestión en línea requieren acceso a Internet para sincronizar la información de licencias con su cuenta de Acronis. Si el servidor permanece offline durante más de 30 días, sus planes de protección dejarán de funcionar y sus cargas de trabajo no estarán protegidas.

Si cierra sesión en su cuenta de Acronis de la consola local, puede que la información de la licencia no se sincronice. Si no vuelve a iniciar sesión en 30 días, los planes de protección dejarán de funcionar y sus cargas de trabajo no estarán protegidas.

Pasos para activar un servidor de gestión offline

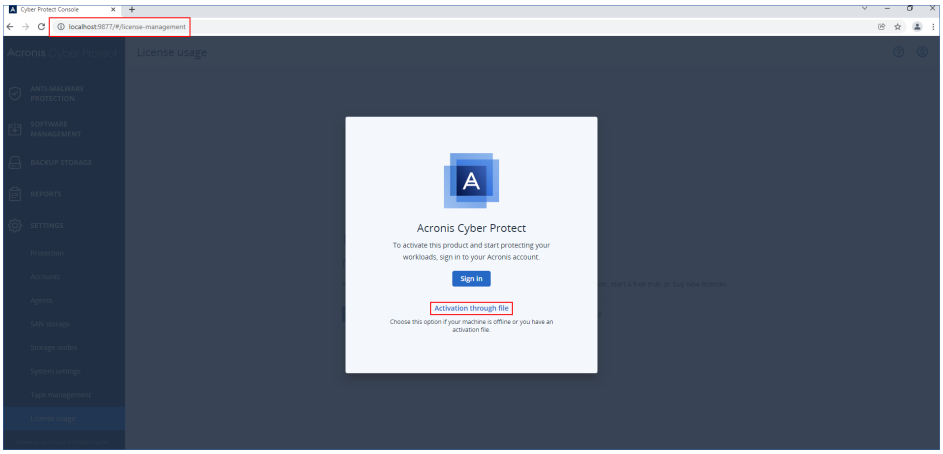
Para esta operación, debe utilizar ambas consolas, la de la nube y la local.

Para acceder a la consola de la nube, necesita un segundo equipo conectado a Internet.

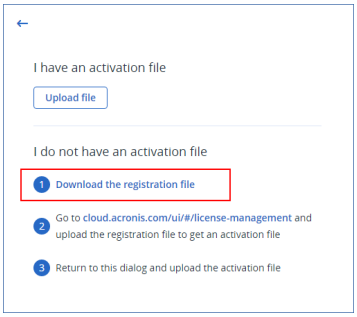
Para acceder a la consola de la nube, necesita un segundo equipo conectado a Internet.

1. Después de instalar el servidor de administración de Acronis Cyber Protect, abra la consola local (`https://<IP>:<port>`).

   `IP` es la dirección de su servidor de administración y `port` es el puerto en el que está disponible la consola de Cyber Protect. De manera predeterminada, este puerto es el 9877.
2. En el cuadro de diálogo que se abra, haga clic en **Activación mediante archivo**.

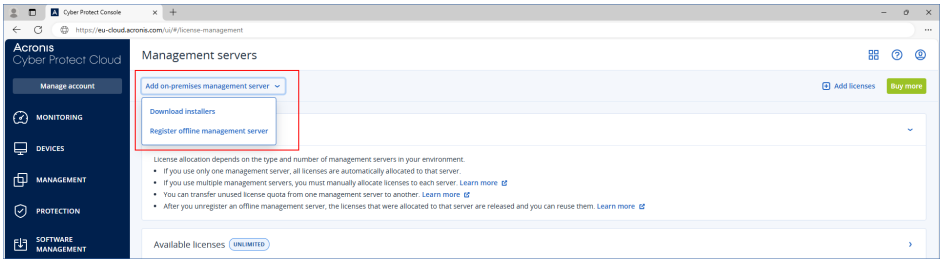


3. En **No tengo un archivo de activación**, haga clic en **Descargar el archivo de registro**.



   El archivo de registro se descarga en su equipo.
4. Mantenga abierto el cuadro de diálogo **Activación mediante archivo**.

5. Copie el archivo de registro descargado a una unidad que pueda utilizar en el equipo con acceso a Internet. Por ejemplo, puede utilizar una unidad flash USB.
6. En el equipo con acceso a Internet, inicie sesión en la consola de la nube (https://cloud.acronis.com) y después vaya a **Configuración** > **Servidores de administración**.
7. Haga clic en **Agregar servidor de administración local** y, a continuación, en **Registrar servidor de administración offline**.

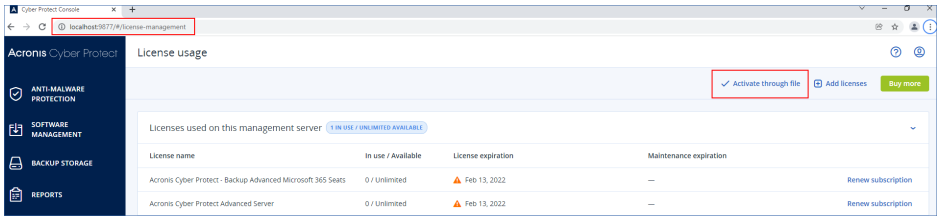


8. En el cuadro de diálogo que se abra, haga clic en **Explorar** y seleccione el archivo de registro que descargó en su servidor de administración offline.
9. En el cuadro de diálogo que se abra, haga clic en **Descargar archivo**.
   Se descargará un archivo de activación en su equipo.

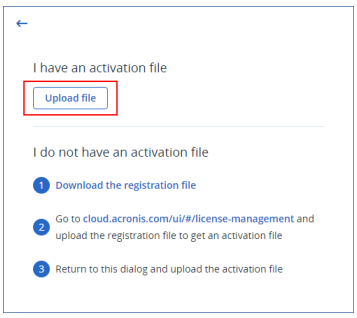
Importante
Si el servidor de gestión offline es el único de su entorno, las licencias de su cuenta de Acronis se asignarán automáticamente a él. El archivo de activación incluirá esta información, por lo que no es necesaria una asignación adicional.
Si no es el único servidor de gestión de su entorno, después de la activación, deberá asignar licencias según el procedimiento disponible en "Asignación de licencias a un servidor de gestión" (p. 39).

10. Copie el archivo de activación descargado a una unidad que pueda usar en el servidor de administración offline. Por ejemplo, puede usar una unidad flash USB.
11. En la consola local del servidor de administración offline (`https://<IP>:<port>`), vaya al cuadro de diálogo **Activación mediante archivo**.
    `IP` es la dirección de su servidor de administración y `port` es el puerto en el que está disponible la consola de Cyber Protect. De manera predeterminada, este puerto es el 9877.

Nota
Si el cuadro de diálogo **Activación mediante archivo** no está abierto, vaya a **Configuración**> **Uso de licencia** y, a continuación, haga clic en **Activar mediante archivo**.



12. En **Tengo un archivo de activación**, haga clic en **Cargar archivo** y, a continuación, seleccione el archivo de activación que haya descargado de la consola de la nube.



Como resultado, el servidor de gestión offline se registra y activa en su cuenta de Acronis.

Nota
Es posible que no pueda activar un servidor de administración que se está ejecutando en una máquina virtual si el UUID de la máquina virtual no es único. Por ejemplo, el UUID puede duplicarse cuando clona una máquina virtual o lo convierte con VMware vCenter Converter. Si se enfrenta a este problema, póngase en contacto con el equipo de soporte.

Para obtener más información acerca de cómo evitar la duplicación de UUID y cómo establecer un UUID único en una máquina virtual de VMware, consulte Modificar o conservar un UUID para una máquina virtual trasladada (1541) en la base de conocimientos de VMware.

Asignación de licencias a un servidor de gestión

Para utilizar una licencia, debe asignar su cuota o parte de su cuota a un servidor de administración.

Puede asignar más de una licencia a un servidor de administración. Además, puede dividir la cuota de licencia y asignar partes de esta a diferentes servidores de administración.

Nota
Si hay un único servidor de administración en su cuenta de Acronis, todas sus licencias se asignarán automáticamente a ese servidor. Para saber cómo reasignar licencias a otro servidor de administración, consulte la sección "Transferencia de la cuota de licencia a otro servidor de gestión" (p. 45).

Si tiene más de un servidor de administración en su cuenta de Acronis, puede ver las nuevas licencias en la consola en la nube (https://cloud.acronis.com), en **Licencias disponibles**. Debe asignar estas licencias manualmente.

Todas las operaciones con licencias se sincronizan automáticamente con los servidores de gestión en línea. Para sincronizar un cambio de asignación con un servidor de administración offline, cree un nuevo archivo de activación y repita el procedimiento de asignación. Para obtener más información acerca de los diferentes servidores de gestión, consulte "Tipos de servidores de gestión" (p. 29).

Para asignar licencias a un servidor de administración

Servidor de gestión en línea

1. En la consola de la nube (https://cloud.acronis.com), haga clic en **Configuración** > **Servidores de administración**.
2. Vaya al servidor de administración al que desee asignar una licencia.
3. Haga clic en **Agregar/eliminar licencias**.
4. En el cuadro de diálogo que se abra, indique la licencia y la cuota de licencia que quiera asignar al servidor.
5. Haga clic en **Confirmar**.

Como resultado, la información de las licencias se sincroniza automáticamente con el servidor de gestión y puede proteger sus cargas de trabajo con la licencia asignada.

Para modificar la asignación, repita el proceso de asignación.

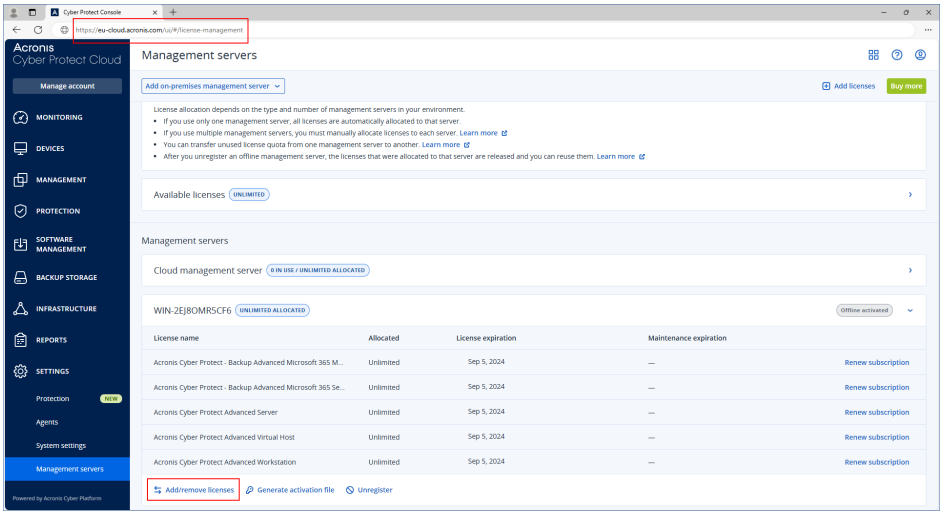
Importante
Si el número de agentes de protección es mayor que la cuota de licencia modificada, los agentes menos cargados dejarán de funcionar. Esta selección es automática. Si no satisface sus necesidades, reasigne las licencias disponibles de forma manual.

Servidor de gestión offline

Para esta operación, debe utilizar ambas consolas, la de la nube y la local.

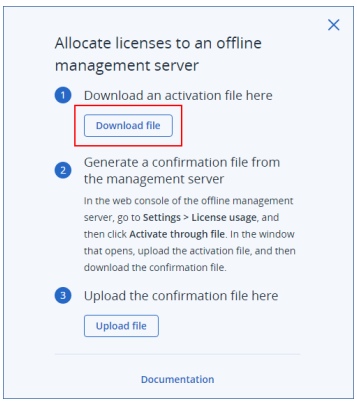
Para acceder a la consola de la nube, necesita un segundo equipo conectado a Internet.

1. En el equipo conectado a Internet, inicie sesión en la consola de la nube (https://cloud.acronis.com) y después vaya a **Configuración** > **Servidores de administración**.
2. Vaya al servidor de administración al que desee asignar una licencia.
3. Haga clic en **Agregar/eliminar licencias**.



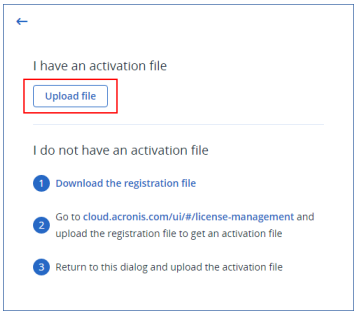
4. En el cuadro de diálogo que se abra, indique la licencia y la cuota de licencia que quiera asignar al servidor.
5. Haga clic en **Confirmar**.

6. En el cuadro de diálogo **Asignar licencias a un servidor de administración offline**, haga clic en **Descargar archivo**.



   El archivo de activación se descarga en su equipo.
7. Copie el archivo de activación descargado a una unidad que pueda usar en el servidor de administración offline. Por ejemplo, puede usar una unidad flash USB.
8. En la consola local del servidor de administración offline (`https://<IP>:<port>`), vaya a **Configuración** > **Uso de licencia** y, a continuación, haga clic en **Activar mediante archivo**.

   `IP` es la dirección de su servidor de administración y `port` es el puerto en el que está disponible la consola de Cyber Protect. De manera predeterminada, este puerto es el 9877.
9. En el cuadro de diálogo que se abra, en **Tengo un archivo de activación**, haga clic en **Cargar archivo** y, a continuación, seleccione el archivo de activación que haya descargado de la consola de la nube.



Como resultado, la información de la licencia se sincroniza entre su cuenta de Acronis y el servidor de gestión offline.

Para aumentar la cuota de licencia asignada, repita el proceso de asignación.

Para disminuir la cuota de licencia asignada, consulte "Disminución de la cuota de licencia asignada a un servidor de gestión offline" (p. 45).

Finalización conjunta de licencias

Puede utilizar la finalización conjunta de licencias para alinear las fechas de caducidad de varias licencias en su cuenta o elegir una fecha de caducidad diferente para una única licencia. Al utilizar la finalización conjunta, solo puede cambiar el plazo de la licencia. No puede cambiar la cuota de esta.

La finalización conjunta se aplica a las licencias de suscripción y al período de mantenimiento activo de las licencias perpetuas heredadas.

La alineación de las fechas de caducidad de las licencias incluye los siguientes procedimientos:

1. Solicitud de finalización conjunta de licencias a su proveedor de servicios.
2. Registro de las licencias finalizadas conjuntamente (alineadas) en su cuenta.
3. [Para servidores de administración offline] Sincronización de la información de licencia entre su cuenta y el servidor de administración offline.

Solicitud de finalización conjunta de licencias

Puede solicitar la finalización conjunta de licencias en la consola de la nube.

Importante
Para evitar facturaciones incorrectas, deshabilite la renovación automática de las licencias compradas en línea cancelando su suscripción. Para obtener más información, consulte este artículo de la base de conocimiento.

Pasos para solicitar la finalización conjunta de licencias

Rol requerido: administrador de la empresa o administrador de protección

1. En la consola de la nube de Cyber Protect, vaya a **Gestión de la empresa** > **Productos**.
2. Haga clic en **Solicitar finalización conjunta**.
3. Seleccione una o más licencias cuya fecha de caducidad desee cambiar.
   Puede seleccionar licencias con suscripción activa o licencias que expiraron hace un máximo de 30 días.
4. Seleccione una nueva fecha de caducidad.
   Puede seleccionar una fecha posterior a la fecha de caducidad de la licencia con el período más largo.
5. Haga clic en **Continuar**.
6. [Si la finalización conjunta no está disponible para todas las licencias seleccionadas] Elimine las licencias afectadas de su selección.
   Se destacan las licencias para las que no está disponible la finalización conjunta.
   a. Haga clic en **Eliminar las licencias afectadas**.
   b. Haga clic en **Continuar**.
7. Especifique una dirección de correo electrónico y haga clic en **Finalización conjunta**.

Como resultado, se crea una solicitud de finalización conjunta.

Cuando se realice el procesamiento de su solicitud de finalización conjunta, un representante de ventas se comunicará con usted. Si necesita ponerse en contacto con el equipo de ventas antes, haga clic en **Contactar con ventas**. Después de que se realice la comprobación de su solicitud de

finalización conjunta, recibirá un pedido de compra, una factura o un número de certificado por correo electrónico.

A continuación, debe registrar las licencias finalizadas conjuntamente (alineadas) en su cuenta. Para obtener más información, consulte "Registro de finalización conjunta de licencias" (p. 43).

Registro de finalización conjunta de licencias

Después de recibir un pedido de compra, una factura o un número de certificado por correo electrónico, debe registrar las licencias finalizadas conjuntamente (alineadas) en su cuenta.

Pasos para registrar la finalización conjunta de licencias

Rol requerido: administrador de la empresa o administrador de protección

1. En la consola de la nube de Cyber Protect, vaya a **Gestión de la empresa** > **Productos**.
2. Haga clic en **Registrar la finalización conjunta**.
3. Especifique su dirección de correo electrónico de facturación y una de las siguientes opciones:
   - Número de pedido de compra
   - Número de factura
   - Número de certificado de licencia

   Puede encontrar estos números en el documento PDF que se ha enviado a su dirección de correo electrónico.
4. Haga clic en **Registrar**.

Como resultado, se actualiza la información de la licencia en su cuenta.

Importante
Si utiliza un servidor de administración offline, debe sincronizar la información de la licencia actualizada con él. Para obtener más información, consulte"Sincronización de renovaciones o finalización conjunta de licencias con un servidor de administración offline" (p. 43).

Sincronización de renovaciones o finalización conjunta de licencias con un servidor de administración offline

Para los servidores de administración offline, debe sincronizar manualmente la información de la licencia de su cuenta de Acronis con el servidor de administración después de realizar cualquiera de las siguientes acciones:

- renovar una licencia de suscripción
- renovar un período de mantenimiento
- finalizar licencias conjuntamente

Para los servidores de administración online, la sincronización es automática.

Requisitos previos

- Ha renovado su licencia de suscripción o el período de mantenimiento, o ha finalizado licencias conjuntamente.
- La información de la licencia actualizada se muestra en el portal para clientes.

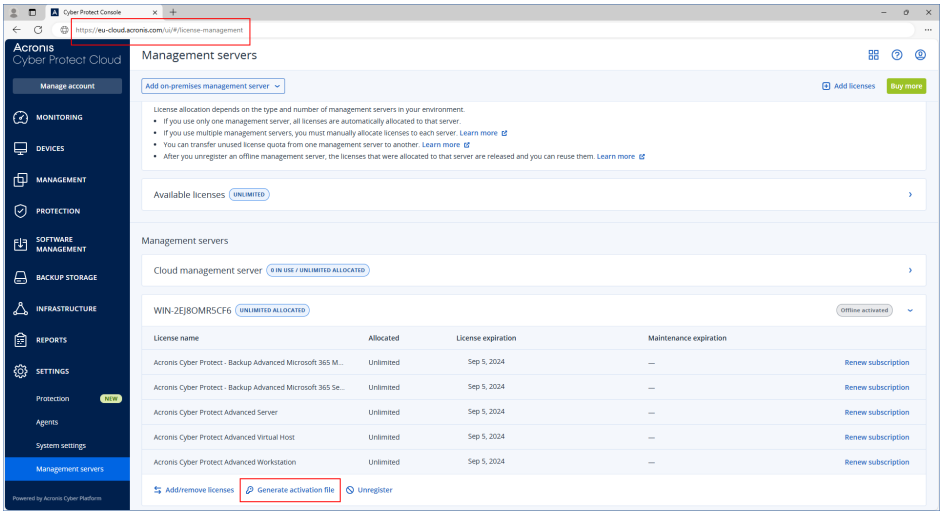
Nota
Para los clientes, el portal de cliente de Acronis forma parte de la consola de la nube. Se redirige a estos clientes a la consola de la nube cuando inician sesión en su cuenta en https://account.acronis.com.

Pasos para sincronizar las renovaciones o finalización conjunta de licencias

Para esta operación, debe utilizar ambas consolas, la de la nube y la local.

Para acceder a la consola de la nube, necesita un segundo equipo conectado a Internet.

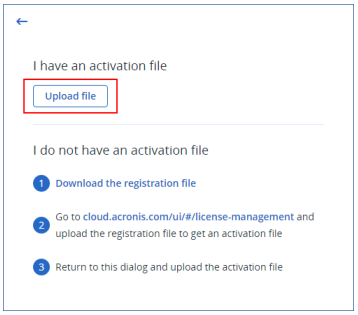
1. En el equipo conectado a Internet, inicie sesión en la consola de la nube (https://cloud.acronis.com) y después vaya a **Configuración** > **Servidores de administración**.
2. Vaya al servidor de administración offline con el que desea sincronizar la información de licencia actualizada.
3. Haga clic en **Generar archivo de activación**.



El archivo de activación se descarga en su equipo.

4. Copie el archivo de activación descargado a una unidad que pueda usar en el servidor de administración offline. Por ejemplo, puede usar una unidad flash USB.
5. En la consola local del servidor de administración offline (`https://<IP>:<port>`), vaya a **Configuración** > **Uso de licencia** y, a continuación, haga clic en **Activar mediante archivo**.
   `IP` es la dirección de su servidor de administración y `port` es el puerto en el que está disponible la consola de Cyber Protect. De manera predeterminada, este puerto es el 9877.
6. En el cuadro de diálogo que se abra, en **Tengo un archivo de activación**, haga clic en **Cargar archivo** y, a continuación, seleccione el archivo de activación que haya descargado de la consola

de la nube.



Como resultado, la información de la licencia se sincroniza entre su cuenta de Acronis y el servidor de gestión offline.

Transferencia de la cuota de licencia a otro servidor de gestión

Puede transferir una cuota de licencia de un servidor de administración a otro. Esta opción es útil cuando ninguna carga de trabajo utiliza las licencias asignadas a un servidor de administración y necesita más cuota de licencia para otro servidor de administración.

Nota
Si hay un único servidor de gestión en su cuenta de Acronis, todas sus licencias se asignarán automáticamente a ese servidor.

Si tiene más de un servidor de administración en su cuenta de Acronis, puede ver las nuevas licencias en la consola en la nube (https://cloud.acronis.com), en **Licencias disponibles**. Debe asignar estas licencias manualmente.

Pasos para transferir la cuota de licencia a otro servidor de gestión

1. Disminuya la cuota de licencia asignada al servidor de administración original.
   Para obtener más información, consulte los siguientes temas:
   - [Para servidores de administración en línea] "Asignación de licencias a un servidor de gestión" (p. 39)"Asignación de licencias a un servidor de gestión" (p. 39)
   - [Para servidores de administración offline] "Disminución de la cuota de licencia asignada a un servidor de gestión offline" (p. 45)

   Como resultado, la cuota de licencia liberada aparece en la sección **Licencias disponibles** de la consola de la nube.
2. Asigne la cuota de licencia al segundo servidor de gestión siguiendo el procedimiento disponible en "Asignación de licencias a un servidor de gestión" (p. 39).

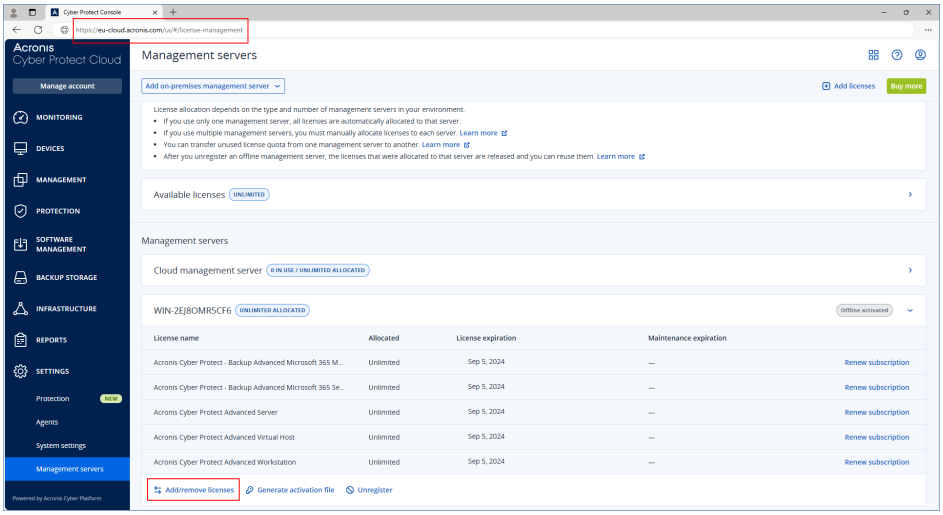
Disminución de la cuota de licencia asignada a un servidor de gestión offline

Para esta operación, debe utilizar ambas consolas, la de la nube y la local.

Para acceder a la consola de la nube, necesita un segundo equipo conectado a Internet.

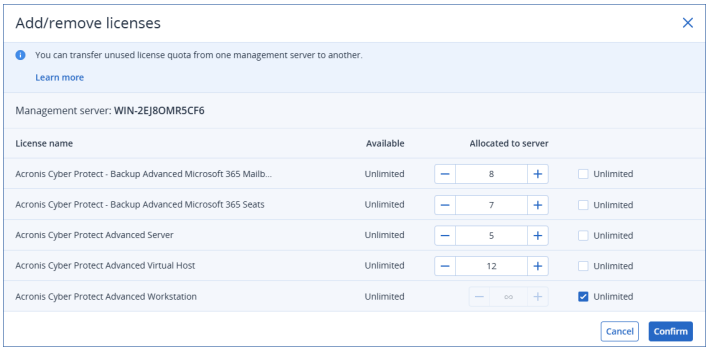
Para reducir la cuota de licencia

1. En el equipo conectado a Internet, inicie sesión en la consola de la nube (https://cloud.acronis.com) y después vaya a **Configuración** > **Servidores de administración**.
2. Vaya al servidor de administración para el que desee reducir la cuota de licencia y, a continuación, haga clic en **Agregar/eliminar licencias**.

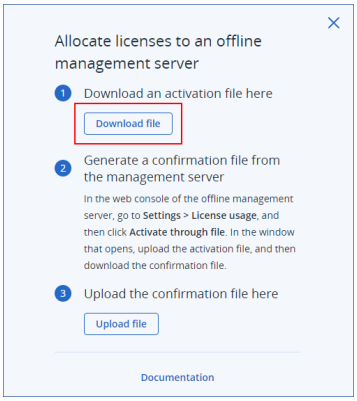


3. En el cuadro de diálogo que se abre, modifique la cuota de licencia según sea necesario y, a continuación, haga clic en **Confirmar**.

   La asignación de una cuota de licencia igual a cero eliminará la licencia del servidor.



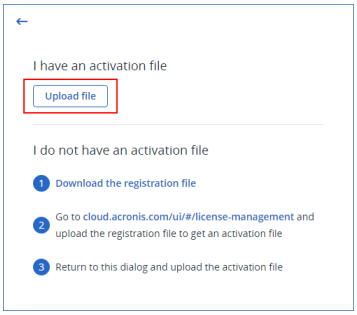
4. En el cuadro de diálogo **Asignar licencias a un servidor de administración offline**, haga clic en **Descargar archivo**.



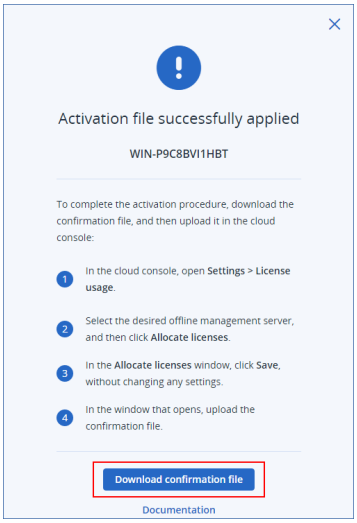
   El archivo de activación se descarga en su equipo.

5. Copie el archivo de activación descargado a una unidad que pueda usar en el servidor de administración offline. Por ejemplo, puede usar una unidad flash USB.
6. En la consola local del servidor de administración offline (`https://<IP>:<port>`), vaya a **Configuración** > **Uso de licencia** y, a continuación, haga clic en **Activar mediante archivo**.

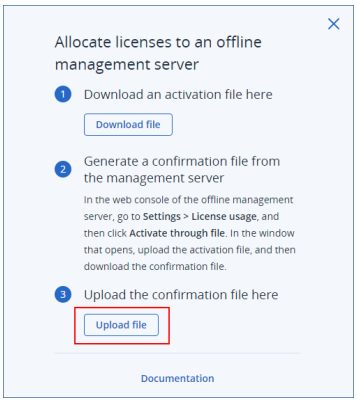
   `IP` es la dirección de su servidor de administración y `port` es el puerto en el que está disponible la consola de Cyber Protect. De manera predeterminada, este puerto es el 9877.
7. En el cuadro de diálogo que se abra, en **Tengo un archivo de activación**, haga clic en **Cargar archivo** y, a continuación, seleccione el archivo de activación que haya descargado de la consola de la nube.



8. En el cuadro de diálogo que se abra, haga clic en **Descargar archivo de confirmación**.



   El archivo de confirmación se descarga en su equipo.
9. Copie el archivo de confirmación descargado en una unidad que pueda utilizar en el equipo con acceso a Internet. Por ejemplo, puede utilizar una unidad flash USB.
10. En el equipo conectado a Internet, inicie sesión en la consola de la nube (https://cloud.acronis.com) y después vaya a **Configuración** > **Servidores de administración**.
11. Vaya al servidor de administración para el que desee reducir la cuota de licencia y, a continuación, haga clic en **Agregar/eliminar licencias**.
12. En el cuadro de diálogo que se abra, haga clic en **Confirmar** sin cambiar la configuración.
13. En el cuadro de diálogo **Asignar licencias a un servidor de administración offline**, haga clic en **Cargar archivo** y, a continuación, seleccione el archivo de confirmación que descargó de su servidor de administración offline.



Como resultado, la información de la licencia se sincroniza entre su cuenta de Acronis y el servidor de gestión offline.

Importante
Si el número de agentes de protección es mayor que la cuota de licencia modificada, los agentes menos cargados dejarán de funcionar. Esta selección es automática. Si no satisface sus necesidades, reasigne las licencias disponibles de forma manual.

Asignar licencias a cargas de trabajo

Un servidor de gestión distribuye las licencias asignadas entre las cargas de trabajo que están registradas en el servidor.

El servidor de administración asigna una licencia a una carga de trabajo la primera vez que aplica un plan de protección a esa carga de trabajo. Si se asigna más de una licencia al servidor de administración, este asigna la licencia más adecuada en función del tipo de carga de trabajo, el sistema operativo y el nivel de protección necesario.

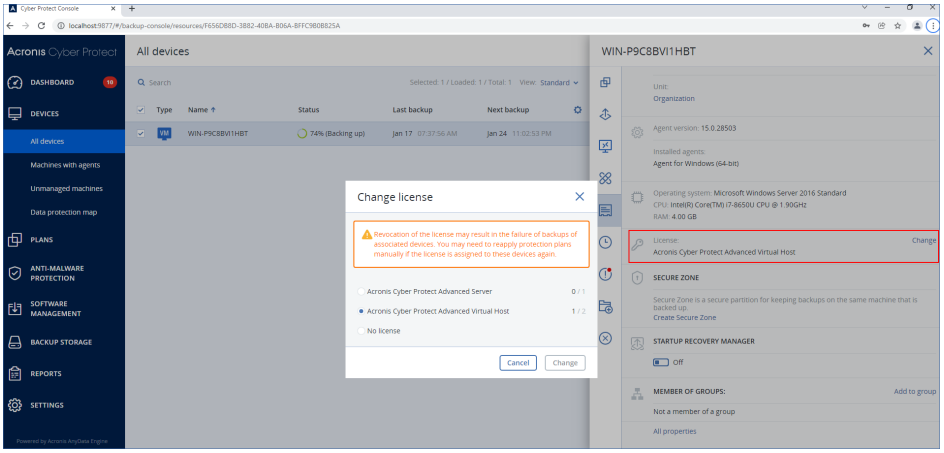
Puede ver la licencia de la carga de trabajo en la pestaña **Detalles** de la carga de trabajo.

Puede modificar manualmente una licencia asignada automáticamente. Las operaciones manuales con licencias solo están disponibles para los administradores de la organización.

Para cambiar una licencia asignada automáticamente

1. En la consola de Cyber Protect, haga clic en **Dispositivos** y, a continuación, seleccione la carga de trabajo.
2. Haga clic en **Detalles**.
3. [Para servidores de gestión in situ] Vaya a la sección **Licencia** y, a continuación, haga clic en **Cambiar**.
4. [Para servidores de gestión de la nube] Vaya a la sección **Cuota de servicio** y, a continuación, haga clic en **Cambiar**.
5. Seleccione la licencia (cuota de servicio) que desea asignar a la carga de trabajo y, a

continuación, haga clic en **Cambiar**.



Limitaciones

- En los servidores de administración offline, el uso actual de la cuota de licencia se muestra solo en la consola local. Esto sucede porque los servidores de administración offline no sincronizan estos datos con su cuenta de Acronis.

Problemas conocidos

- El uso de la licencia o la asignación de la licencia de **Virtual Host** pueden mostrarse de forma incorrecta en la consola de la nube. Para obtener más información, consulte este artículo de la base de conocimientos.

Cancelación del registro de un servidor de gestión

Puede cancelar el registro de un servidor de administración y reutilizar las licencias asignadas en otro servidor de administración de su cuenta.

Después de cancelar el registro, las licencias asignadas se liberan y puede gestionarlas en la consola de la nube. Las licencias están disponibles en la pestaña **Configuración** > **Servidores de administración**, en la sección **Licencias disponibles**.

Pasos para cancelar el registro de un servidor de administración en línea

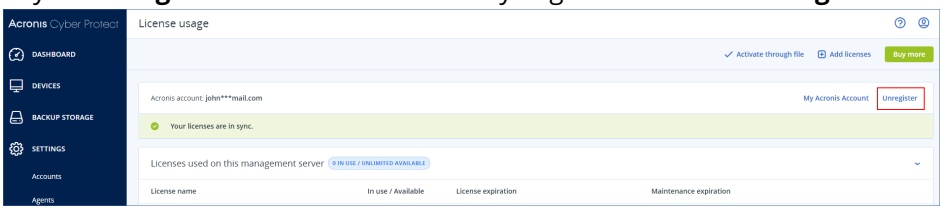
Puede cancelar el registro de un servidor de administración en línea mediante la consola local o la consola de la nube. Ambos procedimientos eliminan el servidor de administración de su cuenta.

Pasos para cancelar el registro de un servidor de gestión en línea

Desde la consola local

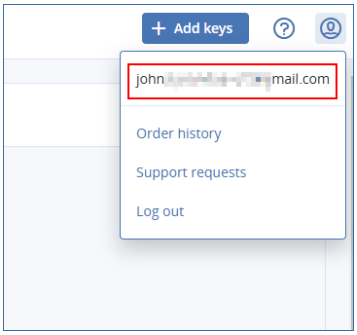
1. Inicie sesión en la consola local del servidor de administración de la que desea cancelar el registro (`https://<IP>:<port>`).
   `IP` es la dirección de su servidor de administración y `port` es el puerto en el que está disponible la consola de Cyber Protect. De manera predeterminada, este puerto es el 9877.

2. Vaya a **Configuración** > **Uso de licencia** y haga clic en **Cancelar registro**.



3. Especifique el inicio de sesión para su cuenta de Acronis y, a continuación, haga clic en **Cancelar registro**.

   Este inicio de sesión es el correo electrónico que utiliza para iniciar sesión en su cuenta en https://account.acronis.com y https://cloud.acronis.com.



Como resultado, todas las licencias que se asignen a este servidor se liberan y se asignan a otro servidor de administración de su cuenta. En la consola local del servidor de administración no registrado, las licencias se restablecen a cero.

Desde la consola de la nube

1. Inicie sesión en la consola de la nube (https://cloud.acronis.com) como administrador.
2. Vaya a **Configuración** > **Servidores de gestión**.
3. Vaya al servidor de administración del que desea cancelar el registro y luego haga clic en **Cancelar registro**.
4. Haga clic en **Cancelar registro** para confirmar su elección.

Como resultado, todas las licencias que se asignen a este servidor se liberan y se asignan a otro servidor de administración de su cuenta. En la consola local del servidor de administración no registrado, las licencias se restablecen a cero.

Pasos para cancelar el registro de un servidor de administración offline

Para esta operación, debe utilizar ambas consolas, la de la nube y la local.

Para acceder a la consola de la nube, necesita un segundo equipo conectado a Internet.

Pasos para cancelar el registro de un servidor de gestión offline

Con Cyber Protect 15, versión 6 y posteriores, puede iniciar el procedimiento de cancelación del registro desde la consola local o desde la consola de la nube. Ambos procedimientos eliminan el

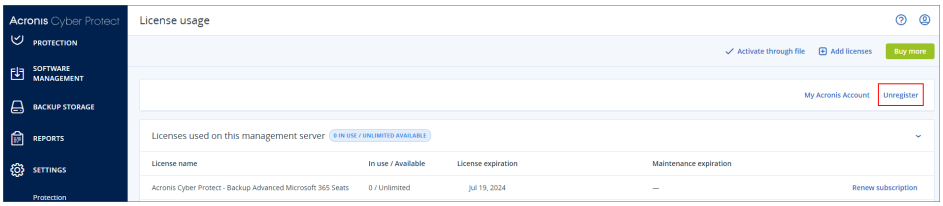
servidor de administración de su cuenta. Con Cyber Protect 15, versión 5 y anteriores, puede iniciar el procedimiento de cancelación del registro solo desde la consola de la nube.

Estos procedimientos se aplican únicamente a los servidores de administración offline a los que puede acceder. Para obtener más información, consulte "Cancelar el registro de un servidor de administración offline inaccesible" (p. 55).

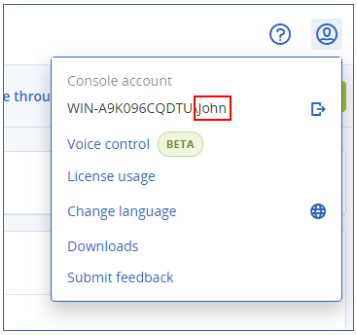
Desde la consola local

Este procedimiento está disponible con Cyber Protect 15, versión 6 y posteriores.

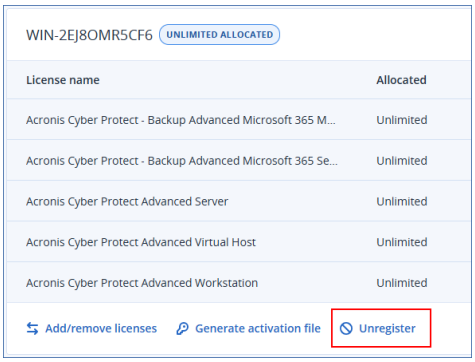
1. Inicie sesión en la consola local del servidor de administración de la que desea cancelar el registro (`https://<IP>:<port>`).
   `IP` es la dirección de su servidor de administración y `port` es el puerto en el que está disponible la consola de Cyber Protect. De manera predeterminada, este puerto es el 9877.
2. Vaya a **Configuración** > **Uso de licencia** y haga clic en **Cancelar registro**.



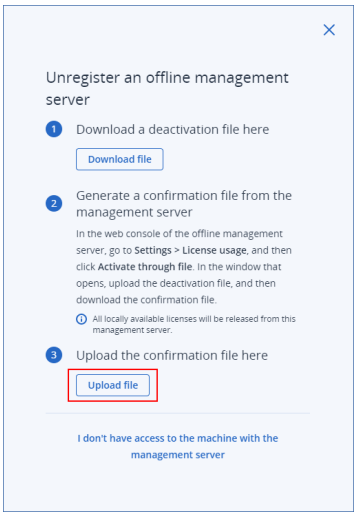
3. Especifique su inicio de sesión de la cuenta de la consola y, a continuación, haga clic en **Cancelar registro**.
   Este inicio de sesión es el nombre que utiliza para iniciar sesión en la consola local.



4. En el cuadro de diálogo **La cancelación del registro se realizó correctamente**, haga clic en **Descargar archivo de cancelación del registro**.
   El archivo `forced_deactivation_file.bin` se descarga en su equipo.
5. Copie el archivo `forced_deactivation_file.bin` en una unidad que pueda utilizar en el equipo con acceso a Internet. Por ejemplo, puede utilizar una unidad flash USB.
6. En un equipo con acceso a Internet, inicie sesión en la consola de la nube (https://cloud.acronis.com).
7. Vaya a **Configuración** > **Servidores de administración** y, a continuación, busque el servidor de administración del que desea cancelar el registro.
8. Haga clic en **Cancelar registro**.



9. En el cuadro de diálogo **Cancelar el registro de un servidor de administración offline**, en **Cargar el archivo de confirmación aquí**, haga clic en **Cargar archivo**.

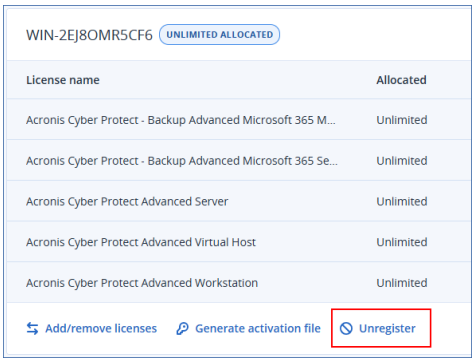


10. Cargue el archivo `forced_deactivation_file.bin`.
11. En el cuadro de diálogo **Se ha cancelado el registro del servidor de administración**, haga clic en **Cerrar**.

Como resultado, todas las licencias que se asignen a este servidor se liberan y se asignan a otro servidor de administración de su cuenta. En la consola local del servidor de administración no registrado, las licencias se restablecen a cero.

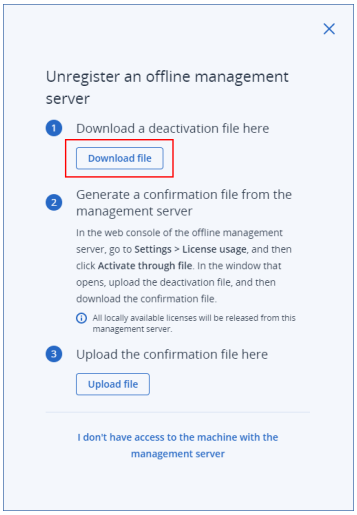
Desde la consola de la nube

1. En el equipo con acceso a Internet, inicie sesión en la consola de la nube (https://cloud.acronis.com) como administrador.
2. Vaya a **Configuración** > **Servidores de gestión**.
3. Vaya al servidor de administración offline del que desea cancelar el registro y luego haga clic en **Cancelar registro**.



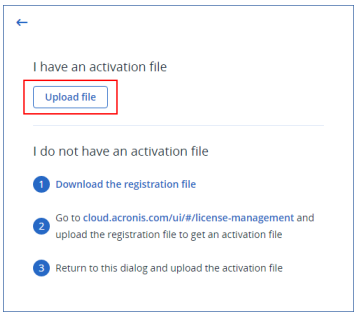
4. En el cuadro de diálogo **Cancelar el registro de un servidor de administración offline**, en **Descargar aquí un archivo de desactivación**, haga clic en **Descargar archivo**.

   El archivo `deactivation_file.bin` se descargará en su equipo.

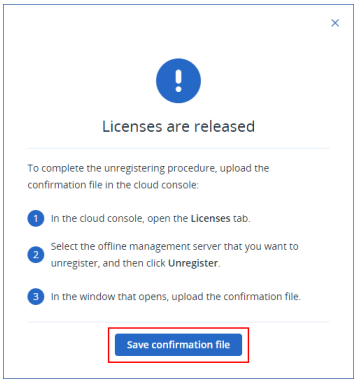


5. Mantenga abierto el cuadro de diálogo **Cancelar registro de un servidor de administración offline**.
6. Copie el archivo `deactivation_file.bin` a una unidad que pueda utilizar en el servidor de administración offline. Por ejemplo, puede utilizar una unidad flash USB.
7. En el servidor de administración offline del que desea cancelar el registro (`https://<IP>:<port>`), inicie sesión en la consola local.

   `IP` es la dirección de su servidor de administración y `port` es el puerto en el que está disponible la consola de Cyber Protect. De manera predeterminada, este puerto es el 9877.
8. Vaya a **Configuración** > **Uso de licencia** y, a continuación, haga clic en **Activar mediante archivo**.
9. En el cuadro de diálogo que se abra, en **Tengo un archivo de activación**, haga clic en **Cargar archivo** y, a continuación, seleccione el archivo `deactivation_file.bin`.

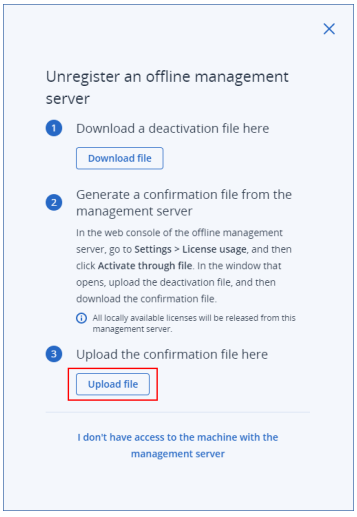


10. En el nuevo cuadro de diálogo que se abra, haga clic en **Guardar archivo de confirmación.**



El archivo `confirmation_file.bin` se descargará en su equipo.

11. Copie el archivo `confirmation_file.bin` en una unidad que pueda utilizar en el equipo con acceso a Internet. Por ejemplo, puede utilizar una unidad flash USB.
12. En un equipo con acceso a Internet, inicie sesión en la consola de la nube (https://cloud.acronis.com) como administrador.
13. [Si no está abierto el cuadro de diálogo **Cancelar el registro de un servidor de administración offline**] Vaya a **Configuración** > **Servidores de administración**, busque el servidor de administración del que desea anular el registro y, a continuación, haga clic en **Cancelar registro**.
14. En el cuadro de diálogo **Cancelar el registro de un servidor de administración offline**, en **Cargar el archivo de confirmación aquí**, haga clic en **Cargar archivo**.



15. Cargue el archivo `confirmation_file.bin`.

16. En el **servidor de administración del que ha cancelado el registro**, haga clic en **Cerrar**.

Como resultado, todas las licencias que se asignen a este servidor se liberan y se asignan a otro servidor de administración de su cuenta. En la consola local del servidor de administración no registrado, las licencias se restablecen a cero.

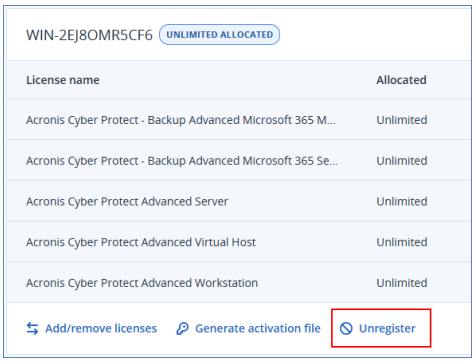
Cancelar el registro de un servidor de administración offline inaccesible

Puede cancelar el registro de un servidor de administración offline al que no tenga acceso.

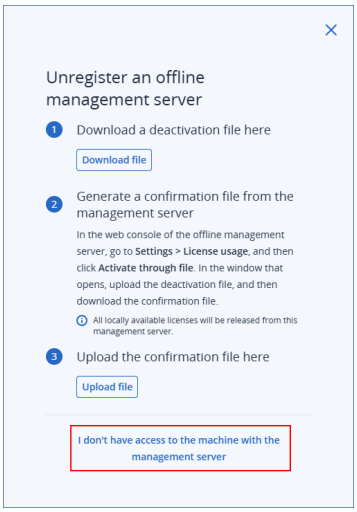
Advertencia.
Este servidor se eliminará permanentemente de su cuenta y no podrá volver a añadirlo.

Pasos para cancelar el registro de un servidor de administración offline

1. Inicie sesión en la consola de la nube (`https://cloud.acronis.com`) como administrador.
2. Vaya a **Configuración** > **Servidores de administración** y, a continuación, busque el servidor de administración del que desea cancelar el registro.
3. Haga clic en **Cancelar registro**.



4. En el cuadro de diálogo **Cancelar el registro de un servidor de administración offline**, haga clic en **No tengo acceso al equipo con el servidor de administración**.



5. Especifique su inicio de sesión para confirmar y, a continuación, haga clic en **Bloquear permanentemente**.

Este inicio de sesión es el correo electrónico que utiliza para iniciar sesión en su cuenta en https://account.acronis.com y https://cloud.acronis.com.

6. En el cuadro de diálogo **Se ha cancelado el registro del servidor de administración**, haga clic en **Cerrar**.

Como resultado, todas las licencias que se asignen a este servidor se liberan y se asignan a otro servidor de administración de su cuenta. En la consola local del servidor de administración no registrado, las licencias se restablecen a cero.

Este servidor está bloqueado y no puede añadirlo a su cuenta de nuevo.

Licencia de Acronis Cyber Protect 15, actualización 2 y anteriores

Para comenzar a utilizar la actualización 2 y anteriores de Acronis Cyber Protect 15, deberá añadir al menos una clave de licencia al servidor de gestión. Se asigna automáticamente una licencia a un equipo cuando se aplica un plan de protección.

Las licencias también pueden asignarse y revocarse manualmente. Las operaciones manuales con licencias solo están disponibles para administradores de la organización. Para obtener más información sobre los administradores, consulte "Unidades y cuentas administrativas" (p. 710).

Conectar claves de licencia a un servidor de gestión

En Acronis Cyber Protect 15, actualización 2 y anteriores, añada las claves de licencia al servidor de gestión.

Pasos para conectar claves de licencia a un servidor de gestión

1. En la consola web de Cyber Protect, vaya a **Configuración** > **Licencias**.
2. Haga clic en **Añadir claves**.
3. Introduzca una o más claves de licencia, una por línea.
4. Haga clic en **Agregar**.
5. [Al añadir las claves de licencia de la suscripción] Para activar una suscripción, inicie sesión en su cuenta de Acronis.
   a. En el formulario de inicio de sesión, introduzca las credenciales que utilice para el portal de clientes de Acronis (https://account.acronis.com) y, a continuación, haga clic en **Iniciar sesión**.
   b. Confirme su cuenta y haga clic en **Sincronizar**.
   c. Cuando la operación se complete, haga clic en **Listo**.
6. En el panel **Añadir claves de licencias**, haga clic en **Listo**.

Nota

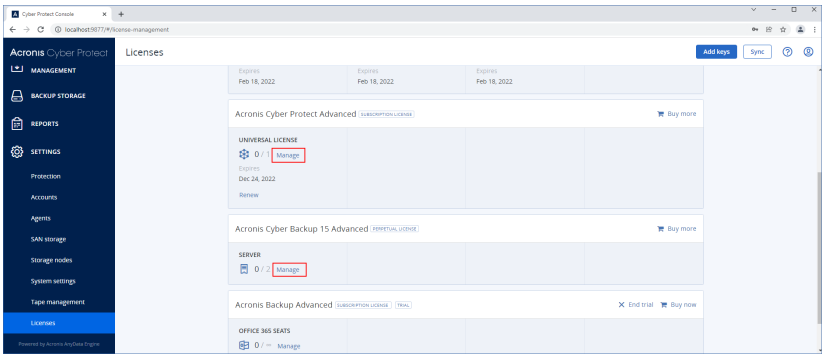
Puede importar automáticamente las claves de licencias de la suscripción que están registradas en su cuenta de Acronis en lugar de añadirlas de nuevo al servidor de gestión. Para importar las claves de licencia, en el panel **Agregar claves de licencia**, haga clic en **Sincronizar con la cuenta de Acronis** y, a continuación, inicie sesión en su cuenta de Acronis.

Gestión de licencias de suscripción

Antes de añadir una licencia a una carga de trabajo, tiene que añadir la clave de licencia al servidor de administración. Para obtener más información consulte "Conectar claves de licencia a un servidor de gestión" (p. 56).

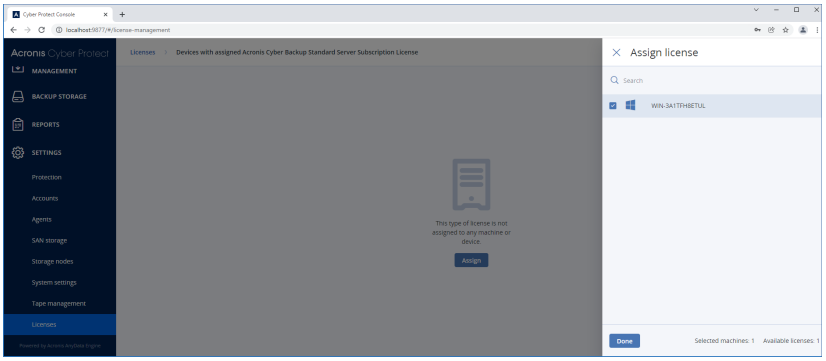
Pasos para asignar una licencia de suscripción a una carga de trabajo

1. En la consola web de Cyber Protect, vaya a **Configuración** > **Licencias**.
2. Vaya a la licencia que desee y, a continuación, haga clic en **Gestionar**.



3. Haga clic en **Asignar**.

   Se muestran las cargas de trabajo a las que puede asignar esta licencia.



4. Seleccione una carga de trabajo y haga clic en **Listo**.

Pasos para revocar una licencia de suscripción de una carga de trabajo

1. En la consola web de Cyber Protect, vaya a **Configuración** > **Licencias**.
2. Vaya a la licencia que desee y, a continuación, haga clic en **Gestionar**.

   Se muestran todas las cargas de trabajo a las que está asignada esta licencia.
3. Seleccione la carga de trabajo de la que desee revocar la licencia.

4. Haga clic en **Revocar**.
5. Confirme su decisión.

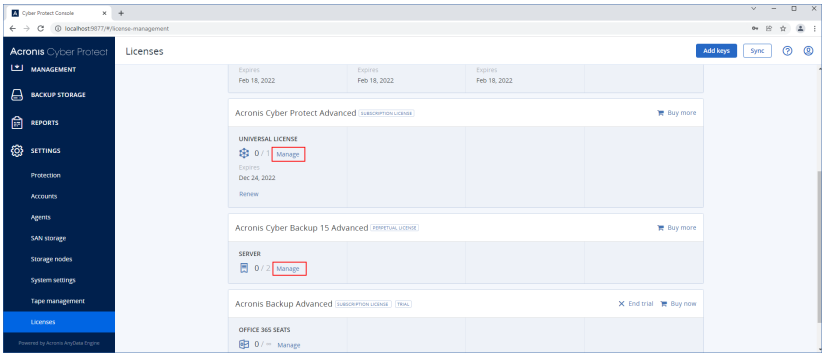
   La licencia revocada se libera y puede asignarla a otra carga de trabajo.

Gestión de licencias perpetuas

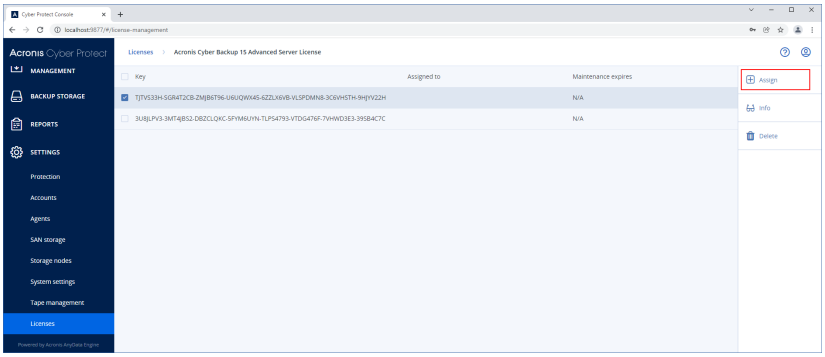
Antes de añadir una licencia a una carga de trabajo, tiene que añadir la clave de licencia al servidor de administración. Para obtener más información consulte "Conectar claves de licencia a un servidor de gestión" (p. 56).

Pasos para asignar una licencia perpetua a una carga de trabajo

1. En la consola web de Cyber Protect, vaya a **Configuración** > **Licencias**.
2. Vaya a la licencia que desee y, a continuación, haga clic en **Gestionar**.



   Se muestran las claves de licencia que corresponden a la licencia seleccionada.
3. Seleccione la clave de licencia que desea asignar a una carga de trabajo.
4. Haga clic en **Asignar**.



   Se muestran las cargas de trabajo a las que puede asignar esta clave de licencia.
5. Seleccione una carga de trabajo y haga clic en **Listo**.

Pasos para revocar una licencia perpetua de una carga de trabajo

1. En la consola web de Cyber Protect, vaya a **Configuración** > **Licencias**.
2. Seleccione la licencia que desee y, a continuación, haga clic en **Gestionar**.

   Se muestran las claves de licencia que corresponden a la licencia seleccionada. Compruebe la carga de trabajo a la que está asignada la clave de licencia en la columna **Asignada a**.

3. Seleccione la clave de licencia que desea revocar.
4. Haga clic en **Revocar**.
5. Confirme su decisión.
   La clave de licencia revocada sigue en la lista de licencias y puede asignarla a otra carga de trabajo.

Instalación

Información general acerca de la instalación

Acronis Cyber Protect admite dos métodos de implementación: local y en la nube. La diferencia principal entre ellos es la ubicación del servidor de administración de Acronis Cyber Protect.

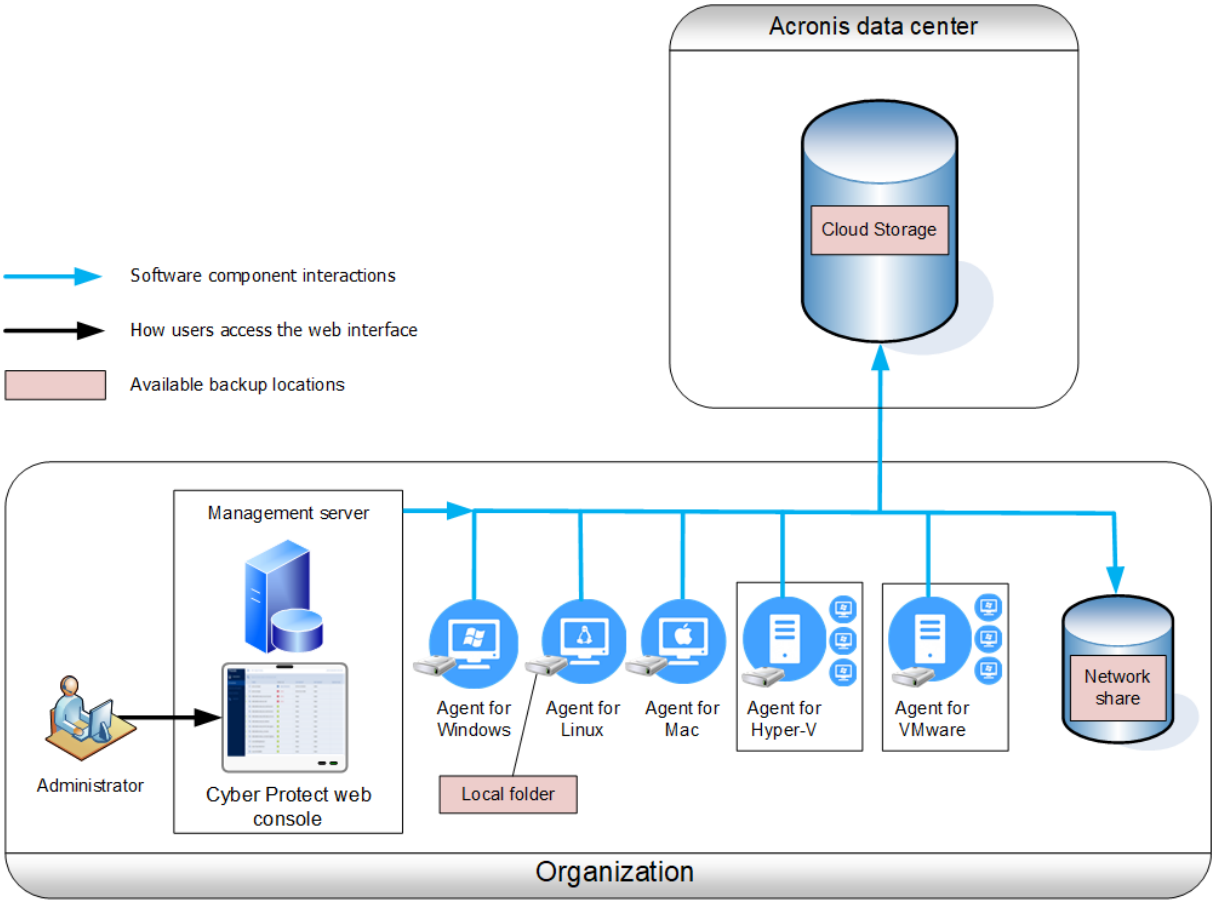
El servidor de administración es el punto central para gestionar todas las copias de seguridad. Con la implementación local, se instala en la red local; con la implementación en la nube, se ubica en uno de los centros de datos de Acronis. La interfaz web a este servidor es lo que se llama una consola web de Cyber Protect.

El servidor de administración se encarga de la comunicación con los agentes de protección y lleva a cabo las funciones de gestión del plan general. Antes de cada protección de actividad, los agentes consultan el servidor de gestión para comprobar los requisitos previos. A veces se puede perder la conexión con el servidor de gestión, por lo que no se implementarán los nuevos planes de protección. Sin embargo, si ya se ha implementado un plan de protección en un equipo, el agente continúa con las operaciones de protección durante 30 días después de que se pierda la comunicación con el servidor de gestión.

Ambos tipos de implementación requieren la instalación de un agente de protección en cada equipo del que desee realizar una copia de seguridad. Los tipos compatibles de almacenamiento también son los mismos: El espacio de almacenamiento en la nube se vende aparte de las licencias de Acronis Cyber Protect.

Implementación local

La implementación local significa que todos los componentes del producto se instalan en la red local. Se trata del único método de implementación disponible con una licencia perpetua. Además, deberá utilizar este método si sus equipos no están conectados a Internet.



Ubicación del servidor de gestión

Puede instalar el servidor de gestión en un equipo que ejecute Windows o Linux.

Se recomienda la instalación en Windows porque así podrá implementar los agentes en otros equipos desde el servidor de gestión. Con la licencia de Advanced, se pueden crear unidades organizativas y añadirles administradores. De esta forma, puede delegar la gestión de protección a otras personas cuyos permisos de acceso estarán estrictamente limitados a las unidades correspondientes.

Se recomienda la instalación en Linux en un entorno exclusivo de Linux. Deberá instalar un agente localmente en los equipos de los que desee realizar copias de seguridad.

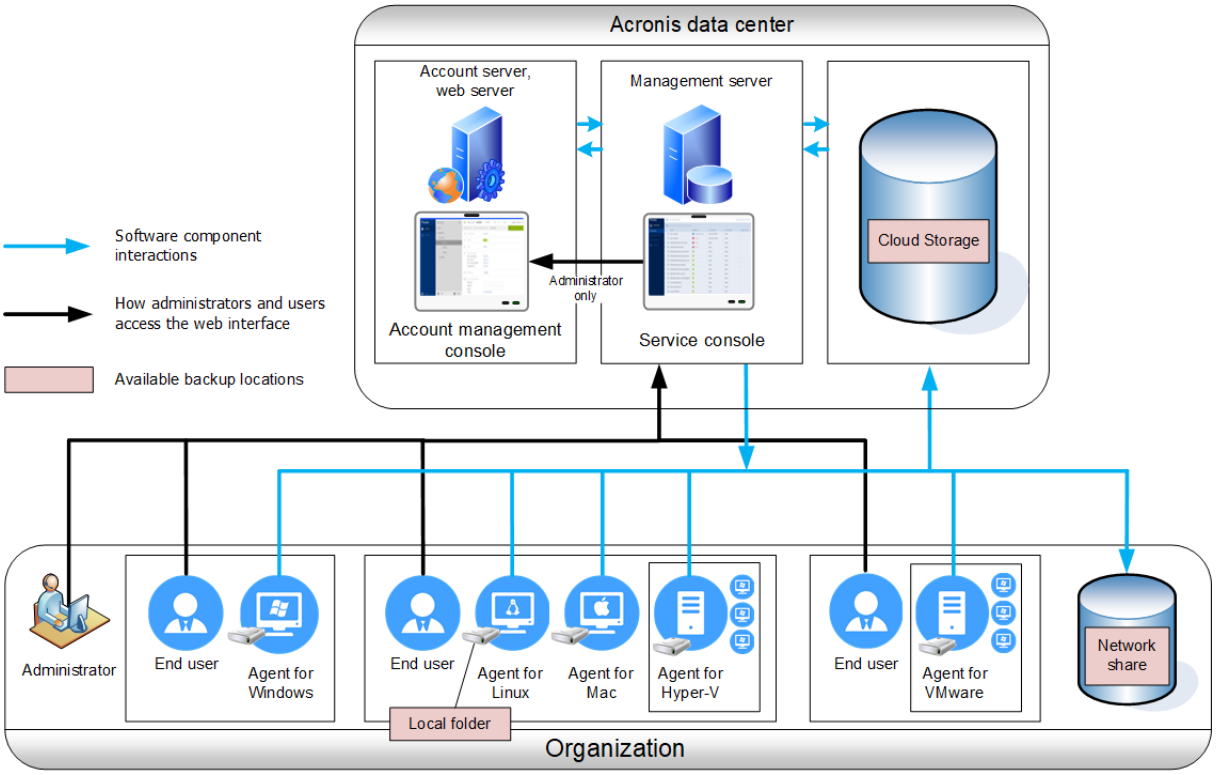
Implementación en la nube

La implementación en la nube significa que el servidor de gestión está ubicado en uno de los centros de datos de Acronis. La ventaja de este enfoque es que no es necesario mantener el servidor de gestión en la red local. Puede considerar Acronis Cyber Protect un servicio de ciberprotección que le presta Acronis.

El acceso al servidor de cuentas le permite crear cuentas de usuarios, establecer cuotas de uso de servicio para ellos y crear grupos de usuarios (unidades) para reflejar la estructura de la

organización. Cada usuario podrá acceder a la consola web de Cyber Protect, descargarse el agente requerido e instalarlo en sus equipos en cuestión de minutos.

Las cuentas de administradores se pueden crear a nivel de unidad o de organización. Cada cuenta tiene una vista centrada en su área de control. Los usuarios solo tienen acceso a sus propias copias de seguridad.



En la tabla siguiente se resumen las diferencias entre las implementaciones locales y en la nube. Cada columna indica las características que están disponibles solo en el tipo de implementación correspondiente.

Implementación local	Implementación en la nube
• Se pueden utilizar licencias perpetuas • Servidor de administración in situ que puede utilizarse en entornos aislados* • Servidor SFTP como ubicación de la copia de seguridad • Acronis Cyber Infrastructure como ubicación de la copia de seguridad • Dispositivos de cintas y nodos de almacenamiento de Acronis como ubicaciones de la copia de seguridad** • Actualización desde versiones anteriores de Acronis Cyber Protect, incluido Acronis Backup para VMware	• Copia de seguridad de la nube a la nube de los datos de Microsoft Office 365, incluida la protección de grupos, carpetas públicas y datos de OneDrive y SharePoint Online • Copia de seguridad de la nube a la nube de los datos de Google Workspace • Agente para Mac es compatible con procesadores basados en ARM y x64, como Apple Silicon M1 y M2 • Agente para Virtuozzo (copia de seguridad de máquinas virtuales Virtuozzo en el nivel del hipervisor) • Agente para oVirt (copia de seguridad de

	máquinas virtuales oVirt KVM en el nivel del hipervisor) • Agente para Virtuozzo Hybrid Infrastructure (copia de seguridad de máquinas virtuales Virtuozzo Hybrid Infrastructure en el nivel del hipervisor) • Recuperación ante desastres como servicio en la nube****

* Para obtener más información sobre cómo activar el servidor de administración en un entorno aislado, consulte "Pasos para activar un servidor de gestión offline" (p. 37).

** La función no está disponible en la edición estándar.

***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 archivo.

**** La función solo está disponible con el complemento de Disaster Recovery.

Componentes

Agentes

Los agentes son aplicaciones que realizan copias de seguridad, recuperación y otras operaciones con los datos de los equipos gestionados por Acronis Cyber Protect.

El Agente para Windows se instala junto con Agent for Exchange, Agente para SQL, Agente para Active Directory y Agent for Oracle. Si instala, por ejemplo, el Agente para SQL, también podrá realizar copias de seguridad de todo el equipo donde se haya instalado el Agente.

Algunos agentes pueden instalarse solo en equipos con roles o aplicaciones específicos. Por ejemplo, el agente para Hyper-V se instala en equipos con el rol Hyper-V, el agente para SQL en equipos que ejecutan bases de datos SQL, el agente para Exchange en equipos con el rol Mailbox de Microsoft Exchange Server y el agente para Active Directory en los controladores de dominio.

Elija un agente teniendo en cuenta los elementos que va a incluir en la copia de seguridad. En la siguiente tabla se resume la información con el fin de ayudarle a decidir.

¿Qué se va a incluir en las copias de seguridad?	¿Qué agente se debe instalar?	¿Dónde se debe realizar la instalación?	Disponibilidad del agente	
			In situ	Cloud
Equipos físicos				
Discos, volúmenes y	Agente para	En el equipo que se	+	+

archivos en equipos físicos que ejecutan Windows.	Windows	incluirá en la copia de seguridad.		
Discos, volúmenes y archivos en equipos físicos que ejecutan Linux.	Agente para Linux		+	+
Discos, volúmenes y archivos en equipos físicos que ejecutan macOS.	Agente para Mac		+	+
Aplicaciones				
Bases de datos SQL	Agente para SQL	En el equipo que ejecuta Microsoft SQL Server.	+	+
Buzones de correo y bases de datos de Exchange	Agente para Exchange	En el equipo que realiza el rol de buzón de correo de Microsoft Exchange Server.* Si solo se necesita una copia de seguridad de los buzones de correo, el agente se puede instalar en cualquier equipo con Windows que tenga acceso de red al equipo que ejecuta el rol de acceso de cliente del servidor de Microsoft Exchange.	+	+ Sin copias de seguridad de los buzones de correo
Buzones de correo de Microsoft 365	Agente para Office 365	En un equipo que ejecute Windows y esté conectado a Internet.	+	+
Equipos que ejecutan Servicios de dominio de Active Directory	Agente para Active Directory	En el controlador de dominio.	+	+
Equipos que ejecutan	Agent para	En el equipo que	+	-

Oracle Database	Oracle	ejecuta Oracle Database.		
Equipos virtuales				
Equipos virtuales VMware ESXi	Agente para VMware (Windows)	En un equipo Windows con acceso de red a vCenter Server y al almacenamiento del equipo virtual.**	+	+
	Agente para VMware (dispositivo virtual)	En el servidor ESXi.	+	+
Equipos virtuales Hyper-V	Agente para Hyper-V	En el servidor Hyper-V.	+	+
Equipos virtuales de Scale Computing HC3	Agent para Scale Computing HC3	En el servidor de Scale Computing HC3.	+	+
Equipos virtuales alojados en Windows Azure.	Ocurre lo mismo con los equipos físicos.***	En el equipo que se incluirá en la copia de seguridad.	+	+
Equipos virtuales alojados en Amazon EC2			+	+
Equipos virtuales de Citrix XenServer			+****	+
Equipos virtuales de Red Hat Virtualization (RHV/RHEV)				
Equipos virtuales basados en Kernel (KVM)				
Equipos virtuales de Oracle				
Equipos virtuales Nutanix AHV				
Dispositivos móviles				
Dispositivos móviles que	Aplicación para	En el dispositivo móvil	-	+

ejecutan Android.	dispositivos móviles de Android	que se incluirá en la copia de seguridad.		
Dispositivos móviles que ejecutan iOS	Aplicación para dispositivos móviles de iOS		-	+

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

** Si su ESXi usa un almacenamiento conectado a SAN, instale el agente en un equipo conectado al mismo SAN. El agente realizará la copia de seguridad de los equipos virtuales directamente desde el almacenamiento en vez de mediante el servidor ESXi y LAN. Para obtener instrucciones detalladas, consulte la sección "Copia de seguridad sin LAN".

*** Un equipo virtual se considera virtual si un agente externo le realiza las copias de seguridad. Si se instala un agente en el sistema invitado, la copia de seguridad y las operaciones de recuperación son iguales que con un equipo físico. No obstante, el equipo se cuenta como virtual al definir las cuotas del número de equipos en una implementación en la cloud.

****Con una licencia de Acronis Cyber Protect Advanced Virtual Host, estos equipos virtuales se consideran virtuales (se utiliza una licencia por servidor). Con una licencia de Acronis Cyber Protect Virtual Host, estos equipos virtuales se consideran físicos (se utiliza una licencia por equipo).

Otros componentes

Componente	Función	¿Dónde se debe realizar la instalación?	Disponibilidad	
			In situ	Cloud
Servidor de gestión	Management Server es el punto central para gestionar todas las copias de seguridad. Con la implementación local, se instala en la red local. Gestiona los agentes y proporciona la interfaz web a los usuarios.	En un equipo que ejecuta Windows o Linux.	+	-
Componentes para la instalación remota	Guarda paquetes de instalación de agentes en una carpeta local.	En el equipo de Windows que ejecuta el servidor de gestión.	+	-

Scan Service	Componente opcional que activa un análisis antimalware de copias de seguridad en un almacenamiento en la nube o en una carpeta local o de red. Scan Service requiere una base de datos de Microsoft SQL Server o de PostgreSQL. No es compatible con la base de datos SQLite predeterminada que utiliza el servidor de gestión.	En el equipo de Windows o Linux que ejecuta el servidor de gestión.	+	-
Bootable Media Builder	Crea dispositivos de arranque.	En un equipo que ejecuta Windows o Linux.	+	-
Herramienta de línea de comandos	Admite la interfaz de la línea de comandos con la utilidad **acrocmd**. **acrocmd** no contiene ninguna herramienta que ejecute los comandos de forma física. Solo proporciona la interfaz de la línea de comandos para los componentes de Cyber Protect: agentes y el servidor de gestión.	En un equipo que ejecuta Windows, Linux o macOS.	+	+
Acronis Cyber Protect 15 Monitor	Proporciona la interfaz gráfica de usuario al Agente para Windows y el Agente para Mac. Muestra información sobre el estado de protección del equipo en el que se instaló y permite a sus usuarios configurar las opciones de cifrado de las copias de seguridad y del	En un equipo que ejecuta Windows o macOS.	+	+

	servidor proxy. En Windows, Acronis Cyber Protect 15 Monitor requiere que el Agente para Windows esté instalado en el mismo equipo.			
Nodo de almacenamiento	Almacena copias de seguridad. Es necesario para la catalogación y la deduplicación. El nodo de almacenamiento requiere que el Agente para Windows esté instalado en el mismo equipo.	En un equipo que ejecuta Windows.	+	-
Servicio de catálogo	Realiza la catalogación de las copias de seguridad en los nodos de almacenamiento.	En un equipo que ejecuta Windows.	+	-
PXE Server	Habilita el inicio de equipos en un dispositivo de arranque a través de la red.	En un equipo que ejecuta Windows.	+	-

Uso de Acronis Cyber Protect con otras soluciones de seguridad en su entorno

Puede usar Acronis Cyber Protect con o sin otras soluciones de seguridad, como el software independiente de antivirus, en su entorno.

Sin otra solución de seguridad, puede utilizar Acronis Cyber Protect como ciberprotección integral o para la copia de seguridad y la recuperación tradicionales, en función de su licencia y de sus necesidades. Para obtener más información sobre las funciones disponibles con cada licencia, consulte «Comparación de ediciones de Acronis Cyber Protect 15 que incluyen implementaciones en la nube». Puede adaptar el ámbito de sus planes de protección habilitando solo los módulos que necesite.

Puede escoger Acronis Cyber Protect como ciberprotección integral (con protección contra virus y otro malware) aunque ya tenga otra solución de seguridad en su entorno. En tal caso, debe deshabilitar o eliminar la otra solución de seguridad para evitar conflictos.

También puede probar a incrementar su ciberprotección sin deshabilitar ni eliminar su solución de seguridad actual. Esta también es una opción, pero asegúrese de no utilizar ni el módulo de antivirus ni el de antimalware en su plan de protección. Todos los otros módulos se pueden utilizar libremente.

Limitaciones

- Para el Análisis antimalware en copias de seguridad debe instalar Scan Service al instalar Cyber Protect Management Server.
- Acceso remoto mediante cliente HTML5 solo estará disponible si Cyber Protect Management Server está instalado en un equipo Linux.

Requerimientos de software

Navegadores web compatibles

La interfaz web es compatible con los siguientes navegadores web:

- Google Chrome 29 o posterior
- Mozilla Firefox 23 o posterior
- Opera 16 o posterior
- Microsoft Edge 25 o posterior
- Safari 8 o una versión posterior que se ejecute en macOS o iOS

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

Sistemas operativos y entornos compatibles

Agentes

Agente para Windows

- Windows XP Professional SP1 (x64), SP2 (x64) y SP3 (x86).

  Nota
  Solo puede instalar el agente en equipos Windows XP con unidades formateadas en NTFS.

- Windows XP Professional SP2 (x86): compatible con una versión especial de Agente para Windows. Para conocer los detalles y las limitaciones de este soporte, consulte "Agente para Windows XP SP2" (p. 77).
- Windows XP Embedded SP3
- Windows Server 2003 SP1/2003 R2 y posteriores (ediciones Standard y Enterprise [x86, x64])

Nota
Acronis Cyber Protect requiere la actualización KB940349 de Microsoft, que ya no puede descargarse de manera independiente. Para garantizar que la funcionalidad proporcionada de forma inicial por KB940349 está disponible en su equipo, instale todas las actualizaciones disponibles para Windows Server 2003.
Para obtener más información sobre KB940349, consulte este artículo de la base de conocimientos.

- Windows Small Business Server 2003/2003 R2
- Windows Server 2008: ediciones Standard, Enterprise, Datacenter, Foundation y Web (x86, x64)
- Windows Small Business Server 2008
- Windows 7: todas las ediciones (x86, x64)

Nota
Para usar Acronis Cyber Protect con Windows 7, debe instalar las siguientes actualizaciones de Microsoft:
  - Actualizaciones de seguridad ampliadas de Windows 7 (ESU)
  - KB4474419
  - KB4490628

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

- Windows Server 2008 R2: ediciones Standard, Enterprise, Datacenter, Foundation y Web
- Windows Home Server 2011
- Windows MultiPoint Server 2010/2011/2012
- Windows Small Business Server 2011: todas las ediciones
- Windows 8/8.1: todas las ediciones (x86, x64), excepto las ediciones Windows RT
- Windows Server 2012/2012 R2: todas las ediciones
- Windows Storage Server 2003/2008/2008 R2/2012/2012 R2/2016
- Windows 10 (ediciones Home, Pro, Education, Enterprise y IoT Enterprise y LTSC, antes LTSB)
- Windows Server 2016: todas las opciones de instalación, excepto Nano Server
- Windows Server 2019: todas las opciones de instalación, excepto Nano Server
- Windows 11: todas las ediciones
- Windows Server 2022: todas las opciones de instalación, excepto Nano Server

Agente para SQL, Agent for Exchange (para copia de seguridad de bases de datos y copias de seguridad compatibles con la aplicación) y Agente para Active Directory

Cada uno de estos agentes se puede instalar en un equipo que ejecute uno de los sistemas operativos mencionados anteriormente y una versión compatible de la aplicación respectiva, con la siguiente excepción:

- Agent for SQL no es compatible con la implementación local en Windows 7 Starter y Home Edition (x86, x64)

Agent for Exchange (para la copia de seguridad de buzones de correo)

Este agente puede instalarse en un equipo con o sin Microsoft Exchange Server.

- Windows Server 2008: ediciones Standard, Enterprise, Datacenter, Foundation y Web (x86, x64)
- Windows Small Business Server 2008
- Windows 7: todas las ediciones
- Windows Server 2008 R2: ediciones Standard, Enterprise, Datacenter, Foundation y Web
- Windows MultiPoint Server 2010/2011/2012
- Windows Small Business Server 2011: todas las ediciones
- Windows 8/8.1: todas las ediciones (x86, x64), excepto las ediciones Windows RT
- Windows Server 2012/2012 R2: todas las ediciones
- Windows Storage Server 2008/2008 R2/2012/2012 R2
- Windows 10: ediciones Home, Pro, Education y Enterprise
- Windows Server 2016: todas las opciones de instalación, excepto Nano Server
- Windows Server 2019: todas las opciones de instalación, excepto Nano Server
- Windows 11: todas las ediciones
- Windows Server 2022: todas las opciones de instalación, excepto Nano Server

Agente para Office 365

- Windows Server 2008: ediciones Standard, Enterprise, Datacenter, Foundation y Web (solo x64)
- Windows Small Business Server 2008
- Windows Server 2008 R2: ediciones Standard, Enterprise, Datacenter, Foundation y Web
- Windows Home Server 2011
- Windows Small Business Server 2011: todas las ediciones
- Windows 8/8.1: todas las ediciones (solo x64), excepto las ediciones Windows RT
- Windows Server 2012/2012 R2: todas las ediciones
- Windows Storage Server 2008/2008 R2/2012/2012 R2/2016 (solo x64)

- Windows 10: ediciones Home, Pro, Education y Enterprise (solo x64)
- Windows Server 2016: todas las opciones de instalación (solo x64), excepto Nano Server
- Windows Server 2019: todas las opciones de instalación (solo x64), excepto Nano Server
- Windows 11: todas las ediciones
- Windows Server 2022: todas las opciones de instalación, excepto Nano Server

Agent para Oracle

- Windows Server 2008 R2: ediciones Standard, Enterprise, Datacenter y Web (x86, x64)
- Windows Server 2012 R2: ediciones Standard, Enterprise, Datacenter y Web (x86, x64)
- Linux: cualquier kernel y distribución compatibles con el Agente para Linux (se indican a continuación)

Agente para Linux

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

Si experimenta problemas al utilizar Acronis Cyber Protect con su combinación de distribución Linux y versión de kernel, contacte con el equipo de soporte técnico para una investigación más detallada.

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

- Red Hat Enterprise Linux 4.x, 5.x, 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*, 8.6*, 8.7*
- Ubuntu 9.10, 10.04, 10.10, 11.04, 11.10, 12.04, 12.10, 13.04, 13.10, 14.04, 14.10, 15.04, 15.10, 16.04, 16.10, 17.04, 17.10, 18.04, 18.10, 19.04, 19.10, 20.04, 20.10, 21.04, 21.10, 22.04
- Fedora 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31
- SUSE Linux Enterprise Server 10, 11, 12, 15

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

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

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

Antes de instalar el producto en un sistema que no use el gestor de paquetes RPM, como un sistema Ubuntu, necesita instalar este gestor de forma manual; por ejemplo, ejecutando el siguiente comando (como usuario raíz): `apt-get install rpm`

Si su distribución Linux no es compatible con el mecanismo D-Bus (por ejemplo, Red Hat Enterprise Linux 6.x o CentOS 6.x), Acronis Cyber Protect utilizará la ubicación predeterminada para almacenar las claves seguras porque el sistema operativo no proporciona una ubicación compatible con D-Bus.

* Solo compatible con kernel de 4.18 a 5.19

Agente para Mac

Nota
Los procesadores basados en ARM, como Apple silicon M1 y M2, son compatibles solo con el despliegue en la nube. No son compatibles con el despliegue in situ. Para obtener más información sobre las diferencias entre el despliegue en la nube y el despliegue in situ, consulte "Información general acerca de la instalación" (p. 60).

- OS X Mavericks 10.9
- OS X Yosemite 10.10
- OS X El Capitan 10.11
- macOS Sierra 10.12
- macOS High Sierra 10.13
- macOS Mojave 10.14
- macOS Catalina 10.15
- macOS Big Sur 11
- macOS Monterey 12
- macOS Ventura 13
- macOS Sonoma 14

Agente para VMware (dispositivo virtual)

Este agente se proporciona como un dispositivo virtual para ejecutarse en un servidor ESXi.

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

Agente para VMware (Windows)

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

- Los sistemas operativos de 32 bits no son compatibles.
- Windows XP, Windows Server 2003/2003 R2 y Windows Small Business Server 2003/2003 R2 no son compatibles.

Agente para Hyper-V

- Windows Server 2008 (solo x64) con el rol Hyper-V, incluido el modo de instalación de Server Core
- Windows Server 2008 R2 con el rol Hyper-V, incluido el modo de instalación de Server Core
- Microsoft Hyper-V Server 2008/2008 R2
- Windows Server 2012/2012 R2 con el rol Hyper-V, incluido el modo de instalación de Server Core
- Microsoft Hyper-V Server 2012/2012 R2
- Windows 8, 8.1 (solo x64) con Hyper-V
- Windows 10: ediciones Pro, Education y Enterprise con Hyper-V
- Windows Server 2016 con el rol Hyper-V: todas las opciones de instalación, excepto Nano Server
- Microsoft Hyper-V Server 2016
- Windows Server 2019 con el rol Hyper-V: todas las opciones de instalación, excepto Nano Server
- Microsoft Hyper-V Server 2019
- Windows Server 2022 con Hyper-V: todas las opciones de instalación, excepto Nano Server

Agent para Scale Computing HC3 (dispositivo virtual)

Este agente se entrega como dispositivo virtual implementado en un clúster de Scale Computing HC3 con la consola web de Cyber Protect. No hay ningún programa de instalación independiente para este agente.

Scale Computing Hypercore 8.8, 8.9 y 9.0

Servidor de gestión (solo para implementación local)

En Windows

- Windows 7: todas las ediciones (x86, x64)

  Nota
  Para usar Acronis Cyber Protect con Windows 7, debe instalar las siguientes actualizaciones de Microsoft:
  - Actualizaciones de seguridad ampliadas de Windows 7 (ESU)
  - KB4474419
  - KB4490628

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

- Windows Server 2008 R2: ediciones Standard, Enterprise, Datacenter y Foundation
- Windows Home Server 2011
- Windows MultiPoint Server 2010/2011/2012
- Windows Small Business Server 2011: todas las ediciones
- Windows 8/8.1: todas las ediciones (x86, x64), excepto las ediciones Windows RT
- Windows Server 2012/2012 R2: todas las ediciones
- Windows Storage Server 2008 R2/2012/2012 R2/2016
- Windows 10 (ediciones Home, Pro, Education, Enterprise y IoT Enterprise y LTSC, antes LTSB)
- Windows Server 2016: todas las opciones de instalación, excepto Nano Server
- Windows Server 2019: todas las opciones de instalación, excepto Nano Server
- Windows 11: todas las ediciones
- Windows Server 2022: todas las opciones de instalación, excepto Nano Server

En Linux

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

Si experimenta problemas al utilizar Acronis Cyber Protect con su combinación de distribución Linux y versión de kernel, contacte con el equipo de soporte técnico para una investigación más detallada.

Linux con kernel desde 2.6.9 hasta 5.19 y glibc 2.3.4 o posterior, incluidas las siguientes distribuciones x86_64.

No se admiten las distribuciones x86.

- Red Hat Enterprise Linux 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*, 8.6*, 8.7*
- Ubuntu 9.10, 10.04, 10.10, 11.04, 11.10, 12.04, 12.10, 13.04, 13.10, 14.04, 14.10, 15.04, 15.10, 16.04, 16.10, 17.04, 17.10, 18.04, 18.10, 19.04, 19.10, 20.04, 20.10, 21.04, 21.10, 22.04
- Fedora 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31
- SUSE Linux Enterprise Server 10, 11, 12, 15

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

- Debian 4.x, 5.x, 6.x, 7.0, 7.2, 7.4, 7.5, 7.6, 7.7, 8.0, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 8.11, 9.0, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6, 9.7, 9.8, 10.x, 11.x
- CentOS 5.x, 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*
- CentOS Stream 8
- Oracle Linux 5.x, 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*– tanto Unbreakable Enterprise Kernel como Red Hat Compatible Kernel
- CloudLinux 5.x, 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*
- ClearOS 5.x, 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*
- AlmaLinux 8.4*, 8.5*
- Rocky Linux 8.4*
- ALT Linux 7.0

Antes de instalar el producto en un sistema que no use el gestor de paquetes RPM, como un sistema Ubuntu, necesita instalar este gestor de forma manual; por ejemplo, ejecutando el siguiente comando (como usuario raíz): `apt-get install rpm`

Si su distribución Linux no es compatible con el mecanismo D-Bus (por ejemplo, Red Hat Enterprise Linux 6.x o CentOS 6.x), Acronis Cyber Protect utilizará la ubicación predeterminada para almacenar las claves seguras porque el sistema operativo no proporciona una ubicación compatible con D-Bus.

* Solo compatible con kernel de 4.18 a 5.19

Nodo de almacenamiento (solo para implementación local)

- Windows Server 2008: ediciones Standard, Enterprise, Datacenter y Foundation (solo x64)
- Windows Small Business Server 2008
- Windows 7: todas las ediciones (solo x64)
- Windows Server 2008 R2: ediciones Standard, Enterprise, Datacenter y Foundation

- Windows Home Server 2011
- Windows MultiPoint Server 2010/2011/2012
- Windows Small Business Server 2011: todas las ediciones
- Windows 8/8.1: todas las ediciones (solo x64), excepto las ediciones Windows RT
- Windows Server 2012/2012 R2: todas las ediciones
- Windows Storage Server 2008/2008 R2/2012/2012 R2/2016
- Windows 10 (ediciones Home, Pro, Education, Enterprise y IoT Enterprise)
- Windows Server 2016: todas las opciones de instalación, excepto Nano Server
- Windows Server 2019: todas las opciones de instalación, excepto Nano Server
- Windows Server 2022: todas las opciones de instalación, excepto Nano Server

Agente para Windows XP SP2

Agente para Windows XP SP2 admite únicamente la versión de 32 bits de Windows XP SP2.

Para proteger equipos que ejecuten Windows XP SP1 (x64), Windows XP SP2 (x64) o Windows XP SP3 (x86), use el Agente para Windows habitual.

Agente para Windows XP SP2 requiere una licencia de Acronis Cyber Backup 12.5. No se admiten claves de licencia de Acronis Cyber Protect 15.

Instalación

Agente para Windows XP SP2 requiere un espacio de disco de 550 MB, como mínimo, y una memoria RAM de, al menos, 150 MB. Mientras se realiza la copia de seguridad, este agente consume normalmente unos 350 MB de memoria. El consumo máximo puede alcanzar los 2 GB, dependiendo de la cantidad de datos que se procesen.

Agente para Windows XP SP2 se puede instalar únicamente en el equipo cuya copia de seguridad desee realizar. Para descargar el programa de instalación del agente, haga clic en el icono de la cuenta que hay en la esquina superior derecha y, a continuación, en **Descargas** > **Agente para Windows XP SP2**.

No se pueden instalar ni Cyber Protect Monitor ni Bootable Media Builder. Para descargar el archivo ISO del dispositivo de arranque, haga clic en el icono de la cuenta en la esquina superior derecha > **Descargas** > **Dispositivo de arranque**.

Actualización

Agente para Windows XP SP2 no admite la funcionalidad de actualización remota. Para actualizar el agente, descargue la nueva versión del programa de instalación y, luego, repita la instalación.

Si ha actualizado Windows XP de SP2 a SP3, desinstale Agente para Windows XP SP2 y, a continuación, instale el Agente para Windows habitual.

Limitaciones

- Solo está disponible la copia de seguridad a nivel de discos. Los archivos individuales se pueden recuperar de la copia de seguridad de un disco o volumen.
- No se admite la programación por eventos.
- No se admiten las condiciones para la ejecución de un plan de protección.
- Únicamente se admiten los siguientes destinos de copias de seguridad:
  - Almacenamiento en la cloud
  - Carpeta local
  - Carpeta de red
  - Secure Zone
- No se admite el formato de copia de seguridad **Versión 12** ni las funciones que requieren el formato de copia de seguridad **Versión 12**. En concreto, no está disponible el envío de datos físicos. La opción **Ventana de copia de seguridad y rendimiento**, si está habilitada, se aplica únicamente a la configuración de nivel verde.
- En la interfaz web, no se pueden seleccionar discos ni volúmenes individualmente para la recuperación ni asignar discos manualmente durante una recuperación. Esta funcionalidad solo está disponible para dispositivos de arranque.
- No se admite el procesamiento de datos fuera del host.
- Agente para Windows XP SP2 no puede realizar las siguientes operaciones siguientes con copias de seguridad:
  - Conversión de copias de seguridad a un equipo virtual
  - Montaje de volúmenes desde una copia de seguridad
  - Extracción de archivos desde copias de seguridad locales
  - Exportación y validación manual de una copia de seguridad.

  Puede realizar estas operaciones si usa otro agente.
- Las copias de seguridad creadas por Agente para Windows XP SP2 no se pueden ejecutar como equipo virtual.

Versiones compatibles de Microsoft SQL Server

- Microsoft SQL Server 2022
- Microsoft SQL Server 2019
- Microsoft SQL Server 2017
- Microsoft SQL Server 2016
- Microsoft SQL Server 2014
- Microsoft SQL Server 2012

Las ediciones de SQL Server Express de las versiones anteriores del servidor SQL también son compatibles.

Versiones compatibles de Microsoft Exchange Server

- Microsoft Exchange Server 2019: todas las ediciones.
- Microsoft Exchange Server 2016: todas las ediciones.
- Microsoft Exchange Server 2013: todas las ediciones, actualización acumulativa 1 (CU1) y posteriores.
- Microsoft Exchange Server 2010: todas las ediciones, todos los Service Pack. Se admite la copia de seguridad de buzón de correo y la recuperación granular desde copias de seguridad de base de datos a partir del Service Pack 1 (SP1).
- Microsoft Exchange Server 2007: todas las ediciones, todos los Service Pack. No se admite la copia de seguridad de buzón de correo y la recuperación granular desde copias de seguridad de base de datos.

Versiones de Microsoft SharePoint compatibles

Acronis Cyber Protect 15 es compatible con las siguientes versiones de Microsoft SharePoint:

- Microsoft SharePoint 2013
- Microsoft SharePoint Server 2010 SP1
- Microsoft SharePoint Foundation 2010 SP1
- Microsoft Office SharePoint Server 2007 SP2*
- Microsoft Windows SharePoint Services 3.0 SP2*

*Para utilizar SharePoint Explorer con estas versiones, es necesaria una granja de recuperación de SharePoint a la que conectar las bases de datos.

Las bases de datos o copias de seguridad desde las que se extraen los datos deben tener su origen en la misma versión de SharePoint que la versión en la que está instalado SharePoint Explorer.

Versiones de Oracle Database compatibles

- Oracle Database versión 11g, todas las ediciones
- Oracle Database versión 12c, todas las ediciones

Solo se admiten configuraciones de una instancia.

Versiones de SAP HANA compatibles

HANA 2.0 SPS 03 instalado en RHEL 7.6 que se ejecuta en un equipo físico o en un equipo virtual VMware ESXi.

Dado que SAP HANA no admite la recuperación de contenedores de bases de datos de múltiples inquilinos con el uso de instantáneas de almacenamiento, esta solución admite contenedores SAP HANA con base de datos de un solo inquilino.

Plataformas de virtualización compatibles

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

Nota
Los siguientes proveedores y versiones admitidos de hipervisor mediante el método **Copia de seguridad desde dentro de un SO huésped** se han probado específicamente. Sin embargo, incluso si ejecuta un hipervisor de un proveedor o un hipervisor con una versión que no se incluye a continuación, el método **Copia de seguridad desde dentro de un SO invitado** seguirá funcionando correctamente en todos los escenarios necesarios.

Si tiene problemas al utilizar Acronis Cyber Protect con su combinación de proveedor y versión de hipervisor, contacte con el equipo de soporte técnico para una investigación más detallada.

VMware

Plataforma	Copia de seguridad a nivel de hipervisor (sin agente)	Copia de seguridad desde dentro de un SO huésped
Versiones de VMware vSphere: 4.1, 5.0, 5.1, 5.5, 6.0, 6.5, 6.7, 7.0 y 8.0 **Ediciones de VMware vSphere:** VMware vSphere Essentials* VMware vSphere Essentials Plus* VMware vSphere Standard* VMware vSphere Advanced VMware vSphere Enterprise VMware vSphere Enterprise Plus	+	+
VMware vSphere Hypervisor (Free ESXi)**		+
VMware Server (VMware Virtual server) VMware Workstation VMware ACE VMware Player		+

* En estas ediciones, el transporte HotAdd para unidades de disco virtual es compatible en vSphere 5.0 y versiones posteriores. Es posible que las copias de seguridad se ejecuten más lentamente en la versión 4.1.

** La copia de seguridad a nivel de hipervisor no es compatible para vSphere Hypervisor porque este producto limita el acceso a la interfaz de la línea de comandos remota (RCLI) al modo de solo lectura. El agente funciona durante el periodo de evaluación de vSphere Hypervisor mientras no se introduzca ninguna clave. Una vez ingresada dicha clave, el agente deja de funcionar.

Nota
Acronis admite oficialmente cualquier actualización dentro de la versión principal de vSphere compatible.

Por ejemplo, el soporte de vSphere 8.0 incluye soporte para cualquier actualización de esta versión, a menos que indica lo contrario. Por ejemplo, la actualización 1 de vSphere 8.0 también es compatible con la versión original lanzada de vSphere 8.0.

Limitaciones

- **Equipos tolerantes a errores**
  Agente para VMware realiza una copia de seguridad de un equipo tolerante a errores, solo si la tolerancia a errores está habilitada en vSphere 6.0 o versiones posteriores. Si ha actualizado desde una versión antigua de vSphere, solo es necesario que deshabilite y habilite la tolerancia a errores para cada equipo. Si está utilizando una versión de vSphere anterior, instale un agente en el sistema operativo invitado.
- **Discos independientes y RDM**
  Agente para VMware no puede realizar copias de seguridad de discos Raw Device Mapping (RDM) en modo de compatibilidad física ni de discos independientes. El agente omite estos discos y añade las advertencias al registro. Puede evitar las advertencias al excluir los discos independientes y RDM en el modo de compatibilidad física del plan de protección. Si desea realizar la copia de seguridad de estos discos o de los datos que estos contienen, instale un agente en el sistema operativo invitado.
- **Conexión iSCSI en invitado**
  Agente para VMware no realiza copias de seguridad de volúmenes de LUN conectados mediante un iniciador iSCSI que funciona en el sistema operativo invitado. Como el hipervisor ESXi no es compatible con tales volúmenes, estos no se incluyen en las instantáneas a nivel de hipervisor y se omiten de una copia de seguridad sin emitir ningún aviso. Si desea realizar la copia de seguridad de estos volúmenes o de los datos que estos contienen, instale un agente en el sistema operativo invitado.
- **Equipos virtuales cifrados** (presentados en VMware vSphere 6.5)
  - Los equipos virtuales cifrados se incluyen en la copia de seguridad en un estado cifrado. Si el cifrado es crucial en su caso, habilite las copias de seguridad al crear un plan de protección.
  - Los equipos virtuales recuperados nunca están cifrados. Puede habilitar el cifrado manualmente una vez se haya completado la recuperación.

- Si realiza copias de seguridad de equipos virtuales cifrados, le recomendamos cifrar el equipo virtual en el que se está ejecutando Agente para VMware. En caso contrario, es posible que las operaciones realizadas con equipos cifrados sean más lentas de lo esperado. Aplique la **directiva de cifrado de equipos virtuales** al equipo del agente mediante vSphere Web Client.
- Los equipos virtuales cifrados se incluirán en la copia de seguridad mediante LAN, incluso si configura el modo de transporte SAN para el agente. El agente recurrirá al transporte NBD, pues VMware no es compatible con el transporte SAN para realizar copias de seguridad de discos virtuales cifrados.

- **Arranque seguro** (presentado en VMware vSphere 6.5)
  El arranque seguro está deshabilitado cuando una máquina virtual se ha recuperado como nueva máquina virtual. Puede habilitar el cifrado manualmente una vez se haya completado la recuperación.
- La **copia de seguridad de configuración de ESXi** no es compatible con VMware vSphere 7.0.

Microsoft

Hyper-V máquinas virtuales que se ejecutan en un clúster hiperconvergente con Storage Spaces Direct (S2D). Storage Spaces Direct también es compatible como almacenamiento de copia de seguridad.

Plataforma	Copia de seguridad a nivel de hipervisor (sin agente)	Copia de seguridad desde dentro de un SO huésped
Windows Server 2008 (x64) con Hyper-V Windows Server 2008 R2 con Hyper-V Microsoft Hyper-V Server 2008/2008 R2 Windows Server 2012/2012 R2 con Hyper-V Microsoft Hyper-V Server 2012/2012 R2 Windows 8, 8.1 (x64) con Hyper-V Windows 10 con Hyper-V Windows Server 2016 con Hyper-V: todas las opciones de instalación, excepto Nano Server Microsoft Hyper-V Server 2016 Windows Server 2019 con Hyper-V: todas las opciones de instalación, excepto Nano Server Microsoft Hyper-V Server 2019 Windows Server 2022 con Hyper-V: todas las opciones de instalación, excepto Nano Server	+	+

Plataforma	Copia de seguridad a nivel de hipervisor (sin agente)	Copia de seguridad desde dentro de un SO huésped
Microsoft Virtual PC 2004 y 2007 Windows Virtual PC		+
Microsoft Virtual Server 2005		+

Limitaciones

- **Disco de paso a través**
  Agente para Hyper-V no realiza copias de seguridad de discos de paso a través. Durante la copia de seguridad, el agente omite estos discos y añade las advertencias al registro. Puede evitar las advertencias al excluir los discos de paso a través del plan de protección. Si desea realizar la copia de seguridad de estos discos o de los datos que estos contienen, instale un agente en el sistema operativo invitado.
- **Agrupación de clústeres Hyper-V invitados**
  El agente para Hyper-V no es compatible con la copia de seguridad de los equipos virtuales de Hyper-V que son nodos de un clúster de conmutación por error de Windows Server. Una instantánea VSS al nivel del servidor puede desconectar temporalmente el disco de quórum externo del clúster. Si desea realizar la copia de seguridad de esos equipos, instale agentes en los sistemas operativos invitados.
- **Conexión iSCSI en invitado**
  Agente para Hyper-V no realiza copias de seguridad de volúmenes de LUN conectados mediante un iniciador iSCSI que funciona en el sistema operativo invitado. Como el hipervisor Hyper-V no es compatible con tales volúmenes, estos no se incluyen en las instantáneas a nivel de hipervisor y se omiten de la copia de seguridad sin emitir ningún aviso. Si desea realizar la copia de seguridad de estos volúmenes o de los datos que estos contienen, instale un agente en el sistema operativo invitado.
- **Nombres de archivos VHD/VHDX con el símbolo et (&)**
  En los servidores de Hyper-V que ejecutan Windows Server 2016 o una versión posterior, no puede hacer copias de seguridad de máquinas virtuales heredadas (versión 5.0) creadas originalmente con Hyper-V 2012 R2 o anterior si los nombres de los archivos VHD/VHDX contienen el símbolo et (&).
  Para poder hacer copias de seguridad de este tipo de equipos, vaya a Hyper-V Manager, desconecte el disco virtual correspondiente de la máquina virtual, elimine el símbolo et (&) del nombre del archivo VHD/VHDX y vuelva a conectar el disco a la máquina virtual.

Scale Computing

Plataforma	Copia de seguridad a nivel de hipervisor (sin agente)	Copia de seguridad desde dentro de un SO huésped
Scale Computing Hypercore 8.8, 8.9, 9.0, 9.1, 9.2, 9.3	+	+

Citrix

Plataforma	Copia de seguridad a nivel de hipervisor (sin agente)	Copia de seguridad desde dentro de un SO huésped
Citrix XenServer 4.1.5, 5.5, 5.6, 6.0, 6.1, 6.2, 6.5, 7.0, 7.1, 7.2, 7.3, 7.4, 7.5 y 7.6		Solo invitados completamente virtualizados (también denominados HVM). No se admiten invitados paravirtualizados (también denominados PV).

Red Hat y Linux

Plataforma	Copia de seguridad a nivel de hipervisor (sin agente)	Copia de seguridad desde dentro de un SO huésped
Red Hat Enterprise Virtualization (RHEV) 2.2, 3.0, 3.1, 3.2, 3.3, 3.4, 3.5 y 3.6 Red Hat Virtualization (RHV) 4.0, 4.1		+
Red Hat Virtualization (gestionada por oVirt) 4.2, 4.3 y 4.4 (solo disponible con el despliegue en la nube)	+	+
Equipos virtuales basados en Kernel (KVM)		+
Máquinas virtuales basadas en Kernel (KVM) gestionadas por oVirt 4.3 ejecutados en Red Hat Enterprise Linux 7.6, 7.7 o	+	+

Plataforma	Copia de seguridad a nivel de hipervisor (sin agente)	Copia de seguridad desde dentro de un SO huésped
CentOS 7.6, 7.7 (solo disponibles con el despliegue en la nube y una licencia avanzada)		
Máquinas virtuales basadas en Kernel (KVM) gestionadas por oVirt 4.4 ejecutados en Red Hat Enterprise Linux 8.x o CentOS Stream 8.x (solo disponibles con el despliegue en la nube y una licencia avanzada)	+	+
Máquinas virtuales basadas en Kernel (KVM) gestionadas por oVirt 4.5 ejecutados en Red Hat Enterprise Linux 8.x o CentOS Stream 8.x (solo disponibles con el despliegue en la nube y una licencia avanzada)	+	+

Limitaciones

Equipos Linux que contienen volúmenes lógicos (LVM)

Las siguientes operaciones no son compatibles con equipos Linux con LVM que incluya en la copia de seguridad en el modo sin agente:

- No puede seleccionar volúmenes LVM de Linux individuales como origen de la copia de seguridad, ni mediante selección directa ni a través de reglas de directivas. Puede llevar a cabo la copia de seguridad de las cargas de trabajo de dichos volúmenes. Para ello seleccione **Todo el equipo** en **Qué incorporar en la copia de seguridad**.
- Los filtros de archivo (inclusiones y exclusiones) no son aplicables. Se ignorarán las inclusiones o exclusiones configuradas. Para obtener más información sobre los filtros de archivo, consulte "Filtros de archivo" (p. 325).

Las siguientes operaciones no son compatibles con equipos Linux con LVM que incluya en la copia de seguridad en el modo basado en agente (es decir, por Agente para Linux instalado en el equipo del que se hace la copia de seguridad):

- Llevar a cabo una migración del equipo mediante la recuperación de su copia de seguridad como una máquina virtual (por ejemplo, por Agente para VMware, Agente para Hyper-V, Agente para Virtuozzo, Agente para la Virtuozzo Hybrid Infrastructure o Agente para Scale Computing para la migración P2V, V2P o V2V). Para recuperar datos desde una copia de seguridad, utilice un dispositivo de arranque.

  Para obtener más información sobre los escenarios de las migraciones, consulte "Migración de equipos" (p. 567).

- Ejecución de un equipo virtual desde una copia de seguridad creada por Agente para Linux o un dispositivo de arranque.

Parallels

Plataforma	Copia de seguridad a nivel de hipervisor (sin agente)	Copia de seguridad desde dentro de un SO huésped
Parallels Workstation		+
Parallels Server 4 Bare Metal		+

Oracle

Plataforma	Copia de seguridad a nivel de hipervisor (sin agente)	Copia de seguridad desde dentro de un SO huésped
Oracle VM Server 3.0, 3.3 y 3.4		Solo invitados completamente virtualizados (también denominados HVM). No se admiten invitados paravirtualizados (también denominados PV).
Oracle VM VirtualBox 4.x		+

Nutanix

Plataforma	Copia de seguridad a nivel de hipervisor (sin agente)	Copia de seguridad desde dentro de un SO huésped
Nutanix Acropolis Hypervisor (AHV) 20160925.x mediante 20180425.x		+

Virtuozzo (solo disponible con el despliegue en la nube)

Plataforma	Copia de seguridad a nivel de hipervisor (sin agente)	Copia de seguridad desde dentro de un SO huésped
Virtuozzo 6.0.10, 6.0.11, 6.0.12	+	Solo equipos virtuales. No se admiten contenedores.
Virtuozzo 7.0.13, 7.0.14	Solo contenedores ploop. No se admiten equipos virtuales.	Solo equipos virtuales. No se admiten contenedores.
Virtuozzo Hybrid Server 7.5	+	Solo equipos virtuales. No se admiten contenedores.

Limitaciones

Equipos Linux que contienen volúmenes lógicos (LVM)

Las siguientes operaciones no son compatibles con equipos Linux con LVM que incluya en la copia de seguridad en el modo sin agente:

- No puede seleccionar volúmenes LVM de Linux individuales como origen de la copia de seguridad, ni mediante selección directa ni a través de reglas de directivas. Puede llevar a cabo la copia de seguridad de las cargas de trabajo de dichos volúmenes. Para ello seleccione **Todo el equipo** en **Qué incorporar en la copia de seguridad**.
- Los filtros de archivo (inclusiones y exclusiones) no son aplicables. Se ignorarán las inclusiones o exclusiones configuradas. Para obtener más información sobre los filtros de archivo, consulte "Filtros de archivo" (p. 325).

Las siguientes operaciones no son compatibles con equipos Linux con LVM que incluya en la copia de seguridad en el modo basado en agente (es decir, por Agente para Linux instalado en el equipo del que se hace la copia de seguridad):

- Llevar a cabo una migración del equipo mediante la recuperación de su copia de seguridad como una máquina virtual (por ejemplo, por Agente para VMware, Agente para Hyper-V, Agente para Virtuozzo, Agente para la Virtuozzo Hybrid Infrastructure o Agente para Scale Computing para la migración P2V, V2P o V2V). Para recuperar datos desde una copia de seguridad, utilice un dispositivo de arranque.

Para obtener más información sobre los escenarios de las migraciones, consulte "Migración de equipos" (p. 567).

- Ejecución de un equipo virtual desde una copia de seguridad creada por Agente para Linux o un dispositivo de arranque.

Virtuozzo Hybrid Infrastructure (solo disponible con el despliegue en la nube)

Plataforma	Copia de seguridad a nivel de hipervisor (sin agente)	Copia de seguridad desde dentro de un SO huésped
Virtuozzo Hybrid Infrastructure 3.5, 4.0 y 4.5	+	+

Limitaciones

Equipos Linux que contienen volúmenes lógicos (LVM)

Las siguientes operaciones no son compatibles con equipos Linux con LVM que incluya en la copia de seguridad en el modo sin agente:

- No puede seleccionar volúmenes LVM de Linux individuales como origen de la copia de seguridad, ni mediante selección directa ni a través de reglas de directivas. Puede llevar a cabo la copia de seguridad de las cargas de trabajo de dichos volúmenes. Para ello seleccione **Todo el equipo** en **Qué incorporar en la copia de seguridad**.
- Los filtros de archivo (inclusiones y exclusiones) no son aplicables. Se ignorarán las inclusiones o exclusiones configuradas. Para obtener más información sobre los filtros de archivo, consulte "Filtros de archivo" (p. 325).

Las siguientes operaciones no son compatibles con equipos Linux con LVM que incluya en la copia de seguridad en el modo basado en agente (es decir, por Agente para Linux instalado en el equipo del que se hace la copia de seguridad):

- Llevar a cabo una migración del equipo mediante la recuperación de su copia de seguridad como una máquina virtual (por ejemplo, por Agente para VMware, Agente para Hyper-V, Agente para Virtuozzo, Agente para la Virtuozzo Hybrid Infrastructure o Agente para Scale Computing para la migración P2V, V2P o V2V). Para recuperar datos desde una copia de seguridad, utilice un dispositivo de arranque.
  Para obtener más información sobre los escenarios de las migraciones, consulte "Migración de equipos" (p. 567).
- Ejecución de un equipo virtual desde una copia de seguridad creada por Agente para Linux o un dispositivo de arranque.

Amazon

Plataforma	Copia de seguridad a nivel de hipervisor (sin agente)	Copia de seguridad desde dentro de un SO huésped
Instancias de Amazon EC2		+

Microsoft Azure

Plataforma	Copia de seguridad a nivel de hipervisor (sin agente)	Copia de seguridad desde dentro de un SO huésped
Equipos virtuales de Azure		+

Paquetes de Linux

Para agregar los módulos necesarios al kernel de Linux, el programa de instalación necesita los siguientes paquetes de Linux:

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

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

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

¿Los paquetes requeridos ya están instalados?

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

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

```
cat /proc/version
```

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

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

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

Para **gcc**, asegúrese de que la versión que el comando devuelva sea la misma que en la `gcc version` del paso 1. Para **hacerlo**, solo tiene que asegurarse de que el comando funcione.

3. Verifique si está instalada la versión apropiada de los paquetes para compilar los módulos de kernel:
   - En Red Hat Enterprise Linux, CentOS y Fedora, ejecute el siguiente comando:

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

   - En Ubuntu, ejecute los siguientes comandos:

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

En cualquier caso, asegúrese de que las versiones del paquete sean las mismas que en la `Linux version` del paso 1.

4. Ejecute el siguiente comando para verificar si el interpretador Perl está instalado:

```
perl --version
```

Si ve información sobre la versión Perl, el interpretador está instalado.

5. En Red Hat Enterprise Linux, CentOS y Fedora, ejecute el siguiente comando para comprobar si `elfutils-libelf-devel` está instalado:

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

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

Instalación de los paquetes del repositorio

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

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

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

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

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

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

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

Instalación manual de los paquetes

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

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

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

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

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

- En Ubuntu, ejecute el siguiente comando:

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

Ejemplo: Instalación manual de los paquetes en Fedora 14

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

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

   ```
   cat /proc/version
   ```

   El resultado de este comando incluye lo siguiente:

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

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

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

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

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

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

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

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

Compatibilidad con software de cifrado

No hay limitaciones en cuanto a las copias de seguridad y la recuperación de los datos que se hayan cifrado con el software de cifrado a *nivel de archivos*.

El software de cifrado a *nivel del disco* cifra los datos simultáneamente. Esta es la razón por la que los datos en la copia de seguridad no están cifrados. El software de cifrado a nivel del disco generalmente modifica áreas del sistema: registros de inicio, tablas de partición o tablas del sistema de archivos. Estos factores afectan a la copia de seguridad y recuperación a nivel del disco y la capacidad de un sistema de iniciar y acceder a Secure Zone.

Puede realizar una copia de seguridad de los datos cifrados con el software de cifrado a nivel del disco siguiente:

- Microsoft BitLocker Drive Encryption
- CheckPoint Harmony Endpoint
- McAfee Endpoint Encryption
- PGP Whole Disk Encryption

Para garantizar la fiabilidad de la recuperación a nivel del disco, siga las reglas comunes y las recomendaciones específicas del software.

Regla común de instalación

Es altamente recomendable instalar el software de cifrado antes que los agentes de protección.

Cómo utilizar Secure Zone

Secure Zone no debe estar cifrada con el cifrado a nivel del disco. Esta es la única forma de utilizar Secure Zone:

1. Instale el software de cifrado.
2. Instale el agente de protección.
3. Cree Secure Zone.
4. Excluya Secure Zone al cifrar el disco o sus volúmenes.

Regla común de copia de seguridad

Puede llevar a cabo una copia de seguridad a nivel del disco en el sistema operativo. No intente realizar la copia de seguridad con un dispositivo de arranque.

Procedimientos de recuperación específicos del software

Microsoft BitLocker Drive Encryption y CheckPoint Harmony Endpoint

Puede recuperar un sistema mediante el uso de una recuperación con reinicio o un soporte de arranque.

Recuperación con reinicio

Para recuperar un sistema cifrado, siga los pasos en "Recuperación en un equipo físico" (p. 364).

Asegúrese de que se cumplen los requisitos disponibles en "Recuperación con reinicio" (p. 371).

Nota
Para los volúmenes cifrados de Bitlocker, la recuperación con reinicio solo está disponible para los equipos basados en UEFI que ejecutan Windows 7 y versiones posteriores o Windows Server 2008 R2 y versiones posteriores. Para los volúmenes cifrados de CheckPoint, la recuperación con reinicio solo está disponible para los equipos basados en UEFI que ejecutan Windows 10 y Windows 11.

La recuperación con reinicio no está disponible en equipos basados en BIOS o equipos que ejecutan Linux o macOS.

Recuperación con soportes de arranque

1. Inicie desde el dispositivo de arranque.
2. Recupere el sistema.

   Importante
   Los datos de la copia de seguridad se recuperan sin cifrar.

3. Reinicie el sistema recuperado.
4. Encienda el software de cifrado.

Si necesita recuperar solo una partición de un disco con múltiples particiones, lleve a cabo la recuperación en el sistema operativo. La recuperación en el dispositivo de arranque puede hacer que Windows no detecte la partición recuperada.

McAfee Endpoint Encryption y PGP Whole Disk Encryption

Solo puede recuperar una partición del sistema cifrado mediante el soporte de arranque.

Si el sistema recuperado no inicia, vuelva a crear el registro de arranque maestro según se describe en el siguiente artículo de la Microsoft Knowledge Base: https://support.microsoft.com/kb/2622803

Compatibilidad con almacenamientos Dell EMC Data Domain

Con Acronis Cyber Protect, puede utilizar dispositivos Dell EMC Data Domain como almacenamiento de copia de seguridad. Es compatible con el bloqueo de retención (modo de gobierno).

Si se habilita el bloque de retención, debe añadir la variable de entorno `AR_RETENTION_LOCK_SUPPORT` al equipo con el agente de protección que utilice este almacenamiento como destino de copias de seguridad.

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

Para añadir la variable en Windows

1. Inicie sesión como administrador en el equipo con el agente de protección.
2. En el **Panel de control**, vaya a **Sistema y seguridad** > **Sistema** > **Configuración avanzada del sistema**.
3. En la **pestaña Opciones avanzadas**, haga clic en **Variables de entorno**.
4. En el panel **Variables del sistema**, haga clic en **Nueva**.
5. En la ventana **Nueva variable del sistema**, añada la nueva variable tal como se indica:
   - Nombre de la variable: `AR_RETENTION_LOCK_SUPPORT`
   - Valor de la variable: `1`
6. Haga clic en **Aceptar**.
7. En la ventana **Variables de entorno**, haga clic en **Aceptar**.
8. Reinicie el equipo.

Para añadir la variable en Linux

1. Inicie sesión como administrador en el equipo con el agente de protección.
2. Vaya al directorio `/sbin` y abra el archivo `acronis_mms` para su edición.
3. Encima de la línea `export LD_LIBRARY_PATH`, añada la línea siguiente:

   ```
   export AR_RETENTION_LOCK_SUPPORT=1
   ```

4. Guarde el archivo `acronis_mms`.
5. Reinicie el equipo.

Para añadir la variable en un dispositivo virtual

1. Inicie sesión como administrador en el equipo del dispositivo virtual.
2. Vaya al directorio `/bin` y abra el archivo `autostart` para su edición.
3. Debajo de la línea `export LD_LIBRARY_PATH`, añada la línea siguiente:

   ```
   export AR_RETENTION_LOCK_SUPPORT=1
   ```

4. Guarde el archivo `autostart`.
5. Reinicie el equipo del dispositivo virtual.

Requisitos del sistema

La tabla siguiente resume los requisitos en cuanto a espacio de disco y memoria para casos de instalación normales. La instalación se realiza con la configuración predeterminada.

Componentes que se deben instalar	Espacio de disco necesario	Consumo de memoria mínimo

	para la instalación	
Agente para Windows	850 MB	150 MB
Agente para Windows y uno de los agentes siguientes: • Agente para SQL • Agente para Exchange	950 MB	170 MB
Agente para Windows y uno de los agentes siguientes: • Agente para VMware (Windows) • Agente para Hyper-V	1170 MB	180 MB
Agente para Office 365	500 MB	170 MB
Agente para Linux	2,0 GB	130 MB
Agente para Mac	500 MB	150 MB
Solo para implementaciones locales		
Servidor de gestión en Windows	1,7 GB	200 MB
Servidor de gestión en Linux	1,5 GB	200 MB
Servidor de gestión y Agente para Windows	2,4 GB	360 MB
Servidor de gestión y agentes en un equipo que ejecute Windows, Microsoft SQL Server, Microsoft Exchange Server y servicios de dominio de Active Directory	3,35 GB	400 MB
Servidor de gestión y Agente para Linux	4,0 GB	340 MB
Nodo de almacenamiento y Agente para Windows • Solo en una plataforma de 64 bits. • Para utilizar la deduplicación, se necesitan 8 GB como mínimo. Para obtener más información, consulte "Mejores prácticas de deduplicación" (p. 692).	1,1 GB	330 MB

Mientras se realiza la copia de seguridad, un agente consume normalmente unos 350 MB de memoria (medidos durante una copia de seguridad de volumen de 500 GB). El consumo máximo puede alcanzar los 2 GB, dependiendo de la cantidad y del tipo de datos que se procesen.

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

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

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

Un servidor de gestión con una carga de trabajo registrado consume 200 MB de memoria. Una carga de trabajo es cualquier tipo de recurso protegido, por ejemplo, un equipo físico, una máquina virtual, un buzón de correo o una instancia de la base de datos. Cada carga de trabajo adicional añade unos 2 MB. Por tanto, un servidor con 100 cargas de trabajo registradas consume aproximadamente 400 MB aparte del sistema operativo y las aplicaciones en funcionamiento.

El número máximo de cargas de trabajo registradas está entre 900 y 1000. Esta limitación procede de la base de datos SQLite integrada del servidor de gestión.

Para superar esta limitación, especifique una instancia de Microsoft SQL Server externa cuando instale el servidor de gestión. Con una base de datos SQL externa, se pueden registrar hasta 8000 cargas de trabajo en el servidor de gestión sin ninguna degradación significativa del rendimiento. Con 8000 cargas de trabajo registradas, la instancia del servidor SQL consumirá unos 8 GB de RAM.

Para disfrutar de un mayor rendimiento de copia de seguridad, gestione las cargas de trabajo por grupos, formados por hasta 500 cargas de seguridad en cada uno.

Sistemas de archivos compatibles

Un agente de protección puede realizar una copia de seguridad de cualquier sistema de archivos que sea accesible desde el sistema operativo en el que el agente está instalado. Por ejemplo, Agente para Windows puede realizar una copia de seguridad y recuperar un sistema de archivos ext4 si el controlador pertinente está instalado en Windows.

En la tabla siguiente se resumen los sistemas de archivos de los que se puede realizar una copia de seguridad y recuperar. Las limitaciones se aplican tanto a los agentes como a los dispositivos de arranque.

Sistema de archivos	Compatibilidad con				Limitaciones
	Agentes	Dispositivo de arranque de WinPE	Dispositivos de arranque basados en Linux	Dispositivos de arranque para Mac	

FAT16/32	Todos los agentes	+	+	+	Sin limitaciones
NTFS		+	+	+	
ext2/ext3/ext4		+	+	-	
HFS+	Agente para Mac	-	-	+	
APFS		-	-	+	• Compatible a partir de macOS High Sierra 10.13 • La configuración del disco deberá volver a crearse manualmente cuando se recupera a un equipo no original o en una recuperación completa.
JFS	Agente para Linux	-	+	-	• Los archivos no se pueden excluir de una copia de seguridad del disco • No es posible habilitar la copia de seguridad diferencial incremental rápida
ReiserFS3		-	+	-	

ReiserFS4		-	+	-	• Los archivos no se pueden excluir de una copia de seguridad del disco • No es posible habilitar la copia de seguridad diferencial incremental rápida • No se puede cambiar el tamaño de los volúmenes durante la recuperación
ReFS	Todos los agentes	+	+	+	
XFS		+	+	+	• Los archivos no se pueden excluir de una copia de seguridad del disco • No es posible habilitar la copia de seguridad diferencial incremental rápida • No se puede cambiar el tamaño de los volúmenes durante la recuperación • No es compatible la recuperación de archivos a partir de una copia de seguridad

					almacenada en una cinta.
Linux swap	Agente para Linux	-	+	-	Sin limitaciones
exFAT	Todos los agentes	+	+ El dispositivo de arranque no se pueda usar para llevar a cabo la recuperación si la copia de seguridad *se almacena en* exFAT	+	• Solo son compatibles las copias de seguridad de disco o volumen • No se pueden excluir archivos de una copia de seguridad • No se pueden recuperar archivos individuales desde una copia de seguridad

El software cambia automáticamente al modo sector por sector al hacer copias de seguridad de unidades con sistemas de archivos no reconocidos o incompatibles. Es posible realizar una copia de seguridad sector por sector para cualquier sistema de archivos que:

- esté basado en bloques;
- abarque un único disco;
- tenga un esquema de partición MBR/GPT estándar;

Si el sistema de archivos no cumple estos requisitos, la copia de seguridad fallará.

Deduplicación de datos

En Windows Server 2012 y versiones posteriores, se puede activar la característica Deduplicación de datos para un volumen NTFS. La deduplicación de datos reduce el espacio utilizado en el volumen, ya que guarda una sola vez los fragmentos duplicados de los archivos del volumen.

Puede recuperar y realizar una copia de seguridad de un volumen donde esté activada la deduplicación de datos a nivel de discos sin ninguna limitación. Está permitido hacer copias de seguridad a nivel de archivo excepto al usar Acronis VSS Provider. Para recuperar archivos a partir de una copia de seguridad del disco, ejecute un equipo virtual desde su copia de seguridad o monte la copia de seguridad en un equipo que ejecute Windows Server 2012 o una versión posterior, y luego copie los archivos desde el volumen montado.

La característica Deduplicación de datos de Windows Server no está relacionada con la característica Deduplicación de Acronis Backup.

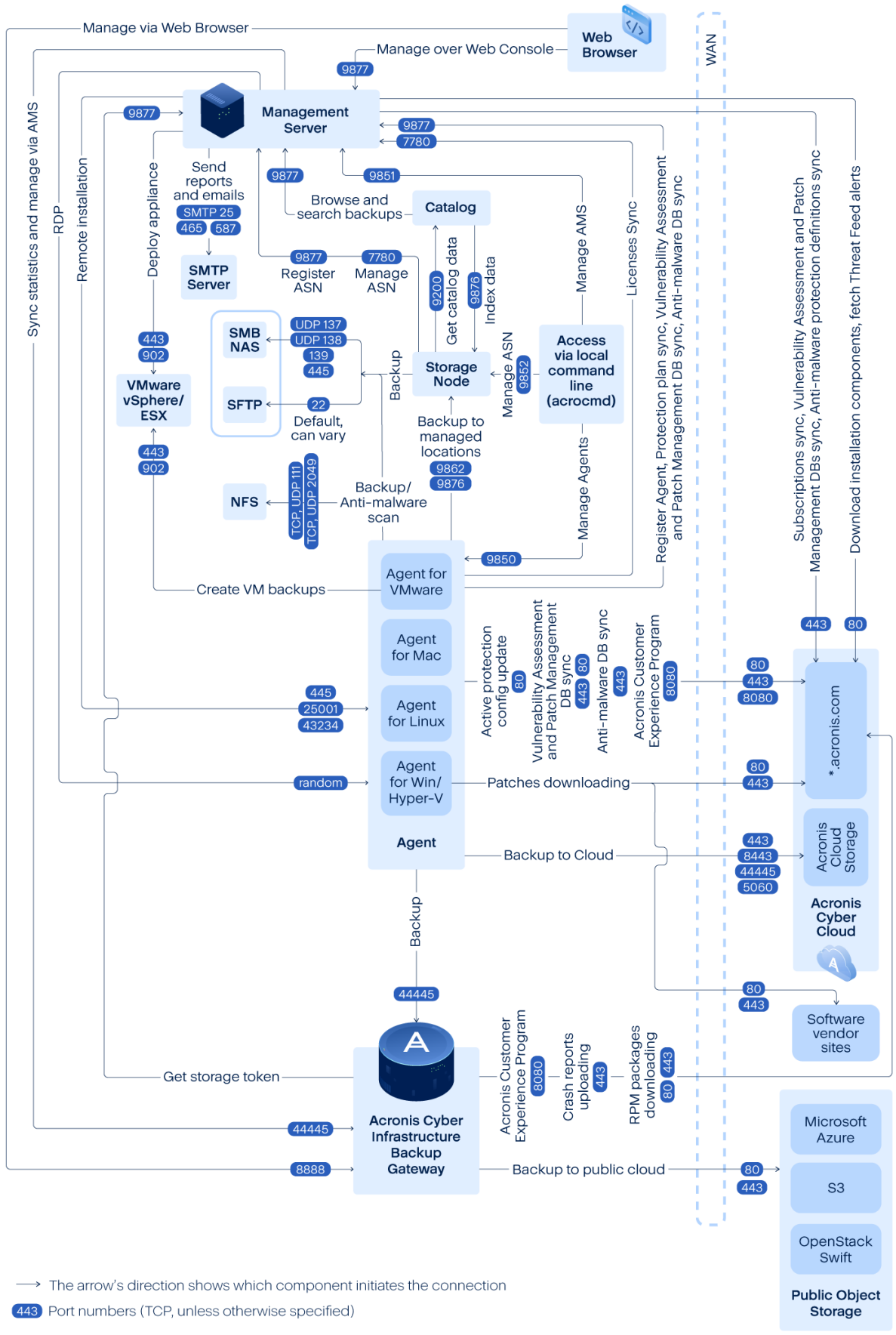
Diagrama de conexión de red para Acronis Cyber Protect

Este tema contiene los diagramas de conexión para Acronis Cyber Protect.

Visite nuestra Base de conocimientos para ver una lista de los puertos, servicios y procesos que utiliza Acronis Cyber Protect:

- En Windows, consulte Servicios y procesos de Windows (65663).
- En Linux, consulte Componentes, servicios y procesos de Linux (67276).

Diagrama de conexión de red: procesos de Cyber Protect



Importante
Los puertos de salida del diagrama de red son dinámicos. Algunos servicios también pueden utilizar puertos dinámicos para las conexiones de entrada. Para solucionar problemas de red, asegúrese de que se permite el tráfico a través de puertos dinámicos.

Los puertos dinámicos los gestiona el sistema operativo y se asignan de manera aleatoria. El rango de puertos dinámicos predeterminado en Windows es 49152 – 65535. Este rango puede variar según el sistema operativo y puede cambiarse manualmente.

El servidor de gestión es el componente central de Acronis Cyber Protect. Expone dos puertos TCP: 7780 y 9877. El puerto 9877, protegido con TLS, se utiliza para proporcionar la API REST y una interfaz de usuario basada en web. Los endpoints de la API REST autentican las solicitudes utilizando tokens de JWT representados como un encabezado HTTP individual o cifrados como una cookie HTTP. El puerto 7780 implementa el protocolo ZeroMQ con la autenticación y el cifrado ZMTP CURVE. Los agentes y el nodo de almacenamiento utilizan el puerto 7780 para intercambiar mensajes de gestión con el servidor de gestión de forma asíncrona. El servidor de gestión también se comunica con los servicios de la nube para descargar actualizaciones de los puertos HTTP y HTTPS estándar.

El **nodo de almacenamiento** es el componente de almacenamiento de Acronis Cyber Protect. Expone el puerto TCP 9876. Este puerto se utiliza para enviar y recibir datos de la copia de seguridad. El transporte se protege con TLS y la autenticación se lleva a cabo con TLS mutuo. El protocolo a nivel de aplicación es propiedad de Acronis. El nodo de almacenamiento se comunica con los sistemas de almacenamiento backend a través de los protocolos y los mecanismos de autenticación adecuados.

El **catálogo** es un componente secundario de Acronis Cyber Protect. Indexa datos en el nodo de almacenamiento mediante al acceso a través del puerto 9876 y expone el índice en el puerto 9200.

La **puerta de enlace de la copia de seguridad** implementa la próxima generación del protocolo de acceso a datos propiedad de Acronis. Si el cliente opta por la copia de seguridad en la nube, se utiliza el mismo componente en Acronis Cyber Cloud. La puerta de enlace utiliza el puerto TCP 44445, registrado en IANA. La protección de datos se lleva a cabo a través de TLS y la autenticación se lleva a cabo con TLS mutuo. Es posible que la puerta de enlace de la copia de seguridad también utilice el puerto 8888 para el servicio de gestión basado en HTTPS.

El **agente** se comunica con el servidor de gestión, el nodo de almacenamiento y la puerta de enlace de la copia de seguridad a través de los puertos, según se describe más arriba. Es posible que el agente también se comunique con los servicios de archivos basados en estándares (SMB, NFS) cuando se utilicen como destino de copia de seguridad. En este caso, se utilizan puertos estándar y protocolos de autenticación adecuados. El agente para VMware utiliza la API de VMware vSphere en los puertos definidos por VMware vSphere cuando se configura esa funcionalidad.

La evaluación de vulnerabilidades para Linux se implementa mediante un servicio CVSS desplegado en Acronis Cyber Cloud. Los agentes de protección escogen dinámicamente el centro de datos más cercano haciendo ping en la lista https://cloud.acronis.com/servicio.json.

Implementación local

Una implementación local incluye varios componentes de software, que se describen en la sección "Componentes" (p. 63). Para obtener detalles sobre la interacción entre esos componentes y los puertos requeridos, consulte "Diagrama de conexión de red para Acronis Cyber Protect" (p. 101).

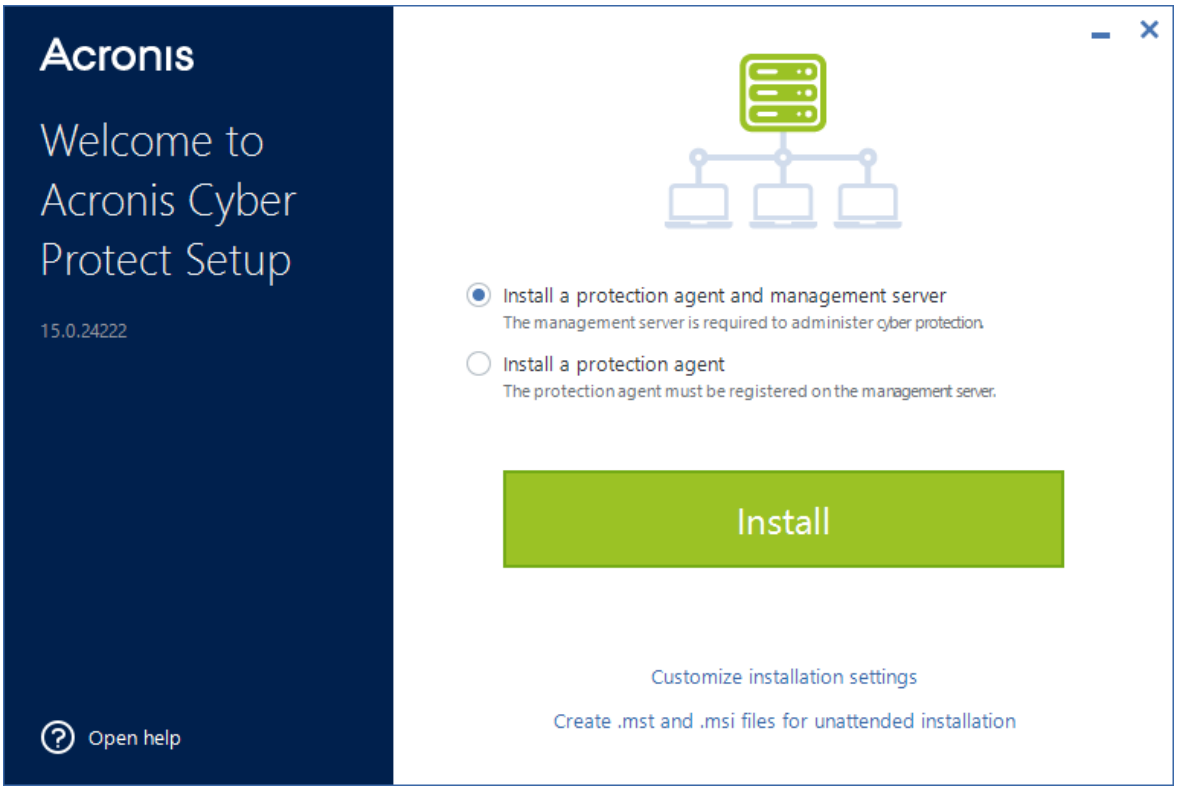
Instalación del servidor de gestión

Instale el servidor de administración solo en los equipos en los que el modo de suspensión y la hibernación estén desactivados.

Instalación en Windows

Para instalar el servidor de gestión

1. Inicie sesión como administrador e inicie el programa de instalación de Acronis Cyber Protect.
2. [Opcional] Para cambiar el idioma del programa de instalación, haga clic en **Idioma de instalación**.
3. Acepte los términos del acuerdo de licencia y la declaración de privacidad y, a continuación, haga clic en **Siguiente**.
4. Mantenga la configuración predeterminada **Instalar un agente de protección y servidor de gestión**.



5. Realice una de las siguientes operaciones:

- Haga clic en **Instalar**.

  Esta es la forma más sencilla de instalar el producto. La mayoría de los parámetros de instalación se establecerán en sus valores predeterminados.

  Se instalarán los componentes siguientes:

  - Servidor de gestión
  - Componentes para la instalación remota
  - Agente para Windows
  - Otros agentes (Agente para Hyper-V, Agent for Exchange, Agente para SQL y Agente para Active Directory), si se detecta el respectivo hipervisor o aplicación en el equipo
  - Bootable Media Builder
  - Herramienta de línea de comandos
  - Cyber Protect Monitor
- Haga clic en **Personalizar los ajustes de instalación** para realizar la configuración.

  Podrá seleccionar los componentes que desea instalar y especificar parámetros adicionales. Para obtener más información, consulte "Personalización de los ajustes de instalación" (p. 106).
- Haga clic en **Crear archivos .mst y .msi para una instalación sin supervisión** para extraer los paquetes de instalación. Compruebe o modifique la configuración de instalación que se añadirá al archivo .mst y haga clic en **Generar**. No se requieren más pasos para este procedimiento.

  Si desea implementar agentes mediante una directiva de grupo, consulte "Implementación de agentes mediante la directiva de grupo" (p. 220).

6. Continúe con la instalación.
7. Cuando haya terminado la instalación, haga clic en **Cerrar**.

Para empezar a usar el servidor de gestión, actívelo iniciando sesión en su cuenta de Acronis o mediante el archivo de activación.

Personalización de los ajustes de instalación

En esta sección se describen los ajustes que pueden modificarse durante la instalación.

Componentes para instalar

En función de si instala un servidor de gestión y un agente de protección o solo un agente de protección, los siguientes componentes estarán seleccionados de forma predeterminada:

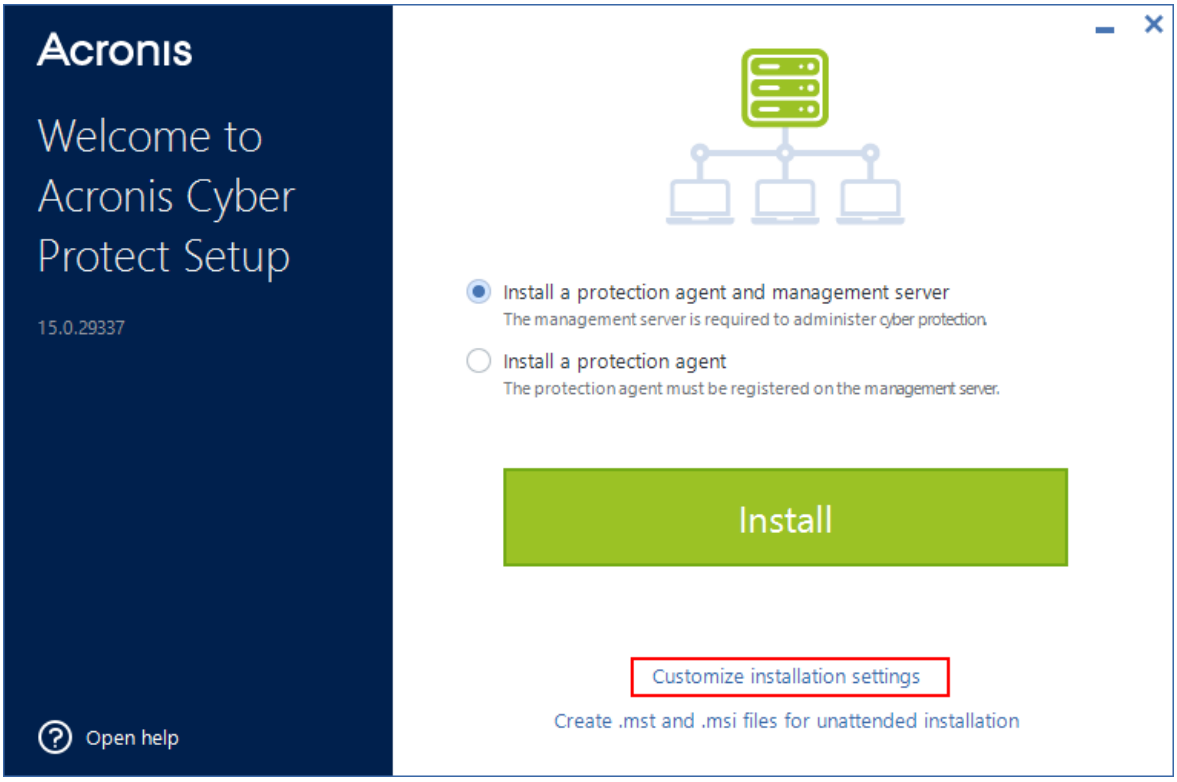
Servidor de gestión y agente de protección	Solo agente de protección
Servidor de gestión	Agente para Windows
Componentes para la instalación remota	Bootable Media Builder

Servidor de gestión y agente de protección	Solo agente de protección
Agente para Windows	Herramienta de línea de comandos
Bootable Media Builder	Cyber Protect Monitor
Herramienta de línea de comandos	
Cyber Protect Monitor	

Para ver la lista completa de los componentes disponibles, consulte "Componentes" (p. 63).

Instalar componentes opcionales

1. En el asistente de instalación, haga clic en **Personalizar configuración de la instalación**.



2. En **Qué instalar**, haga clic en **Cambiar**.
3. Seleccione los componentes que desee y, a continuación, haga clic en **Listo**.
4. Si se le solicita, configure los ajustes de los componentes seleccionados.
5. Haga clic en **Instalar**.

Cuenta de inicio de sesión en el servicio

Puede cambiar la cuenta con la que se ejecuta el agente o el servidor de gestión mediante las opciones **Cuenta de inicio de sesión para el servicio de agente** y **Cuenta de inicio de sesión para el servicio de servidor de gestión**, respectivamente.

Puede escoger una de las siguientes opciones:

- **Usar cuentas de usuario del servicio** (opción predeterminada para el servicio de agente)

  Las **cuentas de usuario del servicio** son cuentas de sistema de Windows que se utilizan para ejecutar servicios. La ventaja de esta opción es que las directivas de seguridad de dominios no afectan a los derechos de usuario de estas cuentas. De forma predeterminada, el agente se ejecuta desde la cuenta **Sistema local**.
- **Crear una cuenta nueva** (opción predeterminada para el servicio de servidor de gestión y servicio de nodo de almacenamiento)

  Los nombres de cuenta son **Acronis Agent User**, **AMS User** y **ASN User** para los servicios de agente, servidor de gestión y nodo de almacenamiento, respectivamente.
- **Utilice la siguiente cuenta**

  Si instala el producto en un controlador de dominios, el programa de instalación le pedirá que especifique las cuentas actuales (o una misma cuenta) para cada servicio. Por razones de seguridad, el programa de instalación no crea automáticamente nuevas cuentas en un controlador de dominio.

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

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

  Además, la selección de **Utilice la siguiente cuenta** le permite utilizar la autenticación de Windows para Microsoft SQL Server si configura el servidor de gestión con una base de datos SQL.

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

Derechos de usuario necesarios para la cuenta de inicio de sesión del servicio

Los agentes de protección se ejecutan en un **Managed Machine Service** (MMS) de un equipo Windows. La cuenta con la que se ejecuta el agente debe tener los siguientes derechos para que el agente funcione correctamente:

1. El usuario MMS debe incluirse en los grupos **Operadores de copia de seguridad** y **Administradores**. En un controlador de dominio, el usuario debe incluirse en el grupo **Administradores del dominio**.
2. El usuario MMS debe contar con los permisos de **Control total** sobre la carpeta `%PROGRAMDATA%\Acronis` (en Windows XP y en Server 2003, `%ALLUSERSPROFILE%\Application Data\Acronis`) y en sus subcarpetas.

3. El usuario MMS debe contar con permiso de **Control total** en las claves de registro en la siguiente clave: `HKEY_LOCAL_MACHINE\SOFTWARE\Acronis`.
4. El usuario MMS debe tener asignados los siguientes derechos de usuario en Windows:
   - **Inicio de sesión como un servicio**
   - **Ajustar cantidades máximas de memoria para un proceso**
   - **Reemplazar símbolo de nivel de un proceso**
   - **Modificar los valores del entorno de firmware**

El **usuario ASN** debe tener derechos de administrador local en el equipo en el que está instalado el Nodo de almacenamiento de Acronis.

Asignar derechos de usuario en Windows

Nota
Este procedimiento utiliza como ejemplo el derecho **Iniciar como derecho de usuario del servicio**. Los pasos para los demás derechos de usuario son los mismos.

1. Inicie sesión en el equipo como administrador.
2. En el **Panel de control**, abra **Herramientas administrativas**. También puede pulsar Win+R en el teclado, escribir **control admintools** y, a continuación, pulsar Intro.
3. Abra **Directiva de seguridad local**.
4. Amplíe **Directivas locales** y haga clic en **Asignación de derechos de usuario**.
5. En el panel de la derecha, haga clic en **Inicio de sesión como un servicio** y seleccione **Propiedades**.
6. Haga clic en **Añadir usuario o grupo...** para agregar un nuevo usuario.
7. En la ventana **Seleccionar usuarios o grupos**, busque al usuario que quiere agregar y haga clic en **Aceptar**.
8. Haga clic en **Aceptar** en la ventana **Inicio de sesión como un servicio** para guardar los cambios.

Nota
El usuario que se agrega al derecho de usuario **Inicio de sesión como un servicio** no puede estar incluido en la directiva **Rechazar inicio de sesión como servicio** en **Directiva de seguridad local**.

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

Base de datos para el servidor de gestión

Puede configurar el servidor de gestión con las siguientes bases de datos:

- SQLite

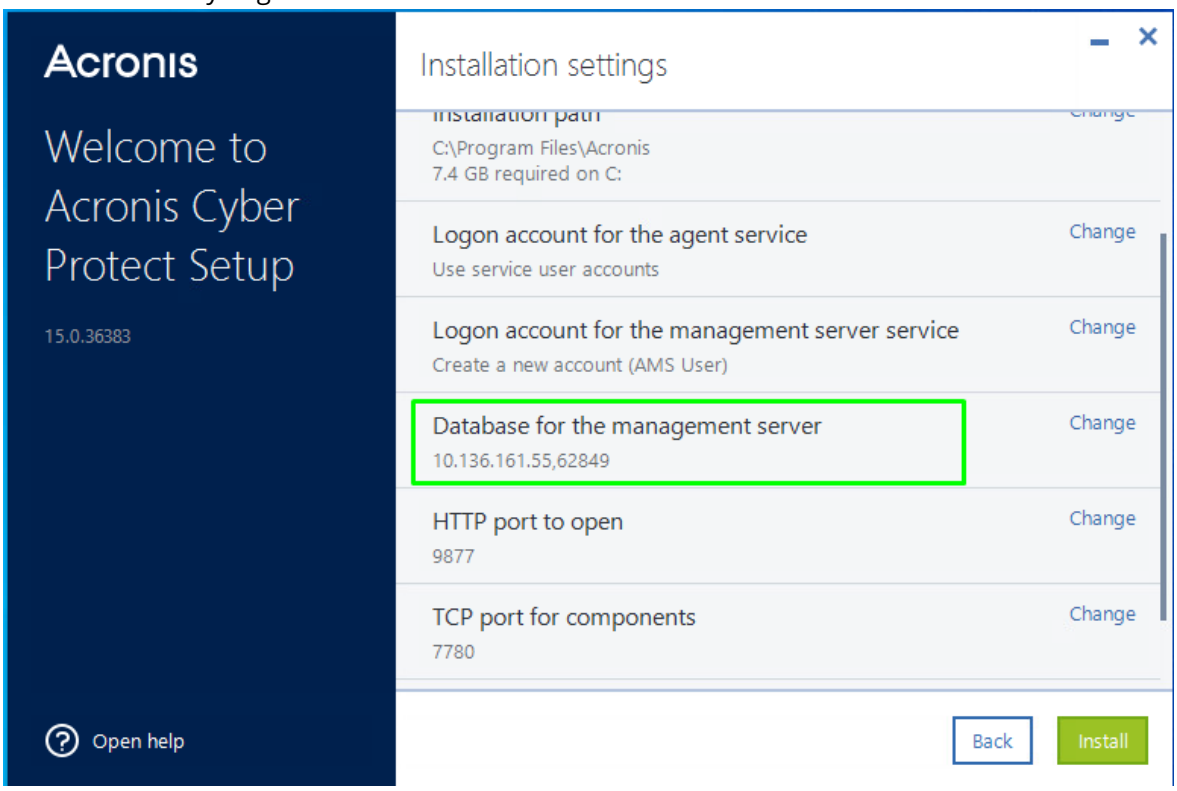
  De manera predeterminada, el servidor de gestión utiliza la base de datos SQLite integrada. Permite el registro de aproximadamente 900-1000 cargas de trabajo en el servidor de gestión. SQLite no es compatible con Scan Service.
- Microsoft SQL

  Microsoft SQL permite el registro de hasta 8000 cargas de trabajo en el servidor de gestión sin ninguna degradación significativa del rendimiento. El servidor de gestión, Scan Service y otros programas pueden utilizar la misma instancia de Microsoft SQL.

  Se admiten las siguientes versiones de MS SQL Server:
  - Microsoft SQL Server 2019 (ejecutada en Windows)
  - Microsoft SQL Server 2017 (ejecutada en Windows)
  - Microsoft SQL Server 2016
  - Microsoft SQL Server 2014
  - Microsoft SQL Server 2012

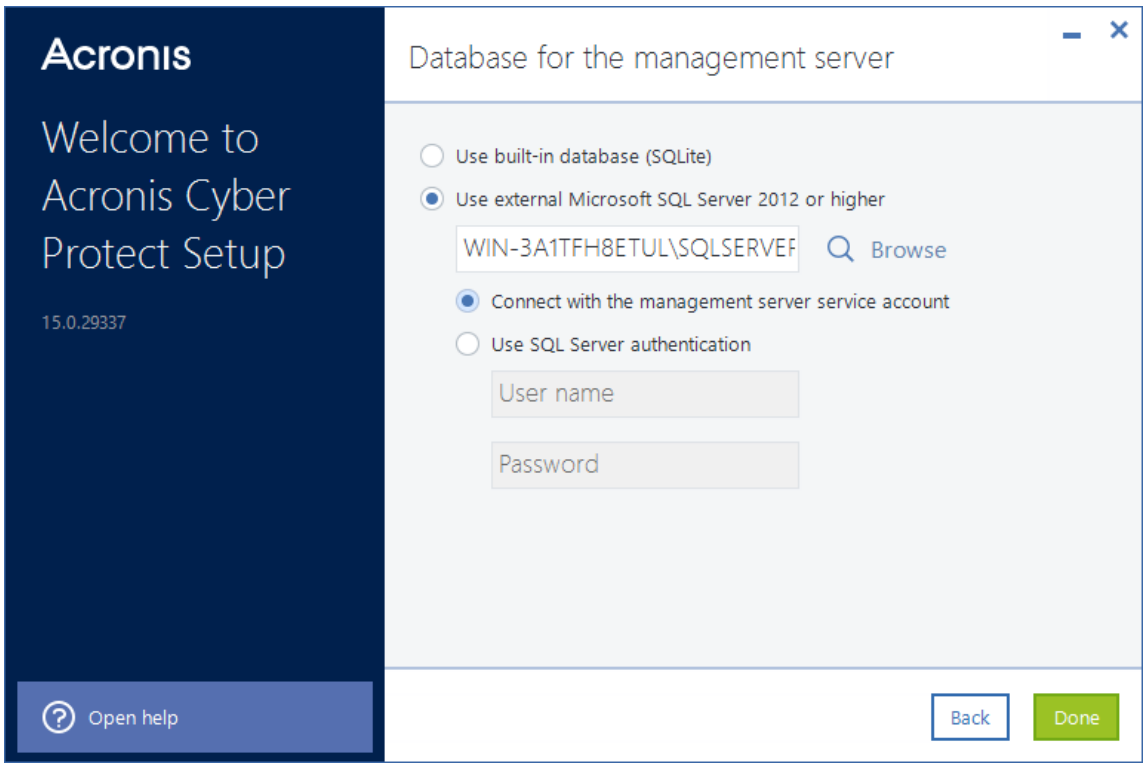
Para conectarse a una base de datos SQL externa

1. En el cuadro de diálogo Configuración, localice la opción **Base de datos para el servidor de administración** y haga clic en **Cambiar**.

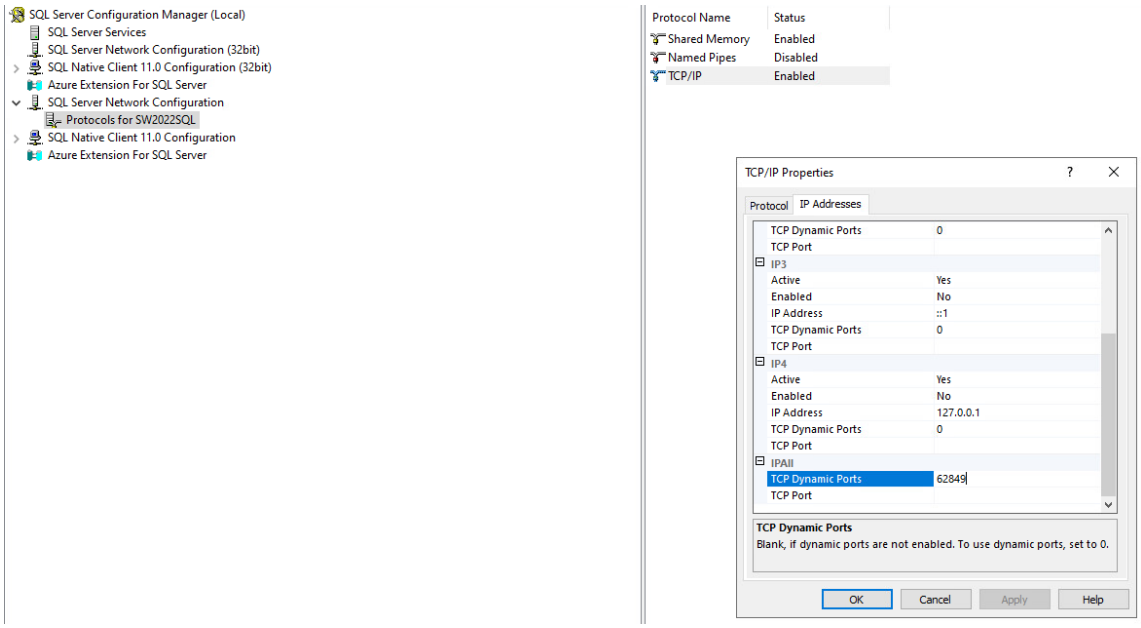


2. Seleccione **Utilizar Microsoft SQL Server 2012 externo o superior** y especifique el nombre de dominio o la dirección del servidor Microsoft SQL.
   - Si se conecta a la instancia de Microsoft SQL predeterminada en el servidor (**MSSQLSERVER**), basta con especificar el nombre del dominio del equipo donde se ejecuta. Si la instancia tiene

un nombre personalizado, debe especificarse con el siguiente formato: `<machine name\instance name>`.



- Si introduce la dirección IP, introduzca también el número de puerto de conexión, utilizando el formato `<ip_address, port>`.



Importante
Verifique que SQL Server Browser Service y el protocolo cliente TCP/IP estén habilitados en el equipo donde se ejecuta la instancia de Microsoft SQL. Para obtener más información sobre cómo iniciar SQL Server Browser Service, consulte la página https://msdn.microsoft.com/es-es/library/ms189093.aspx. Puede habilitar el protocolo TCP/IP al utilizar un procedimiento similar.

3. Seleccione cómo conectarse a la instancia Microsoft SQL especificada:
   - Autenticación de Windows (**Conectar con la cuenta de servicio del servidor de gestión**)
     Puede utilizar este método si configuró la opción C**uenta de inicio de sesión para el servicio del servidor de administración** en el cuadro de diálogo Configuración con la opción **Utilizar la siguiente cuenta** activada. La cuenta especificada debe seguir el formato `<MACHINE NAME>\Administrator` y debe tener la función **dbcreator** o **sysadmin** en Microsoft SQL Server.
     Para obtener más información la cuenta de inicio de sesión, consulte "Derechos de usuario necesarios para la cuenta de inicio de sesión del servicio" (p. 108).
   - Autenticación de SQL Server (**Utilice la autenticación de SQL Server**)
     Puede utilizar este método independientemente de otras configuraciones. La cuenta especificada debe tener la función **dbcreator** o **sysadmin** en Microsoft SQL Server.

Scan Service

Scan Service es un componente opcional que activa un análisis antimalware de copias de seguridad en un almacenamiento en la nube o en una carpeta local o de red. Scan Service requiere que el servidor de gestión esté instalado en el mismo equipo.

La instalación de Scan Service da acceso a las siguientes funcionalidades:

- Análisis de planes de copia de seguridad
- Widget de detalles del análisis de copias de seguridad
- Lista blanca corporativa
- Recuperación segura
- La columna **Estado** de la lista de copias de seguridad

Puede instalar Scan Service durante la instalación del servidor de gestión o añadirlo más adelante mediante la modificación de la instalación existente. Para obtener más información sobre cómo instalar componentes opcionales como Scan Service, consulte "Instalar componentes opcionales" (p. 107).

Importante

Scan Service no es compatible con la base de datos SQLite predeterminada que utiliza el servidor de gestión.

Puede configurar Scan Service con una base de datos Microsoft SQL o PostgreSQL. Consulte "Base se datos para Scan Service" (p. 114) para obtener más información sobre cómo elegir una.

Base se datos para Scan Service

Scan Service no es compatible con SQLite, la base de datos predeterminada para el servidor de gestión.

Si su servidor de gestión utiliza SQLite, puede configurar Scan Service únicamente con una base de datos PostgreSQL. Se admite PostgreSQL 9.6 y versiones posteriores.

Si su servidor de gestión utiliza Microsoft SQL Server, puede configurar Scan Service con la misma base de datos sin necesidad de más ajustes. También puede configurar Scan Service con una base de datos PostgreSQL.

Configurar Scan Service con una base de datos PostgreSQL

1. En el asistente de instalación, en **Base se datos para el servicio de detección**, haga clic en **Cambiar**.
2. Seleccione **Base de datos de PostgreSQL Server**.
3. Especifique el nombre del servidor de la instancia de PostgreSQL, o bien la dirección IP y el puerto.
4. Especifique las credenciales de un usuario que tenga el privilegio **CREATEDB** o que sea superusuario.

   Nota
   No se admite el método de autenticación SCRAM-SHA-256 de PostgreSQL 10 y versiones posteriores.

5. Haga clic en **Realizado**.

Puertos

Puede personalizar el puerto que utilizará un navegador web para acceder al servidor de gestión (de manera predeterminada, 9877) y el puerto que se utilizará para la comunicación entre los componentes del producto (de manera predeterminada, 7780). Si cambia este último puerto después de completar la instalación, deberá registrar de nuevo todos los componentes.

El cortafuegos de Windows se configura automáticamente durante la instalación. Si utiliza un cortafuegos diferente, asegúrese de que los puertos estén abiertos tanto para solicitudes entrantes como salientes a través de ese cortafuegos.

Servidor proxy

Puede elegir si los agentes de protección utilizan un servidor proxy HTTP cuando se realizan copias de seguridad a un almacenamiento en la cloud o una recuperación desde este almacenamiento.

Además, se utiliza el mismo servidor proxy para la comunicación entre los distintos componentes de Acronis Cyber Protect.

Para utilizar un servidor proxy, especifique el nombre del servidor, o la dirección IP y el número de puerto. Si el servidor proxy requiere autenticación, especifique las credenciales de acceso.

Nota
No es posible Actualizar las definiciones de protección (definiciones de antivirus y antimalware, definiciones avanzadas de detección, definiciones de análisis de vulnerabilidades y gestión de parches) cuando se utiliza un servidor proxy.

Instalación en Linux

Preparación

1. Si desea instalar Agente para Linux junto con el servidor de gestión, asegúrese de que los paquetes de Linux necesarios se han instalado en el equipo.
2. Seleccione la base de datos que debe utilizar el servidor de gestión.

Limitación

Los servidores de gestión que se ejecutan en equipos Linux no son compatibles con la instalación remota de agentes de protección que se utiliza, por ejemplo, en el procedimiento de autodetección. Para obtener más información acerca de una posible solución, consulte nuestra base de conocimientos: https://kb.acronis.com/content/69553.

Instalación

Para instalar el servidor de gestión necesita al menos 4 GB de espacio libre en disco.

Para instalar el servidor de gestión

1. Como el usuario raíz, vaya al directorio con el archivo de instalación, haga el archivo ejecutable y ejecútelo.

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

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

2. Acepte los términos del acuerdo de licencia.
3. [Opcional] Seleccione los componentes que desea instalar.
   De forma predeterminada, se instalarán los componentes siguientes:
   - Servidor de gestión
   - Agente para Linux
   - Bootable Media Builder
4. Especifique el puerto que utilizará un navegador web para acceder al servidor de gestión. El preajuste es 9877.

5. Especifique el puerto que utilizará para la comunicación entre los componentes del producto. El preajuste es 7780.
6. Haga clic en **Siguiente** para proceder con la instalación.
7. Cuando haya terminado la instalación, seleccione **Abrir consola web** y, después, haga clic en **Salir**. La consola web de Cyber Protect se abrirá en el navegador web predeterminado.

Para empezar a usar el servidor de gestión, actívelo iniciando sesión en su cuenta de Acronis o mediante el archivo de activación.

Instalación en un contenedor Docker

Para instalar el servidor de administración en un contenedor Docker, instale primero Docker Engine en su entorno.

Para más información, consulte https://docs.docker.com/engine/install/.

Instalación del servidor de gestión

Requisitos previos

Para instalar el servidor de administración en un contenedor Docker, necesita los siguientes archivos:

- `AB_AMS_prepare_env_ams.sh`.
- La imagen Docker del servidor de administración.
  Para obtener el archivo de imagen, póngase en contacto con su representante de ventas en Acronis.
  El siguiente procedimiento utiliza `acronisbackup15ams_29098.image` como ejemplo.

Para instalar el servidor de administración en un contenedor Docker

Nota
Para ejecutar los comandos de este procedimiento, utilice `sudo` o ejecútelos con la cuenta `root`.

1. Cargue la imagen Docker para el servidor de administración.
   Plantilla de entrada

   ```
   docker load -i /<path>/<image file>
   ```

   Ejemplo de entrada

   ```
   sudo docker load -i ./acronisbackup15ams_29098.image
   ```

2. Abra el archivo `AB_AMS_prepare_env_ams.sh` para editarlo y asegúrese de que el script utiliza el nombre de imagen y el número de compilación correctos.
   En este ejemplo, `acronisbackup15ams:29098`.

```
1 #! /bin/bash
2
3 DOCKER_IMAGE=acronisbackup15ams:29098
```

3. Si es necesario, edite la secuencia de comandos y, a continuación, guarde el archivo `AB_AMS_prepare_env_ams.sh`.
4. Asigne el permiso de ejecución al archivo `AB_AMS_prepare_env_ams.sh` y, a continuación, ejecútelo.

Plantilla de entrada

```
chmod +x /<path>/AB_AMS_prepare_env_ams.sh
```

```
/<path>/AB_AMS_prepare_env_ams.sh
```

Ejemplo de entrada

```
sudo chmod +x ./AB_AMS_prepare_env_ams.sh
```

```
sudo ./AB_AMS_prepare_env_ams.sh
```

Ejemplo de salida

```
[root@centos7x64-UEFI ~]# docker load -i acronisbackup15ams_29098.image.1
d6bb3538baeb: Loading layer [==================================================>]
3.584kB/3.584kB
7119294a5178: Loading layer [==================================================>]
2.041GB/2.041GB
Loaded image: acronisbackup15ams:29098

[root@centos7x64-UEFI ~]# ./AB_AMS_prepare_env_ams.sh
=== Check docker swarm exist ===
OK
=== Check docker volume exist: AcronisAMS_var_log ===
[]
Error: No such volume: AcronisAMS_var_log
Try to fix.
Creating docker volume: AcronisAMS_var_log
AcronisAMS_var_log
OK
=== Check docker volume exist: AcronisAMS_opt_acronis ===
[]
Error: No such volume: AcronisAMS_opt_acronis
Try to fix.
Creating docker volume: AcronisAMS_opt_acronis
AcronisAMS_opt_acronis
OK
=== Check docker volume exist: AcronisAMS_etc ===
[]
Error: No such volume: AcronisAMS_etc
```

```
Try to fix.
Creating docker volume: AcronisAMS_etc
AcronisAMS_etc
OK
=== Check docker volume exist: AcronisAMS_usr_sbin ===
[]
Error: No such volume: AcronisAMS_usr_sbin
Try to fix.
Creating docker volume: AcronisAMS_usr_sbin
AcronisAMS_usr_sbin
OK
=== Check docker volume exist: AcronisAMS_var_lib_acronis ===
[]
Error: No such volume: AcronisAMS_var_lib_acronis
Try to fix.
Creating docker volume: AcronisAMS_var_lib_acronis
AcronisAMS_var_lib_acronis
OK
=== Check docker volume exist: AcronisAMS_usr_lib_acronis ===
[]
Error: No such volume: AcronisAMS_usr_lib_acronis
Try to fix.
Creating docker volume: AcronisAMS_usr_lib_acronis
AcronisAMS_usr_lib_acronis
OK
Copying files from container: /etc/* -> docker volume "etc"
Copying files: /var/log/* -> docker volume "var_log"
Copying files: /usr/sbin/* -> docker volume "usr_sbin"
+ FILE_VERS=/var/lib/Acronis/BackupAndRecovery_version.txt
+ prepare_mode=no
+ getopts ph flag
+ case "${flag}" in
+ prepare_mode=yes
+ getopts ph flag
+ '[' -f /var/lib/Acronis/BackupAndRecovery_version.txt ']'
+ '[' '!' -f /var/lib/Acronis/BackupAndRecovery_version.txt ']'
+ /tmp/AcronisBackup.x86_64 -a --id=AcronisCentralizedManagementServer
Initializing...Done
Warning
The following issues have been detected in the system configuration:

* The following devices from '/proc/partitions' are missing from '/dev' and will be
created automatically:
sda(8,0)
sda1(8,1)
sda2(8,2)
sda3(8,3)
sdb(8,16)

Installing the required package 'java-1.8.0-openjdk-headless'...Trying to install the
required packages by using YUM.
```

```
Done
Stopping services...Done
Installing Acronis Cyber Protect Packages
MonitoringServer-15.0.29098-1
WebConsole-15.0.29098-1
AcronisCentralizedManagementServer-15.0.29098-1
Upgrading services...
Starting services...Done
Upgrading services stage after-start...
Congratulations!
Acronis Cyber Protect has been successfully installed in the system.

Warning: A firewall has been detected in the system.
Please configure the firewall to allow connections
to Acronis Cyber Protect.

+ [[ yes == \y\e\s ]]
+ echo 'prepare_mode=yes: exit 0 from container'
prepare_mode=yes: exit 0 from container
+ echo 'sleep 60'
sleep 60
+ sleep 60
+ exit 0
Docker secret ams_masterkey already created

Command to run docker service for ams:
docker service create -p 9877:9877 -p 7780:7780 --name="ams"     --mount
target="/var/log",source="AcronisAMS_var_log" --mount
target="/opt/acronis",source="AcronisAMS_opt_acronis" --mount
target="/etc",source="AcronisAMS_etc" --mount target="/usr/sbin",source="AcronisAMS_
usr_sbin" --mount target="/var/lib/Acronis",source="AcronisAMS_var_lib_acronis" --
mount target="/usr/lib/Acronis",source="AcronisAMS_usr_lib_acronis" --secret src=ams_
masterkey,target="/var/lib/Acronis/CredStore/masterkey.local" --secret="ams_
masterkey" "acronisbackup15ams:29098"
```

5. Ejecute el servicio Docker para crear el contenedor con Acronis Management Server.

Plantilla de entrada

```
docker service create -p 9877:9877 -p 7780:7780 --name="ams" --mount
target="/var/log",source="AcronisAMS_var_log" --mount
target="/opt/acronis",source="AcronisAMS_opt_acronis" --mount
target="/etc",source="AcronisAMS_etc" --mount target="/usr/sbin",source="AcronisAMS_
usr_sbin" --mount target="/var/lib/Acronis",source="AcronisAMS_var_lib_acronis" --
mount target="/usr/lib/Acronis",source="AcronisAMS_usr_lib_acronis" --secret src=ams_
masterkey,target="/var/lib/Acronis/CredStore/masterkey.local" --secret="ams_
masterkey" "<image:build>"
```

Ejemplo de entrada

```
sudo docker service create -p 9877:9877 -p 7780:7780 --name="ams" --mount
target="/var/log",source="AcronisAMS_var_log" --mount
```

```
target="/opt/acronis",source="AcronisAMS_opt_acronis" --mount
target="/etc",source="AcronisAMS_etc" --mount target="/usr/sbin",source="AcronisAMS_
usr_sbin" --mount target="/var/lib/Acronis",source="AcronisAMS_var_lib_acronis" --
mount target="/usr/lib/Acronis",source="AcronisAMS_usr_lib_acronis" --secret src=ams_
masterkey,target="/var/lib/Acronis/CredStore/masterkey.local" --secret="ams_
masterkey" "acronisbackup15ams:29098"
```

Nota

Al final de este comando, debe utilizar un nombre de imagen y un número de compilación que dependan del archivo de imagen.

En el ejemplo anterior, son `acronisbackup15ams:29098`. Para comprobarlos en su imagen, ejecute el comando `docker images` y consulte las columnas `REPOSITORY` y `TAG`.

Ejemplo de entrada

```
sudo docker images
```

Ejemplo de salida

```
# REPOSITORY            TAG     IMAGE ID        CREATED       SIZE
# acronisbackup15ams    29098   9f473ae338b7    4 weeks ago   2.14GB
```

6. Introduzca el contenedor y, a continuación, establezca la contraseña para el usuario raíz.
   a. Compruebe el ID del contenedor.

      Ejemplo de entrada

      ```
      sudo docker service ps -a
      ```

      Ejemplo de salida

      ```
      # CONTAINER ID     IMAGE                       COMMAND                  CREATED
           STATUS        PORTS               NAMES
      # bfb9d14d4879     acronisbackup15ams:29098   "/bin/bash -c'/opt/..."   2 minutes
      ago   Up 2 minutes  7780/tcp, 9877/tcp  ams.1.ko7xklvta28rasyukn6kic1ka
      ```

   b. Entre en el contenedor.

      Plantilla de entrada

      ```
      docker exec -it <container ID> bash
      ```

      Ejemplo de entrada

      ```
      sudo docker exec -it bfb9d14d4879 bash
      ```

   c. Establezca la contraseña para el usuario raíz.

      Plantilla de entrada

      ```
      echo root:<your_new_root_password> | chpasswd
      ```

Ejemplo de entrada

```
sudo echo root:MyPassword | chpasswd
```

7. Conéctese como usuario raíz a la consola Cyber Protect en http://ip_docker_host:9877.

Actualizar el servidor de administración

Los procedimientos de actualización y los requisitos previos dependen de la versión del servidor de administración que utilice.

Compilación 26981 o anterior

Acronis Cyber Protect La versión 15 Actualización 2 se publicó como build 26981 el 7 de mayo de 2021.

Puede actualizar el servidor de administración a la compilación 29486 (publicada el 19 de abril de 2022) o posterior.

Requisitos previos

Para actualizar el servidor de administración en un contenedor Docker, necesita los siguientes archivos:

- `AB_AMS_migrate_data_to_volumes.sh`.
- `AB_AMS_prepare_env_ams.sh`.
- La imagen Docker de la nueva versión del servidor de administración.
  Para obtener el archivo de imagen, póngase en contacto con su representante de ventas en Acronis.
  El siguiente procedimiento utiliza `acronisbackup15ams_29098.image` como ejemplo.

Para actualizar el servidor de administración en un contenedor Docker

Nota
Para ejecutar los comandos de este procedimiento, utilice `sudo` o ejecútelos con la cuenta `root`.

1. Compruebe las imágenes Docker cargadas.

   Ejemplo de entrada

   ```
   sudo docker images
   ```

   Ejemplo de salida

   ```
   # REPOSITORY                                                    TAG       IMAGE
   ID       CREATED        SIZE
   # acronisbackup12.5ams                                          27009
   26b7ba78400f   9 months ago   3.18GB
   ```

2. Detenga el servicio AMS. Puede utilizar el nombre del servicio o el ID del servicio en este comando.

   Ejemplo de entrada

   ```
   sudo docker service rm ams
   ```

3. Asigne permiso de ejecución al archivo `AB_AMS_migrate_data_to_volumes.sh` y, a continuación, ejecútelo para migrar los datos del servidor de administración a volúmenes docker.

   Plantilla de entrada

   ```
   chmod +x /<path>/AB_AMS_migrate_data_to_volumes.sh
   ```

   ```
   /<path>/AB_AMS_migrate_data_to_volumes.sh -i <image:build>
   ```

   Ejemplo de entrada

   ```
   sudo chmod +x ./AB_AMS_migrate_data_to_volumes.sh
   ```

   ```
   sudo ./AB_AMS_migrate_data_to_volumes.sh -i acronisbackup12.5ams:27009
   ```

4. Cargue la imagen Docker con la versión más reciente del AcronisServidor de administración.

   Plantilla de entrada

   ```
   docker load -i /<path>/<image file>
   ```

   Ejemplo de entrada

   ```
   sudo docker load -i ./acronisbackup15ams_29098.image
   ```

   Ejemplo de salida

   ```
   # REPOSITORY                                                    TAG       IMAGE
   ID       CREATED        SIZE
   # acronisbackup12.5ams                                          27009
   26b7ba78400f   9 months ago   3.18GB
   # acronisbackup15ams                                            29098
   5d20f7d3155f   26 hours ago   2.38GB
   ```

5. Abra el archivo `AB_AMS_prepare_env_ams.sh` para editarlo y asegúrese de que el script utiliza el nombre de imagen y el número de compilación correctos.

   En este ejemplo, `acronisbackup15ams:29098`.

   ```
   1 #! /bin/bash
   2
   3 DOCKER_IMAGE=acronisbackup15ams:29098
   ```

6. Si es necesario, edite la secuencia de comandos y, a continuación, guarde el archivo `AB_AMS_prepare_env_ams.sh`.

7. Asigne el permiso de ejecución al archivo `AB_AMS_prepare_env_ams.sh` y, a continuación, ejecútelo.

   Plantilla de entrada

   ```
   chmod +x /<path>/AB_AMS_prepare_env_ams.sh
   ```

   ```
   /<path>/AB_AMS_prepare_env_ams.sh
   ```

   Ejemplo de entrada

   ```
   sudo chmod +x ./AB_AMS_prepare_env_ams.sh
   ```

   ```
   sudo ./AB_AMS_prepare_env_ams.sh
   ```

8. Ejecute el servicio Docker para crear el contenedor con Acronis Management Server.

   Plantilla de entrada

   ```
   docker service create -p 9877:9877 -p 7780:7780 --name="ams" --mount
   target="/var/log",source="AcronisAMS_var_log" --mount
   target="/opt/acronis",source="AcronisAMS_opt_acronis" --mount
   target="/etc",source="AcronisAMS_etc" --mount target="/usr/sbin",source="AcronisAMS_
   usr_sbin" --mount target="/var/lib/Acronis",source="AcronisAMS_var_lib_acronis" --
   mount target="/usr/lib/Acronis",source="AcronisAMS_usr_lib_acronis" --secret src=ams_
   masterkey,target="/opt/CredStore/masterkey.local" --secret="ams_masterkey"
   "<image:build>"
   ```

   Ejemplo de entrada

   ```
   sudo docker service create -p 9877:9877 -p 7780:7780 --name="ams" --mount
   target="/var/log",source="AcronisAMS_var_log" --mount
   target="/opt/acronis",source="AcronisAMS_opt_acronis" --mount
   target="/etc",source="AcronisAMS_etc" --mount target="/usr/sbin",source="AcronisAMS_
   usr_sbin" --mount target="/var/lib/Acronis",source="AcronisAMS_var_lib_acronis" --
   mount target="/usr/lib/Acronis",source="AcronisAMS_usr_lib_acronis" --secret src=ams_
   masterkey,target="/opt/CredStore/masterkey.local" --secret="ams_masterkey"
   "acronisbackup15ams:29098"
   ```

Nota

Al final de este comando, debe utilizar un nombre de imagen y un número de compilación que dependan del archivo de imagen.

En el ejemplo anterior, son `acronisbackup15ams:29098`. Para comprobarlos en su imagen, ejecute el comando `docker images` y consulte las columnas `REPOSITORY` y `TAG`.

Ejemplo de entrada

```
sudo docker images
```

Ejemplo de salida

```
# REPOSITORY            TAG     IMAGE ID        CREATED       SIZE
# acronisbackup15ams    29098   9f473ae338b7    4 weeks ago   2.14GB
```

9. Introduzca el contenedor y, a continuación, establezca la contraseña para el usuario raíz.
   a. Compruebe el ID del contenedor.

      Ejemplo de entrada

      ```
      sudo docker service ps -a
      ```

      Ejemplo de salida

      ```
      # CONTAINER ID     IMAGE                       COMMAND                  CREATED
           STATUS         PORTS                NAMES
      # bfb9d14d4879     acronisbackup15ams:29098   "/bin/bash -c'/opt/..."   2 minutes
      ago    Up 2 minutes   7780/tcp, 9877/tcp   ams.1.ko7xklvta28rasyukn6kic1ka
      ```

   b. Entre en el contenedor.

      Plantilla de entrada

      ```
      docker exec -it <container ID> bash
      ```

      Ejemplo de entrada

      ```
      sudo docker exec -it bfb9d14d4879 bash
      ```

   c. Establezca la contraseña para el usuario raíz.

      Plantilla de entrada

      ```
      echo root:<your_new_root_password> | chpasswd
      ```

      Ejemplo de entrada

      ```
      sudo echo root:MyPassword | chpasswd
      ```

10. Conéctese como usuario raíz a la consola Cyber Protect en http://ip_docker_host:9877.

Compilación 29240 o posterior

Acronis Cyber Protect La versión 15 Actualización 4 se publicó como build 29240 el 7 de marzo de 2022.

Requisitos previos

Para actualizar el servidor de administración en un contenedor Docker, necesita los siguientes archivos:

- `AB_AMS_prepare_env_ams.sh`.
- La imagen Docker de la nueva versión del servidor de administración.
  Para obtener el archivo de imagen, póngase en contacto con su representante de ventas en Acronis.
  El siguiente procedimiento utiliza `acronisbackup15ams_29098.image` como ejemplo.

Para actualizar el servidor de administración en un contenedor Docker

Nota
Para ejecutar los comandos de este procedimiento, utilice `sudo` o ejecútelos con la cuenta `root`.

1. Compruebe las imágenes Docker cargadas.
   Ejemplo de entrada

   ```
   sudo docker images
   ```

   Ejemplo de salida

   ```
   # REPOSITORY                                                TAG       IMAGE ID
        CREATED        SIZE
   # acronisbackup15ams                                        29094
   26b7ba78400f   9 months ago   3.18GB
   ```

2. Detenga el servicio AMS. Puede utilizar el nombre del servicio o el ID del servicio en este comando.
   Ejemplo de entrada

   ```
   sudo docker service rm ams
   ```

3. Cargue la imagen Docker con la versión más reciente del AcronisServidor de administración.
   Plantilla de entrada

   ```
   docker load -i /<path>/<image file>
   ```

   Ejemplo de entrada

   ```
   sudo docker load -i ./acronisbackup15ams_29098.image
   ```

   Ejemplo de salida

```
# REPOSITORY                                                    TAG       IMAGE
ID       CREATED        SIZE
# acronisbackup15ams                                           29094
26b7ba78400f   9 months ago   3.18GB
# acronisbackup15ams                                           29098
5d20f7d3155f   26 hours ago   2.38GB
```

4. Abra el archivo `AB_AMS_prepare_env_ams.sh` para editarlo y asegúrese de que el script utiliza el nombre de imagen y el número de compilación correctos.

   En este ejemplo, `acronisbackup15ams:29098`.

```
1 #! /bin/bash
2
3 DOCKER_IMAGE=acronisbackup15ams:29098
```

5. Si es necesario, edite la secuencia de comandos y, a continuación, guarde el archivo `AB_AMS_prepare_env_ams.sh`.
6. Asigne el permiso de ejecución al archivo `AB_AMS_prepare_env_ams.sh` y, a continuación, ejecútelo.

   Plantilla de entrada

```
chmod +x /<path>/AB_AMS_prepare_env_ams.sh
```

```
/<path>/AB_AMS_prepare_env_ams.sh
```

   Ejemplo de entrada

```
sudo chmod +x ./AB_AMS_prepare_env_ams.sh
```

```
sudo ./AB_AMS_prepare_env_ams.sh
```

7. Ejecute el servicio Docker para crear el contenedor con Acronis Management Server.

   Plantilla de entrada

```
docker service create -p 9877:9877 -p 7780:7780 --name="ams" --mount
target="/var/log",source="AcronisAMS_var_log" --mount
target="/opt/acronis",source="AcronisAMS_opt_acronis" --mount
target="/etc",source="AcronisAMS_etc" --mount target="/usr/sbin",source="AcronisAMS_
usr_sbin" --mount target="/var/lib/Acronis",source="AcronisAMS_var_lib_acronis" --
mount target="/usr/lib/Acronis",source="AcronisAMS_usr_lib_acronis" --secret src=ams_
masterkey,target="/opt/CredStore/masterkey.local" --secret="ams_masterkey"
"<image:build>"
```

   Ejemplo de entrada

```
sudo docker service create -p 9877:9877 -p 7780:7780 --name="ams" --mount
target="/var/log",source="AcronisAMS_var_log" --mount
target="/opt/acronis",source="AcronisAMS_opt_acronis" --mount
```

```
target="/etc",source="AcronisAMS_etc" --mount target="/usr/sbin",source="AcronisAMS_
usr_sbin" --mount target="/var/lib/Acronis",source="AcronisAMS_var_lib_acronis" --
mount target="/usr/lib/Acronis",source="AcronisAMS_usr_lib_acronis" --secret src=ams_
masterkey,target="/opt/CredStore/masterkey.local" --secret="ams_masterkey"
"acronisbackup15ams:29098"
```

Nota

Al final de este comando, debe utilizar un nombre de imagen y un número de compilación que dependan del archivo de imagen.

En el ejemplo anterior, son `acronisbackup15ams:29098`. Para comprobarlos en su imagen, ejecute el comando `docker images` y consulte las columnas `REPOSITORY` y `TAG`.

Ejemplo de entrada

```
sudo docker images
```

Ejemplo de salida

```
# REPOSITORY            TAG     IMAGE ID        CREATED       SIZE
# acronisbackup15ams    29098   9f473ae338b7    4 weeks ago   2.14GB
```

8. Introduzca el contenedor y, a continuación, establezca la contraseña para el usuario raíz.
   a. Compruebe el ID del contenedor.

      Ejemplo de entrada

      ```
      sudo docker service ps -a
      ```

      Ejemplo de salida

      ```
      # CONTAINER ID     IMAGE                        COMMAND                  CREATED
           STATUS         PORTS               NAMES
      # bfb9d14d4879     acronisbackup15ams:29098   "/bin/bash -c'/opt/..."   2 minutes
      ago   Up 2 minutes  7780/tcp, 9877/tcp  ams.1.ko7xklvta28rasyukn6kic1ka
      ```

   b. Entre en el contenedor.

      Plantilla de entrada

      ```
      docker exec -it <container ID> bash
      ```

      Ejemplo de entrada

      ```
      sudo docker exec -it bfb9d14d4879 bash
      ```

   c. Establezca la contraseña para el usuario raíz.

      Plantilla de entrada

      ```
      echo root:<your_new_root_password> | chpasswd
      ```

Ejemplo de entrada

```
sudo echo root:MyPassword | chpasswd
```

9. Conéctese como usuario raíz a la consola Cyber Protect en http://ip_docker_host:9877.

Dispositivo Acronis Cyber Protect

Con el dispositivo Acronis Cyber Protect, puede obtener fácilmente un equipo virtual con el software siguiente:

- CentOS
- Componentes de Acronis Cyber Protect:
  - Servidor de gestión
  - Agente para Linux
  - Agent for VMware (Linux)

El dispositivo se proporciona como un archivo zip. El archivo comprimido contiene los archivos .ovf y .iso. Puede implementar el archivo .ovf a un servidor ESXi o utilizar el archivo .iso para iniciar un equipo virtual existente. El archivo comprimido también incluye el archivo .vmdk, que debería colocarse en el mismo directorio que el .ovf.

Nota
VMware Host Client (un cliente web para gestionar ESXi 6.0+ independiente) no permite la implementación de plantillas OVF con una imagen ISO en su interior. Si este es su caso, cree un equipo virtual que cumpla los requisitos siguientes y, a continuación, utilice el archivo .iso para instalar el software.

Estos son los requisitos para el dispositivo virtual:

- Requisitos mínimos del sistema:
  - 2 CPU
  - 6 GB de RAM
  - Un disco virtual de 10 GB (se recomiendan 40 GB)
- En la configuración del equipo virtual VMware, haga clic en la pestaña **Opciones** > **General** > **Parámetros de configuración** y, a continuación, asegúrese de que el valor del parámetro `disk.EnableUUID` sea `true`.

Limitación

Los servidores de gestión que se ejecutan en equipos Linux, incluido el dispositivo de Acronis Cyber Protect, no son compatibles con la instalación remota de agentes de protección que se utiliza, por ejemplo, en el procedimiento de autodetección. Para obtener más información acerca de una posible solución, consulte nuestra base de conocimientos: https://kb.acronis.com/content/69553.

Instalar el software

1. Realice uno de los siguientes procedimientos:
   - Implementar el dispositivo desde el archivo .ovf. Una vez finalizada la implementación, inicie el equipo resultante.
   - Inicie un equipo virtual existente desde .iso.
2. Seleccione **Instalar o actualizar Acronis Cyber Protect** y pulse **Intro**. Espere a que aparezca la ventana de configuración inicial.
3. [Opcional] Para cambiar los ajustes de instalación, seleccione **Cambiar configuración** y pulse **Intro**. Puede especificar los ajustes siguientes:
   - El nombre de servidor del dispositivo (de forma predeterminada, `AcronisAppliance-<random part>`).
   - La contraseña de la cuenta raíz que se utilizará para iniciar sesión en la consola web de Cyber Protect (de forma predeterminada, **no especificado**).

     Si mantiene el valor predeterminado, se le pedirá que especifique la contraseña una vez instalado Acronis Cyber Protect. Sin la contraseña, no podrá iniciar sesión en la consola web de Cyber Protect ni en la consola web Cockpit.
   - Configuración de red de una tarjeta de interfaz de red:
     - **Usar DHCP** (opción predeterminada)
     - **Definir dirección IP estática**

     Si el equipo tiene varias tarjetas de interfaz de red, el software selecciona una de ellas aleatoriamente y le aplica la configuración.
4. Seleccione **Instalar con la configuración actual**.

Como resultado, CentOS y Acronis Cyber Protect se instalarán en el equipo.

Otras acciones

Una vez finalizada la instalación, el software muestra los enlaces a la consola web de Cyber Protect y a la consola web Cockpit. Conéctese a la consola web de Cyber Protect para empezar a utilizar Acronis Cyber Protect (añadir más dispositivos, crear planes de copias de seguridad, etc.).

Para añadir equipos virtuales ESXi, haga clic en **Agregar** > **VMware ESXi** y especifique la dirección y las credenciales del vCenter Server o el servidor ESXi independiente.

Ningún ajuste de Acronis Cyber Protect se configura en la consola web Cockpit. La consola se proporciona por comodidad y para solucionar problemas.

Actualización del software

1. Descargue y descomprima el archivo zip con la nueva versión del dispositivo.
2. Inicie el equipo desde el archivo .iso descomprimido en el paso anterior.

a. Guarde el .iso en su almacén de datos de vSphere.
b. Conecte el .iso a la unidad de CD/DVD del equipo.
c. Reinicie el equipo.
d. [Solo durante la primera actualización] Presione **F2**, y modifique el orden de arranque para que vaya primero la unidad de CD/DVD.

3. Seleccione **Instalar o actualizar Acronis Cyber Protect** y pulse **Intro**.
4. Seleccione **Actualizar** y pulse **Intro**.
5. Una vez completada la actualización, desconecte el .iso de la unidad de CD/DVD del equipo.

Como resultado, se actualizará Acronis Cyber Protect. Si la versión de CentOS en el archivo .iso también es más reciente que la versión en el disco, el sistema operativo se actualizará antes de actualizar Acronis Cyber Protect.

Añadir equipos desde la consola web de Cyber Protect

Puede añadir un equipo de una de las siguientes formas:

- Descargue el programa de instalación y ejecútelo de forma local en el equipo de destino.
- Instale un agente de protección remotamente en el equipo de destino.

Limitaciones

- La instalación remota solo está disponible con un servidor de administración que se ejecute en un equipo Windows. Los equipos de destino también deben ejecutar Windows.
- La instalación remota no es compatible con equipos que ejecutan Windows XP.
- La instalación remota no es compatible con los controladores de dominios. Para obtener más información sobre cómo instalar un agente de protección en un controlador de dominio, consulte "Instalación en Windows" (p. 139). Asegúrese de personalizar la configuración de la instalación mediante la selección de **Utilizar la siguiente cuenta** en **Cuenta de inicio de sesión para el servicio de agente**. Para obtener más información acerca de esta opción, consulte "Derechos de usuario necesarios para la cuenta de inicio de sesión del servicio" (p. 108).

Adición de un equipo que ejecute Windows

Puede añadir un equipo Windows mediante la instalación de un agente de protección de forma remota, en la consola web de Cyber Protect, o mediante la descarga y ejecución del programa de instalación de forma local.

Pasos para instalar un agente remotamente

Importante
Antes de comenzar la instalación, asegúrese de que se cumplen los requisitos previos para la instalación remota. Consulte "Prerrequisitos para la instalación remota" (p. 132).

Se requiere al menos un agente en línea en su entorno. Este agente se utilizará como agente de implementación. Consulte "Agente de despliegue" (p. 134).

Para obtener más información sobre la instalación o actualización remota de un agente de protección en un equipo de 32 bits, consulte este artículo de la base de conocimiento.

1. En la consola web de Cyber Protect, vaya a **Dispositivos** > **Todos los dispositivos**.
2. Haga clic en **Agregar**.
3. [Para instalar Agente para Windows] Haga clic en **Windows**.
4. [Para instalar otro agente compatible] Haga clic en el botón que corresponde a la aplicación que desea proteger.
   Los agentes disponibles son los siguientes:
   - Agente para Hyper-V
   - Agente para SQL + Agente para Windows
   - Agent for Exchange + Agente para Windows
     Si ha hecho clic en **Microsoft Exchange Server** > **Buzones de correo de Exchange** y ya hay registrado al menos un Agent for Exchange, vaya al paso 9.
   - Agente para Active Directory + Agente para Windows
   - Agente para Office 365
5. En el panel que se abre, seleccione el agente de despliegue.
6. Especifique el nombre del servidor o la dirección IP del equipo de destino, y las credenciales de una cuenta con derechos de administración para ese equipo.
   Se recomienda usar la cuenta de administrador integrada. Para usar otra cuenta, añada la cuenta al grupo de administradores y modifique el registro del equipo de destino según se describe en el siguiente artículo: https://support.microsoft.com/es-es/help/951016/description-of-user-account-control-and-remote-restrictions-in-windows.
7. Seleccione el nombre o la dirección IP del servidor de administración que el agente utilizará para acceder a ese servidor.
   De forma predeterminada, se selecciona el nombre del servidor. Puede que deba seleccionar la dirección IP en su lugar si su servidor de administración tiene más de una interfaz de red o si está experimentando problemas de DNS que provocan que el registro del agente falle.
8. Haga clic en **Instalar**.
9. Si ha seleccionado **Microsoft Exchange Server** > **Buzones de correo de Exchange** en el paso 4, especifique el equipo en el que esté habilitado el rol **Servidor de acceso de cliente** (CAS) de Microsoft Exchange Server. Para obtener más información, consulte "Copia de seguridad de casillas de correo" (p. 509).

Pasos para descargar e instalar un agente de forma local

1. En la consola web de Cyber Protect, haga clic en el icono de la cuenta en la esquina superior derecha y luego haga clic en **Descargas**.
2. Haga clic en el nombre del programa de instalación de Windows que necesite.
   El programa de instalación se descargará en su equipo.
3. Ejecute el programa de instalación en el equipo que quiera proteger. Para obtener más información, consulte "Instalación en Windows" (p. 139).

Prerrequisitos para la instalación remota

- Para que la instalación se realice correctamente en un equipo remoto con Windows 7 o una versión posterior, la opción **Panel de control** > **Opciones de carpeta** > **Ver** > **Uso del asistente para compartir** se debe *desactivar* en ese equipo.
- Para una instalación correcta en un equipo remoto que *no* sea miembro de un dominio de Active Directory, el control de cuentas de usuario (UAC) debe estar *deshabilitado* en ese equipo. Para obtener más información sobre cómo desactivarlo, consulte "Pasos para deshabilitar UAC" (p. 133).
- De forma predeterminada, se necesitan las credenciales de la cuenta de administrador incorporada para la instalación remota de cualquier equipo Windows. Para llevar a cabo la instalación remota usando las credenciales de otra cuenta de administrador, las restricciones remotas del control de cuentas de usuario (UAC) deben estar *deshabilitadas*. Para obtener más información sobre cómo desactivarlos, consulte "Pasos para deshabilitar las restricciones remotas de UAC" (p. 133).
- El uso compartido de archivos e impresoras deben estar *habilitado* en el equipo remoto. Para acceder a esta opción:
  - [En un equipo con Windows 2003 Server] Vaya a **Panel de control** > **Firewall de Windows** > **Excepciones** > **Uso compartido de archivos e impresoras**.
  - [En un equipo con Windows Server 2008, Windows 7 o una versión posterior] Vaya a **Panel de control** > **Firewall de Windows** > **Centro de redes y uso compartido** > **Cambiar las configuraciones avanzadas de uso compartido**.
- Acronis Cyber Protect utiliza los puertos TCP **445**, **25001** y **43234** para la instalación remota.
  El puerto **445** se abre automáticamente cuando habilita Compartir archivos e impresoras. Los puertos 43234 y 25001 se abren automáticamente por medio del cortafuegos de Windows. Si usa un cortafuegos diferente, asegúrese de que estos tres puertos estén abiertos (añadidos a excepciones) para las solicitudes entrantes y salientes.
  Una vez finalizada la instalación remota, el puerto **25001** se cierra automáticamente mediante el cortafuegos de Windows. Los puertos **445** y **43234** deberán permanecer abiertos si desea actualizar el agente de forma remota en el futuro. El puerto **25001** se abre y se cierra automáticamente mediante el cortafuegos de Windows en cada actualización. Si usa otro cortafuegos, mantenga los tres puertos abiertos.

Nota
La instalación remota no es compatible con equipos que ejecutan Windows XP.

Nota
La instalación remota no es compatible con los controladores de dominios. Para obtener más información sobre cómo instalar un agente de protección en un controlador de dominio, consulte "Instalación en Windows" (p. 139). Asegúrese de personalizar la configuración de la instalación mediante la selección de **Utilizar la siguiente cuenta** en **Cuenta de inicio de sesión para el servicio de agente**. Para obtener más información acerca de esta opción, consulte "Derechos de usuario necesarios para la cuenta de inicio de sesión del servicio" (p. 108).

Requisitos del control de cuentas de usuario (UAC)

En un equipo que ejecute Windows 7 o posterior y no sea miembro de un dominio de Active Directory, las operaciones de administración centralizadas (incluyendo la instalación remota) necesitan que UAC y las restricciones remotas de UAC estén deshabilitados.

Pasos para deshabilitar UAC

Realice una de las siguientes acciones según el sistema operativo:

- **En un sistema operativo de Windows anterior a Windows 8:**
  Vaya al **Panel de control > Vista por: Iconos pequeños > Cuentas de usuario > Cambiar la configuración de control de la cuenta de usuario** y después mueva el control deslizante a **No notificar**. Después, reinicie el equipo.
- **En cualquier sistema operativo de Windows**:
  1. Abra el Editor del registro.
  2. Busque la siguiente clave del registro: **HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System**
  3. Para el valor **EnableLUA**, cambie el ajuste a **0**.
  4. Reinicie el equipo.

Pasos para deshabilitar las restricciones remotas de UAC

1. Abra el Editor del registro.
2. Busque la siguiente clave del registro: **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System**
3. Para el valor **LocalAccountTokenFilterPolicy**, cambie el ajuste a **1**.
   Si el valor **LocalAccountTokenFilterPolicy** no existe, créelo como DWORD (32 bits). Para obtener más información sobre este valor, consulte la documentación de Microsoft: https://support.microsoft.com/en-us/help/951016/description-of-user-account-control-and-remote-restrictions-in-windows.

Nota
Por motivos de seguridad, cuando acabe la operación de gestión, por ejemplo, la instalación remota, se recomienda revertir ambos ajustes a su estado original: **EnableLUA**=**1** y **LocalAccountTokenFilterPolicy**=**0**.

Agente de despliegue

Para instalar agentes de protección en equipos remotos desde la consola web de Cyber Protect, debe tener al menos un agente instalado en el entorno. Este agente servirá como agente de despliegue para la instalación remota y se conectará al servidor de administración y al equipo remoto de destino.

Por lo general, el primer agente de protección del entorno es el agente que instala junto con el servidor de administración. Sin embargo, puede seleccionar que todos los Agentes para Windows del entorno sean agentes de despliegue.

Nota
Cuando utiliza la autodetección para instalar agentes de protección en varios equipos, el agente de protección se llama agente de detección.

Cómo funciona el agente de despliegue

1. El agente de despliegue se conecta al servidor de administración y descarga el archivo `web_installer.exe`.
2. El agente de despliegue se conecta al equipo remoto mediante el nombre de servidor o la dirección IP de ese equipo y las credenciales de administrador que especifique y carga el archivo `web_installer.exe` en él.
3. El archivo `web_installer.exe` se ejecuta en el equipo remoto en el modo de interacción.
4. Según el ámbito de la instalación requerida, el instalador web recupera los paquetes de instalación adicionales de la carpeta `installation_files` en el servidor de gestión y los instala en el equipo de destino con el comando `msiexec`.
   La carpeta `installation_files` está ubicada en:
   - Windows: `\Program Files\Acronis\RemoteInstallationFiles\`
   - Linux: `/usr/lib/Acronis/RemoteInstallationFiles/`
5. Cuando se completa la instalación, el agente se registra en el servidor de administración.

Componentes para la instalación remota

Los componentes para la instalación remota se instalan de forma predeterminada al instalar el servidor de administración.

Según el sistema operativo del equipo en el que se ejecuta el servidor de administración, puede encontrar estos componentes en las siguientes ubicaciones:

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

Estas ubicaciones podrían no estar disponibles si ha realizado una actualización desde una versión anterior de Acronis Cyber Protect o si ha excluido explícitamente **Componentes para la instalación remota** al instalar el servidor de administración. En este caso, debe añadir los componentes para la instalación remota manualmente. Para ello, actualice y modifique la instalación existente de Acronis Cyber Protect.

Pasos para añadir componentes para la instalación remota a una instalación existente

1. Descargue el archivo de instalación más reciente de Acronis Cyber Protect desde el sitio web de Acronis.

   Seleccione el archivo de instalación que corresponda con el valor de bits de su sistema operativo. En la mayoría de los casos, necesitará el archivo del programa de instalación de **Windows de 64 bits**. Para obtener más información sobre la instalación o actualización remota de un agente de protección en un equipo de 32 bits, consulte este artículo de la base de conocimientos.
2. En el equipo en el que se ejecuta el servidor de administración, inicie el archivo de instalación y seleccione **Actualizar**.
3. Cuando se complete la actualización, inicie de nuevo el archivo de instalación y seleccione **Modificar la instalación actual**.
4. Seleccione **Componentes para la instalación remota** y haga clic en **Listo**.

Cuando se complete la instalación, podrá instalar agentes de protección en equipos remotos desde la consola web de Cyber Protect.

Adición de un equipo que ejecute Linux

Solo puede añadir un equipo de Linux mediante la instalación local del agente de protección. La instalación remota no es compatible.

Pasos para añadir un equipo que ejecute Linux

1. En la consola web de Cyber Protect, haga clic en **Todos los dispositivos** > **Añadir**.
2. Haga clic en **Linux**.

   El programa de instalación se descargará en su equipo.
3. Ejecute el programa de instalación en el equipo que quiera proteger. Para obtener más información, consulte "Instalación en Linux" (p. 142).

Añadir un equipo que ejecute macOS

Solo puede añadir un equipo macOS mediante la instalación local del agente de protección. La instalación remota no es compatible.

Pasos para añadir un equipo que ejecute macOS

1. En la consola web de Cyber Protect, haga clic en **Todos los dispositivos** > **Añadir**.
2. Haga clic en **Mac**.

   El programa de instalación se descargará en su equipo.
3. Ejecute el programa de instalación en el equipo que quiera proteger. Para obtener más información, consulte "Instalación en macOS" (p. 143).

Adición de un servidor vCenter o ESXi

Existen cuatro métodos para añadir un servidor vCenter o ESXi independiente a un servidor de gestión:

- Implementación de Agente para VMware (dispositivo virtual)

  Este es el método recomendado en la mayoría de los casos. El dispositivo virtual se implementará automáticamente en cada servidor gestionado por el vCenter que indique. Puede seleccionar los servidores y personalizar la configuración del dispositivo virtual.
- Instalación de Agente para VMware (Windows)

  Puede que quiera instalar Agente para VMware en un equipo físico que ejecute Windows para obtener una copia de seguridad sin LAN o descargada.
  - **Copia de seguridad descargada**

    Utilice esta opción si sus servidores ESXi de producción están tan cargados que no sería deseable ejecutar dispositivos virtuales.
  - **Copia de seguridad sin LAN**

    Si su ESXi usa un almacenamiento conectado a SAN, instale el agente en un equipo conectado al mismo SAN. El agente realizará la copia de seguridad de los equipos virtuales directamente desde el almacenamiento en vez de mediante el servidor ESXi y LAN. Para obtener instrucciones detalladas, consulte la sección "Copia de seguridad sin LAN".

  Si el servidor de gestión se ejecuta en Windows, el agente se implementará automáticamente en el equipo que indique. De lo contrario, debe instalar el agente manualmente.
- Registro de un Agente para VMware ya instalado

  Se trata de un paso necesario una vez que haya reinstalado el servidor de gestión. También puede registrar y configurar el Agente para VMware (dispositivo virtual) implementado desde una plantilla de OVF.
- Configuración de un Agente para VMware ya registrado

  Se trata de un paso necesario una vez que haya instalado manualmente el Agente para VMware (Windows) o implementado el dispositivo Acronis Cyber Protect. Además, puede asociar un Agente para VMware ya configurado a otro vCenter Server o servidor ESXi independiente.

Implementación del Agente para VMware (dispositivo virtual) a través de la interfaz web

1. Haga clic en **Todos los dispositivos** > **Añadir**.
2. Haga clic en **VMware ESXi**.

3. Seleccione **Implementar como dispositivo virtual en cada servidor de vCenter**.
4. Especifique la dirección y las credenciales de acceso de vCenter Server o del servidor ESXi independiente. Le recomendamos utilizar una cuenta que tenga asignado el rol de **Administrador**. En otro caso, proporcione una cuenta con los privilegios necesarios en el servidor vCenter Server oESXi.
5. Seleccione el nombre o la dirección IP del servidor de administración que el agente utilizará para acceder a ese servidor.

   De forma predeterminada, se selecciona el nombre del servidor. Puede que deba seleccionar la dirección IP en su lugar si su servidor de administración tiene más de una interfaz de red o si está experimentando problemas de DNS que provocan que el registro del agente falle.
6. [Opcional] Haga clic en **Configuración** para personalizar la configuración de la implementación:
   - Los servidores ESXi en los que desea implementar el agente (solo si se indicó un vCenter Server en el paso anterior).
   - El nombre del dispositivo virtual.
   - El almacén de datos donde se ubicará el dispositivo.
   - El grupo de recursos o vApp que contendrá el dispositivo.
   - La red a la que se conectará el adaptador de red del dispositivo virtual.
   - Configuración de red del dispositivo virtual. Puede elegir la configuración automática de DHCP o especificar los valores de forma manual incluyendo una dirección IP estática.
7. Haga clic en **Implementar**.

Instalación de Agente para VMware (Windows)

Preparación

Siga los pasos preparatorios descritos en la sección "Adición de un equipo que ejecute Windows".

Instalación

1. Haga clic en **Todos los dispositivos** > **Añadir**.
2. Haga clic en **VMware ESXi**.
3. Seleccione **Instalar remotamente en un equipo que ejecute Windows**.
4. Seleccione el agente de implementación.
5. Especifique el nombre del servidor o la dirección IP del equipo de destino, y las credenciales de una cuenta con privilegios de administración en ese equipo.
6. Seleccione el nombre o la dirección IP del servidor de administración que el agente utilizará para acceder a ese servidor.

   De forma predeterminada, se selecciona el nombre del servidor. Puede que deba seleccionar la dirección IP en su lugar si su servidor de administración tiene más de una interfaz de red o si está experimentando problemas de DNS que provocan que el registro del agente falle.

7. Haga clic en **Conectar**.
8. Especifique la dirección y las credenciales del vCenter Server o servidor ESXi independiente y, a continuación, haga clic en **Conectar**. Le recomendamos utilizar una cuenta que tenga asignado el rol de **Administrador**. En otro caso, proporcione una cuenta con los privilegios necesarios en el servidor vCenter Server oESXi.
9. Haga clic en **Instalar** para instalar el agente.

Registro de un Agente para VMware ya instalado

Esta sección describe el registro de Agente para VMware a través de la interfaz web.

Métodos de registro alternativos:

- Puede registrar Agente para VMware (dispositivo virtual) especificando el servidor de gestión en la interfaz de usuario del dispositivo virtual. Consulte el paso 3 en "Configuración del dispositivo virtual" en la sección "Implementación del Agente para VMware (dispositivo virtual) desde una plantilla de OVF".
- Agente para VMware (Windows) se registra durante su instalación local.

Para registrar Agente para VMware

1. Haga clic en **Todos los dispositivos** > **Añadir**.
2. Haga clic en **VMware ESXi**.
3. Seleccione **Registrar un agente ya instalado**.
4. Seleccione el agente de implementación.
5. Si registra *Agente para VMware (Windows)*, especifique el nombre del servidor o la dirección IP del equipo donde se ha instalado el agente y las credenciales de una cuenta con privilegios de administración en ese equipo.

   Si registra *Agente para VMware (dispositivo virtual)*, especifique el nombre del servidor o la dirección IP del dispositivo virtual y las credenciales del vCenter Server o servidor ESXi independiente donde se ejecuta el dispositivo.
6. Seleccione el nombre o la dirección IP del servidor de administración que el agente utilizará para acceder a ese servidor.

   De forma predeterminada, se selecciona el nombre del servidor. Puede que deba seleccionar la dirección IP en su lugar si su servidor de administración tiene más de una interfaz de red o si está experimentando problemas de DNS que provocan que el registro del agente falle.
7. Haga clic en **Conectar**.
8. Especifique el nombre del servidor o la dirección IP del vCenter Server o servidor ESXi independiente y sus credenciales de acceso, y haga clic en **Conectar**. Le recomendamos utilizar una cuenta que tenga asignado el rol de **Administrador**. En otro caso, proporcione una cuenta con los privilegios necesarios en el servidor vCenter Server oESXi.
9. Haga clic en **Registrar** para registrar el agente.

Configuración de un Agente para VMware ya registrado

En esta sección se describe cómo asociar el Agente para VMware con un servidor vCenter Server o ESXi en la interfaz web. Como alternativa, puede hacer esto mismo en la consola del Agente para VMware (dispositivo virtual).

Mediante este procedimiento, también puede cambiar la asociación existente del agente a un servidor vCenter Server o ESXi. Como alternativa, puede llevar esta operación a cabo en la consola del Agente para VMware (dispositivo virtual), o bien haciendo clic en **Configuración** > **Agentes** > el agente > **Detalles** > **vCenter/ESXi**.

Para configurar un Agente para VMware

1. Haga clic en **Todos los dispositivos** > **Añadir**.
2. Haga clic en **VMware ESXi**.
3. El software muestra el Agente para VMware no configurado que aparece en primer lugar por orden alfabético.

   Si todos los agentes registrados en el servidor de gestión están configurados, haga clic en **Configurar un agente ya registrado**, y el software mostrará el agente que aparece en primer lugar por orden alfabético.
4. Si es necesario, haga clic en **Equipos con agentes** y seleccione el agente que desea configurar.
5. Especifique o cambie el nombre de servidor o dirección IP del vCenter Server o servidor ESXi, y sus credenciales de acceso. Le recomendamos utilizar una cuenta que tenga asignado el rol de **Administrador**. En otro caso, proporcione una cuenta con los privilegios necesarios en el servidor vCenter Server oESXi.
6. Haga clic en **Configurar** para guardar los cambios.

Añadir un clúster de Scale Computing HC3

Para añadir un clúster de Scale Computing HC3 al servidor de gestión Cyber Protect

1. Implementación de Agent para Scale Computing HC3 (dispositivo virtual) en el clúster.
2. Configure su conexión tanto para este clúster como para el servidor de gestión Cyber Protect.

Instalación de agentes localmente

Instalación en Windows

Para instalar Agente para Windows, Agente para Hyper-V, Agent for Exchange, Agente para SQL o Agente para Active Directory

1. Inicie sesión como administrador e inicie el programa de instalación de Acronis Cyber Protect.
2. [Opcional] Para cambiar el idioma del programa de instalación, haga clic en **Idioma de instalación**.

3. Acepte los términos del acuerdo de licencia y la declaración de privacidad y, a continuación, haga clic en **Siguiente**.
4. Seleccione **Instalar un agente de protección**.
5. Realice una de las siguientes operaciones:
   - Haga clic en **Instalar**.

     Esta es la forma más sencilla de instalar el producto. La mayoría de los parámetros de instalación se establecerán en sus valores predeterminados.

     Se instalarán los componentes siguientes:
     - Agente para Windows
     - Otros agentes (Agente para Hyper-V, Agent for Exchange, Agente para SQL y Agente para Active Directory), si se detecta el respectivo hipervisor o aplicación en el equipo
     - Bootable Media Builder
     - Herramienta de línea de comandos
     - Cyber Protect Monitor
   - Haga clic en **Personalizar los ajustes de instalación** para realizar la configuración.

     Podrá seleccionar los componentes que desea instalar y especificar parámetros adicionales. Para obtener más información, consulte "Personalización de los ajustes de instalación" (p. 106).
   - Haga clic en **Crear archivos .mst y .msi para una instalación sin supervisión** para extraer los paquetes de instalación. Compruebe o modifique la configuración de instalación que se añadirá al archivo .mst y haga clic en **Generar**. No se requieren más pasos para este procedimiento.

     Si desea implementar agentes mediante una directiva de grupo, siga el procedimiento descrito en "Implementación de agentes mediante la directiva de grupo" (p. 220).
6. Especifique el servidor de gestión en el que se registrará el equipo con el agente:
   a. Especifique el nombre del servidor o la dirección IP del equipo donde está instalado el servidor de gestión.
   b. Especifique las credenciales de un administrador del servidor de gestión o un token de registro.

      Para obtener más información sobre cómo generar un token de registro, consulte "Paso 1: Generar un token de registro" (p. 221).
   c. Haga clic en **Realizado**.
7. Si se le pregunta, seleccione si desea que el equipo con el agente se añada a la organización o a una de sus unidades.

   Este mensaje aparece si ha administrado más de una unidad o una organización con al menos una unidad. De lo contrario, el equipo se añadirá silenciosamente a la unidad que administra o a la organización. Para obtener más información, consulte "Unidades y cuentas administrativas" (p. 710).

8. Continúe con la instalación.
9. Cuando haya terminado la instalación, haga clic en **Cerrar**.
10. Si ha instalado Agent for Exchange, podrá realizar la copia de seguridad de bases de datos de Exchange. Si desea realizar la copia de seguridad de buzones de correo de Exchange, abra la consola web de Cyber Protect, haga clic en **Añadir** > **Microsoft Exchange Server** > **Buzones de correo de Exchange** y especifique el equipo en el que esté habilitado el rol **Servidor de acceso de cliente** (CAS) de Microsoft Exchange Server. Para obtener más información, consulte "Copia de seguridad de casillas de correo" (p. 509).

Para instalar el Agente para VMware (Windows), Agente para Office 365, Agent for Oracle o Agent for Exchange en un equipo sin Microsoft Exchange Server

1. Inicie sesión como administrador e inicie el programa de instalación de Acronis Cyber Protect.
2. [Opcional] Para cambiar el idioma del programa de instalación, haga clic en **Idioma de instalación**.
3. Acepte los términos del acuerdo de licencia y la declaración de privacidad y, a continuación, haga clic en **Siguiente**.
4. Seleccione **Instalar un agente de protección** y haga clic en **Personalizar los ajustes de instalación**.
5. Junto a **Qué instalar**, haga clic en **Cambiar**.
6. Active la casilla de verificación del agente que desea instalar. Desactive las casillas de verificación de los componentes que no desea instalar. Haga clic en **Realizado** para continuar.
7. Especifique el servidor de gestión en el que se registrará el equipo con el agente:
   a. Junto a **Acronis Cyber Protect Management Server**, haga clic en **Especificar**.
   b. Especifique el nombre del servidor o la dirección IP del equipo donde está instalado el servidor de gestión.
   c. Especifique las credenciales de un administrador del servidor de gestión o un token de registro.
      Para obtener más información sobre cómo generar un token de registro, consulte "Paso 1: Generar un token de registro" (p. 221).
   d. Haga clic en **Realizado**.
8. Si se le pregunta, seleccione si desea que el equipo con el agente se añada a la organización o a una de sus unidades.
   Este mensaje aparece si ha administrado más de una unidad o una organización con al menos una unidad. De lo contrario, el equipo se añadirá silenciosamente a la unidad que administra o a la organización. Para obtener más información, consulte "Unidades y cuentas administrativas" (p. 710).
9. [Opcional] Cambie otros ajustes de la instalación según se describe en "Personalización de los ajustes de instalación" (p. 106).
10. Haga clic en **Instalar** para proceder con la instalación.

11. Cuando haya terminado la instalación, haga clic en **Cerrar**.
12. [Solo al instalar el Agente para VMware (Windows)] Siga el procedimiento descrito en la sección "Configuración de un Agente para VMware ya registrado" (p. 139).
13. [Solo al instalar Agent for Exchange] Abra la consola web de Cyber Protect, haga clic en **Añadir** > **Microsoft Exchange Server** > **Buzones de correo de Exchange** y especifique el equipo en el que esté habilitado el rol **Servidor de acceso de cliente** (CAS) de Microsoft Exchange Server. Para obtener más información, consulte "Copia de seguridad de casillas de correo" (p. 509).

Instalación en Linux

Preparación

1. Asegúrese de que los paquetes de Linux necesarios se han instalado en el equipo.
2. Al instalar el agente en SUSE Linux, asegúrese de utilizar `su -` en lugar de `sudo`. De lo contrario, ocurre el siguiente error al intentar registrar el agente a través de la consola web de Cyber Protect: `Error al iniciar el navegador web. No hay ninguna visualización que mostrar.` Algunas distribuciones de Linux, como SUSE, no pasan la variable `DISPLAY` cuando se utiliza `sudo`, y el programa de instalación no puede abrir el navegador en la interfaz gráfica de usuario (GUI).

Instalación

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

Para instalar Agente para Linux

1. Como el usuario raíz, vaya al directorio con el archivo de instalación (.i686 or .x86_64 file), haga el archivo ejecutable y ejecútelo.

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

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

2. Acepte los términos del acuerdo de licencia.
3. Especifique los componentes que desee instalar:
   a. Seleccione la casilla de verificación **Acronis Cyber Protect Management Server**.
   b. Seleccione las casillas de verificación de los agentes que desea instalar. Los agentes disponibles son los siguientes:
      - **Agente para Linux**
      - **Agent para Oracle**

      Agent for Oracle requiere que el Agente para Linux esté instalado.
   c. Haga clic en **Siguiente**.
4. Especifique el servidor de gestión en el que se registrará el equipo con el agente:

a. Especifique el nombre del servidor o la dirección IP del equipo donde está instalado el servidor de gestión.
b. Especifique el nombre de usuario y la contraseña del administrador del servidor de gestión.
c. Haga clic en **Siguiente**.

5. Si se le pregunta, seleccione si desea que el equipo con el agente se añada a la organización o a una de sus unidades, y pulse **Intro**.
   Este mensaje aparece si la cuenta especificada en el paso anterior administra más de una unidad o una organización con al menos una unidad.
6. Si el arranque seguro UEFI se habilita en el equipo, se le informará de que debe reiniciar el sistema tras la instalación. Asegúrese de que recuerda qué contraseña (la del usuario raíz o "acronis") debe utilizar.

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

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

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

Instalación en macOS

Para instalar Agente para Mac

1. Haga doble clic sobre el archivo de instalación (.dmg).
2. Espere mientras el sistema operativo monta la imagen del disco de instalación.
3. Haga doble clic en **Instalar** y, a continuación, haga clic en **Continuar**.
4. [Opcional] Haga clic en **Cambiar ubicación de instalación** para cambiar el disco en el que se instalará el software. De forma predeterminada, se selecciona el disco de inicio del sistema.
5. Haga clic en **Instalar**. Si se le solicita, introduzca el nombre de usuario y la contraseña del administrador.
6. Especifique el servidor de gestión en el que se registrará el equipo con el agente:
   a. Especifique el nombre del servidor o la dirección IP del equipo donde está instalado el servidor de gestión.

b. Especifique el nombre de usuario y la contraseña del administrador del servidor de gestión.

c. Haga clic en **Registrar**.

7. Si se le pregunta, seleccione si desea que el equipo con el agente se añada a la organización o a una de sus unidades, y haga clic en **Finalizado**.
   Este mensaje aparece si la cuenta especificada en el paso anterior administra más de una unidad o una organización con al menos una unidad.
8. Cuando haya terminado la instalación, haga clic en **Cerrar**.

Instalación o desinstalación sin supervisión

Instalación o desinstalación sin supervisión en Windows

En esta sección se describe cómo instalar o desinstalar Acronis Cyber Protect en el modo de interacción en un equipo que ejecute Windows, o mediante Windows Installer (el programa `msiexec`). En un dominio de Active Directory, otra manera de realizar una instalación sin supervisión es a través de una directiva de grupo. Consulte "Implementación de agentes mediante la directiva de grupo" (p. 220).

Durante la instalación, puede utilizar un archivo conocido como una **transformación** (un archivo .mst). Una transformación es un archivo con parámetros de instalación. Como alternativa, puede especificar los parámetros de instalación directamente en la línea de comando.

Creación de la transformación .mst y extracción de los paquetes de instalación

1. Inicie sesión como administrador e inicie el programa de instalación.
2. Haga clic en **Crear archivos .mst y .msi para una instalación sin supervisión**.
3. [No disponible en todos los programa de instalación] En **Valor de bits del componente**, seleccione **32 bits** o **64 bits**.
4. En **Qué instalar**, seleccione los componentes que desea instalar y haga clic en **Listo**.
   Los paquetes de instalación de estos componentes se extraerán del programa de instalación.
5. En **Acronis Cyber ProtectManagement Server**, seleccione **Usar credenciales** o **Usar token de registro**. Según lo que elija, especifique las credenciales o el token de registro y haga clic en **Listo**.
   Para obtener más información sobre cómo generar un token de registro, consulte "Paso 1: Generar un token de registro" (p. 221).
6. [Solamente cuando instale en un controlador de dominio] En **Cuenta de inicio de sesión para el servicio de agente**, seleccione **Utilizar la siguiente cuenta**. Especifique la cuenta de usuario en la que se ejecutará el servicio de agente. Después, haga clic en **Listo**. Por razones de seguridad, el programa de instalación no crea automáticamente nuevas cuentas en un controlador de dominio.

Nota

A la cuenta de usuario que especifique se le debe conceder el privilegio `Iniciar sesión como un servicio`.

Esta cuenta ya debe haberse usado en el controlador de dominio para que se cree su carpeta de perfiles en dicho equipo.

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

7. Compruebe o modifique otros ajustes de la instalación que se añadirá al archivo .mst y haga clic en **Continuar**.
8. Seleccione la carpeta en la que se generará la transformación .mst y los paquetes de instalación .msi y .cab se extraerán y, a continuación, haga clic en **Generar**.

Como resultado, se genera la transformación .mst y los paquetes de instalación .msi y .cab se extraen a la carpeta especificada.

Instalación del producto mediante la transformación .mst

En la línea de comandos, ejecute el siguiente comando:

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

Donde:

- <package name> es el nombre del archivo .msi. Este nombre es **AB.msi** o **AB64.msi**, dependiendo de los bits del sistema operativo.
- <transform name> es el nombre de la transformación. Este nombre es **AB.msi.mst** o **AB64.msi.mst**, dependiendo de los bits de sistema operativo.

Por ejemplo, `msiexec /i AB64.msi TRANSFORMS=AB64.msi.mst`

Instalación o desinstalación del producto especificando parámetros manualmente

En la línea de comandos, ejecute el siguiente comando:

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

Aquí, <package name> es el nombre del archivo .msi. Este nombre es **AB.msi** o **AB64.msi**, dependiendo de los bits del sistema operativo.

Los parámetros disponibles y sus valores se describen en "Parámetros comunes" (p. 146).

Ejemplos

- Instalación del servidor de gestión y componentes para una instalación remota.

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

- Instalación del Agente para Windows, la herramienta de línea de comandos y Cyber Protect Monitor. Registro del equipo con el agente en un servidor de gestión instalado previamente.

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

- Actualizar el servidor de gestión, el nodo de almacenamiento, el servicio de catálogo y el agente de protección.

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

Parámetros de instalación o desinstalación sin supervisión

Esta sección describe parámetros utilizados en una instalación o desinstalación sin supervisión en Windows.

Además de estos parámetros, puede utilizar otros parámetros de `msiexec`, como se describe en https://msdn.microsoft.com/en-us/library/windows/desktop/aa367988(v=vs.85).aspx.

Parámetros de instalación

Parámetros comunes

`ADDLOCAL=<list of components>`

Los componentes que se van a instalar, separados con comas sin espacios. Todos los componentes especificados deben extraerse del programa de instalación antes de realizar la instalación.

La lista completa de componentes es la siguiente.

Componente	Debe instalarse junto con	Número de bits	Nombre o descripción del componente
AcronisCentralizedManagementServer	WebConsole	32 bits / 64 bits	Servidor de gestión

WebConsole	AcronisCentralizedManagementServer	32 bits / 64 bits	Consola web
ComponentRegisterFeature	AcronisCentralizedManagementServer	32 bits / 64 bits	Componentes para la instalación remota
AtpScanService	AcronisCentralizedManagementServer	32 bits / 64 bits	Scan Service
AgentsCoreComponents		32 bits / 64 bits	Componentes fundamentales de los agentes
BackupAndRecoveryAgent	AgentsCoreComponents	32 bits / 64 bits	Agente para Windows
ArxAgentFeature	BackupAndRecoveryAgent	32 bits / 64 bits	Agente para Exchange
ArsAgentFeature	BackupAndRecoveryAgent	32 bits / 64 bits	Agente para SQL
ARADAgentFeature	BackupAndRecoveryAgent	32 bits / 64 bits	Agente para Active Directory
OracleAgentFeature	BackupAndRecoveryAgent	32 bits / 64 bits	Agent para Oracle
ArxOnlineAgentFeature	AgentsCoreComponents	32 bits / 64 bits	Agente para Office 365
AcronisESXSupport	AgentsCoreComponents	32 bits / 64 bits	Agente para VMware (Windows)
HyperVAgent	AgentsCoreComponents	32 bits / 64 bits	Agente para Hyper-V
ESXVirtualAppliance		32 bits / 64 bits	Agente para VMware (dispositivo virtual)
ScaleVirtualAppliance		32 bits / 64 bits	Agent para Scale Computing

			HC3 (dispositivo virtual)
CommandLineTool		32 bits / 64 bits	Herramienta de línea de comandos
TrayMonitor	BackupAndRecoveryAgent	32 bits / 64 bits	Cyber Protect Monitor
BackupAndRecoveryBootableComponents		32 bits / 64 bits	Bootable Media Builder
ServidorPXE		32 bits / 64 bits	PXE Server
Servidor de almacenamiento	BackupAndRecoveryAgent	64 bits	Nodo de almacenamiento
CatalogBrowser	JRE 8 Update 111 o posterior	64 bits	Servicio de catálogo

`TARGETDIR=<path>`

La carpeta donde se instalará el producto.

`REBOOT=ReallySuppress`

Si se especifica el parámetro, se prohíbe el reinicio del equipo.

`CURRENT_LANGUAGE=<language ID>`

El idioma del producto. Los valores disponibles son: `en`, `en_GB`, `cs`, `da`, `de`, `es_ES`, `fr`, `ko`, `it`, `hu`, `nl`, `ja`, `pl`, `pt`, `pt_BR`, `ru`, `tr`, `zh`, `zh_TW`.

`ACEP_AGREEMENT={0,1}`

Si el valor es `1`, el equipo participará en el Programa de Experiencia del Cliente (PECA) de Acronis.

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

El nombre del servidor o la dirección IP del equipo en el que está instalado el servidor de gestión. Los agentes, el nodo de almacenamiento y el servicio de catalogación especificados en el parámetro `ADDLOCAL` se registrarán en este servidor de gestión. El número del puerto es obligatorio si es distinto al valor predeterminado (9877).

Con este parámetro, debe especificar el parámetro `REGISTRATION_TOKEN`, o los parámetros `REGISTRATION_LOGIN` y `REGISTRATION_PASSWORD`.

`REGISTRATION_TOKEN=<token>`

Token de registro que se generó en la consola web de Cyber Protect, como se indica en Implementación de agentes mediante la directiva de grupo.

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

Nombre de usuario y contraseña del administrador del servidor de gestión.

`REGISTRATION_TENANT=<unit ID>`

La unidad dentro de la organización. Los agentes, el nodo de almacenamiento y el servicio de catalogación especificados en el parámetro `ADDLOCAL` se añadirán a esta unidad.

Para averiguar el ID de una unidad, en la consola web de Cyber Protect haga clic en **Configuración** > **Cuentas**, seleccione la unidad y haga clic en **Detalles**.

Este parámetro no funciona sin `REGISTRATION_TOKEN` o `REGISTRATION_LOGIN` y `REGISTRATION_PASSWORD`. En este caso, los componentes se añadirán a la organización.

Sin este parámetro, los componentes se añadirán a la organización.

`REGISTRATION_REQUIRED={0,1}`

La instalación tendrá lugar en caso de que falle el registro. Si el valor es `1`, la instalación da error. Si el valor es `0`, la instalación se lleva a cabo correctamente aunque el componente no se haya registrado.

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

Estos parámetros mutuamente excluyentes definen el método de comprobación del certificado del servidor de gestión durante el registro. Compruebe el certificado si quiere verificar la autenticidad del servidor de gestión para evitar ataques de intermediario.

Si el valor es `1`, la verificación usa la CA del sistema o el paquete de la CA proporcionado con el producto, como corresponda. Si se especifica una clave pública anclada, la verificación emplea dicha clave. Si el valor es `0` o no están especificados los parámetros, no se lleva a cabo la verificación del certificado, pero el tráfico de registro se mantiene cifrado.

`/l*v <log file>`

Si se especifica el parámetro, el registro de instalación en modo detallado se guardará en el archivo especificado. El archivo de registro se puede utilizar para analizar problemas de instalación.

Parámetros de instalación del servidor de gestión

`WEB_SERVER_PORT=<port number>`

El puerto que utilizarán los navegadores web para acceder al servidor de gestión. El valor predeterminado es 9877.

`AMS_ZMQ_PORT=<port number>`

El puerto que se utilizará para la comunicación entre los componentes del producto. El valor predeterminado es 7780.

`SQL_INSTANCE=<instance>`

La base de datos que debe utilizar el servidor de gestión. Puede seleccionar cualquier edición de Microsoft SQL Server 2012, Microsoft SQL Server 2014 o Microsoft SQL Server 2016. La instancia que escoja se puede usar también en otros programas.

Sin este parámetro, se utilizará la base de datos SQLite integrada.

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

Credenciales de una cuenta de acceso a Microsoft SQL Server El servidor de gestión utilizará estas credenciales para establecer una conexión con la instancia de SQL Server seleccionada. Sin estos parámetros, el servidor de gestión utilizará las credenciales de la cuenta de servicio del servidor de gestión (**AMS User**).

Cuenta con la que se ejecutará el servicio del servidor de gestión

Especifique alguno de los parámetros siguientes:

- `AMS_USE_SYSTEM_ACCOUNT={0,1}`

  Si el valor es `1`, se utilizará la cuenta del sistema.
- `AMS_CREATE_NEW_ACCOUNT={0,1}`

  Si el valor es `1`, se creará una nueva cuenta.
- `AMS_SERVICE_USERNAME=<user name>` y `AMS_SERVICE_PASSWORD=<password>`

  Se utilizará la cuenta especificada.

Parámetros de instalación del agente

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

Servidor proxy HTTP que utilizará el agente. Sin estos parámetros, no se utilizará ningún servidor proxy.

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

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

`HTTP_PROXY_ONLINE_BACKUP={0,1}`

Si el valor es `0`, o el parámetro no está especificado, el agente usará el servidor proxy únicamente para realizar copias de seguridad y recuperaciones desde el cloud. Si el valor es `1`, el agente también se conectará al servidor de gestión a través del servidor proxy.

`SET_ESX_SERVER={0,1}`

Si el valor es `0`, el Agent for VMware que se esté instalando no se conectará al vCenter Server ni al servidor ESXi. Tras finalizar la instalación, realice los pasos descritos en «Configuración de un Agente para VMware ya registrado".

Si el valor es 1, especifique los siguientes parámetros:

`ESX_HOST=<host name or IP address>`

El nombre del servidor o dirección IP del vCenter Server o servidor ESXi.

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

Credenciales para acceder al vCenter Server o al servidor ESXi.

Cuenta con la que se ejecutará el servicio de agente

Especifique alguno de los parámetros siguientes:

- `MMS_USE_SYSTEM_ACCOUNT={0,1}`
  Si el valor es 1, se utilizará la cuenta del sistema.
- `MMS_CREATE_NEW_ACCOUNT={0,1}`
  Si el valor es 1, se creará una nueva cuenta.
- `MMS_SERVICE_USERNAME=<user name>` y `MMS_SERVICE_PASSWORD=<password>`
  Se utilizará la cuenta especificada.

Parámetros de instalación del nodo de almacenamiento

Cuenta con la que se ejecutará el servicio del nodo de almacenamiento

Especifique alguno de los parámetros siguientes:

- `ASN_USE_SYSTEM_ACCOUNT={0,1}`
  Si el valor es 1, se utilizará la cuenta del sistema.
- `ASN_CREATE_NEW_ACCOUNT={0,1}`
  Si el valor es 1, se creará una nueva cuenta.
- `ASN_SERVICE_USERNAME=<user name>` y `ASN_SERVICE_PASSWORD=<password>`
  Se utilizará la cuenta especificada.

Parámetros de instalación del servicio de catálogo

`CATALOG_DATA_MIGRATION_PATH=<path>`

Utilice este parámetro para migrar los datos de catálogo a la nueva versión del servicio de catálogo de Acronis Cyber Protect 15, actualización 4. Especifique la ruta a la carpeta temporal a la que se exportarán los datos del catálogo.

`SKIP_CATALOG_DATA_MIGRATION=1`

Utilice este parámetro para omitir la migración de los datos del catálogo.

Los parámetros `SKIP_CATALOG_DATA_MIGRATION` y `CATALOG_DATA_MIGRATION_PATH` se excluyen mutuamente.

Parámetros de desinstalación

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

Los componentes que se van a eliminar, separados con comas sin espacios.

Los componentes disponibles se han descrito anteriormente en esta sección.

Si el valor es `ALL`, se desinstalarán todos los componentes del producto. Además, puede especificar el parámetro siguiente:

`DELETE_ALL_SETTINGS={0, 1}`

Si el valor es `1`, se eliminarán los registros, tareas y ajustes de configuración del producto.

Instalación o desinstalación sin supervisión en Linux

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

Para instalar o desinstalar el producto

1. Abra el Terminal.
2. Ejecute el siguiente comando:

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

   Donde `<package name>` es el nombre del paquete de instalación (un archivo .i686 o .x86_64).
3. [Solo cuando se instala Agente para Linux] Si el arranque seguro UEFI se habilita en el equipo, se le informará de que debe reiniciar el sistema tras la instalación. Asegúrese de que recuerda qué contraseña (la del usuario raíz o "acronis") debe utilizar. Durante el reinicio del sistema, opte por la gestión de MOK (clave del propietario del equipo), seleccione **Registrar MOK** y, a continuación, registre la clave por medio de la contraseña recomendada.

Si habilita el arranque seguro UEFI después de la instalación del agente, repita la instalación, incluido el paso 3. En caso contrario, las copias de seguridad fallarán.

Parámetros de instalación

Parámetros comunes

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

Los componentes que se van a instalar, separados con comas sin espacios.

Los siguientes componentes están disponibles para la instalación:

Componente	Descripción de componentes
AcronisCentralizedManagementServer	Servidor de gestión
BackupAndRecoveryAgent	Agente para Linux
BackupAndRecoveryBootableComponents	Bootable Media Builder

Sin este parámetro, se instalarán todos los componentes anteriores.

`--language=<language ID>`

El idioma del producto. Los valores disponibles son: `en`, `en_GB`, `cs`, `da`, `de`, `es_ES`, `fr`, `ko`, `it`, `hu`, `nl`, `ja`, `pl`, `pt`, `pt_BR`, `ru`, `tr`, `zh`, `zh_TW`.

`{-d|--debug}`

Si se especifica el parámetro, el registro de instalación se escribe en modo detallado. El registro se encuentra en el archivo **/var/log/trueimage-setup.log**.

`{-t|--strict}`

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

`{-n|--nodeps}`

Si se especifica el parámetro, se omitirá la ausencia de paquetes de Linux requeridos durante la instalación.

Parámetros de instalación del servidor de gestión

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

El puerto que utilizarán los navegadores web para acceder al servidor de gestión. El valor predeterminado es 9877.

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

El puerto que se utilizará para la comunicación entre los componentes del producto. El valor predeterminado es 7780.

Parámetros de instalación del agente

Especifique alguno de los parámetros siguientes:

- `--skip-registration`
  - No registra el agente en el servidor de gestión.
- `{-C |--ams=}<host name or IP address>`
  - El nombre del servidor o la dirección IP del equipo en el que está instalado el servidor de gestión. El agente se registrará en este servidor de gestión.

    Si instala el agente y el servidor de gestión con un comando, el agente se registrará en este servidor de gestión independientemente del parámetro `-C`.

    Con este parámetro, debe especificar el parámetro `token`, o los parámetros `login` y `password`.

    `--token=<token>`

Token de registro que se generó en la consola web de Cyber Protect, como se indica en Implementación de agentes mediante la directiva de grupo.

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

Credenciales de un administrador del servidor de gestión.

`--unit=<unit ID>`

La unidad dentro de la organización. El agente se añadirá a esta unidad.

Para averiguar el ID de una unidad, en la consola web de Cyber Protect haga clic en **Configuración** > **Cuentas**, seleccione la unidad y haga clic en **Detalles**.

Sin este parámetro, el agente se añadirá a la organización.

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

Método de comprobación del certificado del servidor de gestión durante el registro. Compruebe el certificado si quiere verificar la autenticidad del servidor de gestión para evitar ataques de intermediario.

Si el valor es `https` o no está especificado el parámetro, no se lleva a cabo la comprobación del certificado, pero el tráfico de registro se mantiene cifrado. Si el valor *no* es `https`, la comprobación usa la CA del sistema o el paquete de la CA proporcionado con el producto, o bien la clave pública anclada, de forma correspondiente.

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

Valor de la clave pública anclada. Este parámetro se debe especificar junto con el parámetro `--reg-transport=https-pinned-public-key` o en lugar de este.

- `--http-proxy-host=<IP address>` y `--http-proxy-port=<port>`
  - El servidor proxy HTTP que el agente usará para realizar la copia de seguridad y la recuperación desde el cloud y para establecer la conexión al servidor de gestión. Sin estos parámetros, no se utilizará ningún servidor proxy.
- `--http-proxy-login=<login>` y `--http-proxy-password=<password>`
  - Credenciales del servidor proxy HTTP. Utilice estos parámetros si el servidor necesita autenticación.
- `--no-proxy-to-ams`
  - El agente de protección se conectará al servidor de gestión sin usar el servidor proxy especificado en los parámetros `--http-proxy-host` y `--http-proxy-port`.

Parámetros de desinstalación

`{-u|--uninstall}`

Desinstala el producto.

`--purge`

Elimina los registros, tareas y ajustes del producto.

Parámetros de información

`{-?|--help}`

Muestra descripción de los parámetros.

`--usage`

Muestra una breve descripción del uso del comando.

`{-v|--version}`

Muestra la versión del paquete de instalación.

`--product-info`

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

Ejemplos

- Instalación del servidor de gestión.

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

- Instalación de Management Server especificando puertos personalizados.

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

- Instalación del Agente para Linux y su registro en el servidor de gestión especificado.

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

- Instalación del Agente para Linux y su registro en el servidor de gestión especificado, en la unidad indicada.

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

Instalación o desinstalación sin supervisión en macOS

En esta sección se describe cómo instalar, registrar y desinstalar el agente de protección en el modo de interacción en un equipo que ejecute macOS mediante una línea de comando. Para obtener información sobre cómo descargar el archivo de instalación (.dmg), consulte "Añadir un equipo que ejecute macOS".

Para instalar Agente para Mac

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

   ```
   mkdir <dmg_root>
   ```

   Aquí, <dmg_root> es un nombre de su elección.
2. Monte el archivo .dmg.

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

   Aquí, <dmg_file> es el nombre del archivo de instalación. Por ejemplo, **AcronisCyberProtect_15_MAC.dmg**.
3. Ejecute el programa de instalación.

   ```
   sudo installer -pkg <dmg_root>/Install.pkg -target LocalSystem
   ```
4. Desconecte el archivo de instalación (.dmg).

   ```
   hdiutil detach <dmg_root>
   ```

Ejemplos

- ```
  mkdir mydirectory
  ```

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

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

  ```
  hdiutil detach mydirectory
  ```

Para registrar Agente para Mac

Realice uno de los siguientes procedimientos:

- Registre el agente en una cuenta de administrador específica.

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

  La <management server address:port> es el nombre del servidor o la dirección IP del equipo en el que está instalado Acronis Cyber Protect Management Server. El número del puerto es obligatorio si es distinto al predeterminado (9877).

  El <user name> y la <password> son las credenciales para la cuenta de administrador en la que se registrará el agente.
- Registre el agente en una unidad específica.
  ```

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

Para averiguar el ID de la unidad, en la consola web de Cyber Protect haga clic en **Configuración** > **Cuentas**, seleccione la unidad que desee y haga clic en **Detalles**.

Importante
Los administradores solo pueden registrar agentes especificando el ID de la unidad en su nivel de la jerarquía organizativa. Los administradores de la unidad pueden registrar equipos en sus unidades y subunidades. Los administradores de la organización pueden registrar equipos en todas las unidades. Para obtener más información sobre las diferentes cuentas de administrador, consulte "Administración de cuentas de usuario y unidades de organización".

- Registre el agente mediante un token de registro.

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

El token de registro es una serie de 12 caracteres separados en tres segmentos por guiones. Puede generar uno en la consola web de Cyber Protect como se describe en "Implementación de agentes mediante la directiva de grupo".

Importante
En macOS 10.14 o posteriores, debe conceder acceso completo al disco al agente de protección. Para hacerlo, vaya a **Aplicaciones** >**Utilidades**, y ejecute el **Asistente para el agente de Cyber Protect**. A continuación, siga las instrucciones de la ventana de la aplicación.

Ejemplos

Registro con un nombre de usuario y una contraseña.

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

Registro con un ID de unidad y credenciales de administrador.

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

Registro con un token.

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

Para desinstalar Agente para Mac

Ejecute el siguiente comando:

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

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

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

Registro y anulación de registro manual de equipos

Los equipos se registran automáticamente en el servidor de administración cuando instala en ellas el agente de protección. Cuando desinstale el agente de protección, se anulará automáticamente el registro de los equipos y desaparecerán de la consola web de Cyber Protect.

También puede registrar un equipo manualmente mediante la interfaz de líneas de comando. Es posible que deba usar el registro manual, por ejemplo, si falla el registro automático o si quiere registrar un equipo existente en una cuenta de usuario nueva.

Puede encontrar la herramienta de registro en las siguientes ubicaciones:

- Windows: `Archivos de Programa\Acronis\RegisterAgentTool\register_agent.exe`
- Linux: `/usr/lib/Acronis/RegisterAgentTool/RegisterAgent`
- macOS: `/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent`

Para registrar un equipo con un nombre de usuario y una contraseña

En Windows

En la línea de comando, ejecute el siguiente comando:

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

Por ejemplo:

```
"C:\Program Files\BackupClient\RegisterAgentTool\register_agent.exe" -o register -a
https://10.250.144.179:9877 -u johndoe -p johnspassword
```

En Linux
```

En la línea de comando, ejecute el siguiente comando:

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -a <management
server address:port> -u <user name> -p <password>
```

Por ejemplo:

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

En macOS

En la línea de comando, ejecute el siguiente comando:

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

Por ejemplo:

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

<management server address:port> es el nombre de host o la dirección IP del equipo en el que está instalado el servidor de administración. Si utiliza el puerto predeterminado 9877, puede omitir especificarlo en este comando.

El <user name> y la <password> son las credenciales de la cuenta bajo la que se registrará el agente. Si la contraseña contiene caracteres especiales o espacios en blanco, consulte "Contraseñas con caracteres especiales o espacios en blanco" (p. 162).

Para registrar un equipo en una unidad específica con un nombre de usuario y una contraseña

En Windows

En la línea de comando, ejecute el siguiente comando:

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

Por ejemplo:

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

En Linux

En la línea de comando, ejecute el siguiente comando:

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

Por ejemplo:

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

En macOS

En la línea de comando, ejecute el siguiente comando:

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

Por ejemplo:

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

<management server address:port> es el nombre de host o la dirección IP del equipo en el que está instalado el servidor de administración. Si utiliza el puerto predeterminado 9877, puede omitir especificarlo en este comando.

El <user name> y la <password> son las credenciales de la cuenta bajo la que se registrará el agente. Si la contraseña contiene caracteres especiales o espacios en blanco, consulte "Contraseñas con caracteres especiales o espacios en blanco" (p. 162).

Para comprobar el ID de la unidad, en la consola web de Cyber Protect, vaya a **Configuración** > **Cuentas**. Seleccione la unidad que necesite y, a continuación, haga clic en **Detalles**.

Importante
Solo puede registrar agentes en su nivel de la jerarquía de la organización. Los administradores de unidad pueden registrar agentes en sus propias unidades y sus subunidades. Los administradores de la organización pueden registrar agentes en todas las unidades. Para obtener más información sobre las distintas cuentas de administrador, consulte "Administración de cuentas de usuario y unidades de organización" (p. 710).

Pasos para registrar un equipo mediante un token de registro:

En Windows

En la línea de comando, ejecute el siguiente comando:

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


Por ejemplo:

```
"C:\Program Files\BackupClient\RegisterAgentTool\register_agent.exe" -o register -a
https://10.250.144.179:9877 --token 3B4C-E967-4FBD
```

En Linux

En la línea de comando, ejecute el siguiente comando:

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

Por ejemplo:

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

En macOS

En la línea de comando, ejecute el siguiente comando:

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

Por ejemplo:

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

Pasos para desregistrar un equipo

En Windows

En la línea de comando, ejecute el siguiente comando:

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

Por ejemplo:

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

En Linux

En la línea de comando, ejecute el siguiente comando:

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

Por ejemplo:

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

En macOS

En la línea de comando, ejecute el siguiente comando:

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

Por ejemplo:

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

Contraseñas con caracteres especiales o espacios en blanco

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

Implementación local

- Plantilla de comando

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

- Windows

  ```
  "C:\Program Files\BackupClient\RegisterAgentTool\register_agent.exe" -o register –a
  https://10.250.144.179:9877 -u johndoe -p "johnspassword"
  ```

- Linux

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

- macOS

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

Implementación en la nube

- Plantilla de comando

  ```
  <path to the registration tool> -o register -t cloud -a <service address> -u <user
  name> -p <"password">
  ```

- Windows

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

- Linux

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

- macOS

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

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

Implementación local

- Plantilla de comando

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

- Windows

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

- Linux

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -a
https://10.250.144.179:9877 -u johndoe -b -p am9obnNwYXNzd29yZA==
```

- macOS

```
sudo "/Library/Application
Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent" -o register -a
https://10.250.144.179:9877 -u johndoe -b -p am9obnNwYXNzd29yZA==
```

Implementación en la nube

- Plantilla de comando

```
<path to the registration tool> -o register -t cloud -a <service address> -u <user
name> -b -p <encoded password>
```

- Windows

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

- Linux

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

- macOS

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

Buscar actualizaciones de software

Esta funcionalidad solo está disponible para administradores de la organización.

Cada vez que inicie sesión en la consola web de Cyber Protect, Acronis Cyber Protect buscará nuevas versiones disponibles en el sitio web de Acronis. En ese caso, la consola web de Cyber Protect muestra un enlace de descarga de la nueva versión en la parte inferior de cada página en las pestañas **Dispositivos**, **Planes** y **Almacenamiento de copias de seguridad**. El enlace también está disponible en la página **Configuración** > **Agentes**.

Para habilitar o deshabilitar las búsquedas automáticas de actualizaciones, cambie el ajuste del sistema **Actualizaciones**.

Para buscar actualizaciones manualmente, haga clic en el icono del signo de interrogación en la esquina superior derecha > **Acerca de** > **Buscar actualizaciones**, o en el icono del signo de interrogación > **Buscar actualizaciones**.

Migración del servidor de administración

Puede migrar un servidor de administración que se ejecute en un equipo Windows a otro equipo Windows del mismo entorno.

El proceso de migración está formado por las siguientes fases:

1. "Operaciones en el equipo de origen" (p. 165)
   En esta fase, prepare los datos del servidor de administración original para migrarlos.
2. "Operaciones en el equipo de destino" (p. 166)
   En esta fase, instale y configure un nuevo servidor de administración y copie los datos del servidor de administración original al nuevo.

Requisitos previos

- El servidor de administración utiliza una base de datos externa de Microsoft SQL Server. La instancia de Microsoft SQL Server se ejecuta en un equipo dedicado.

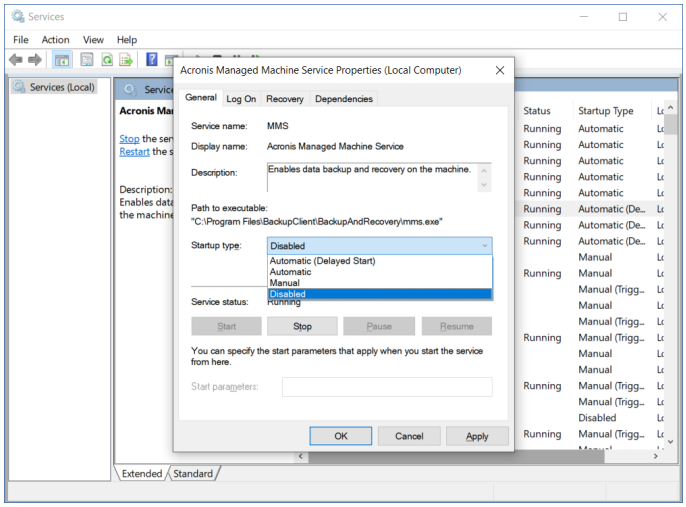
- Los agentes de protección se registran en el servidor de administración con su nombre de host, no con la dirección IP.
- La versión del servidor de administración es Acronis Cyber Protect actualización 4 (compilación 29486) o posterior.
- La misma versión del servidor de administración se instala en el equipo de origen y en el de destino.

Operaciones en el equipo de origen

En esta fase, prepare los datos del servidor de administración original para migrarlos.

Cómo preparar los datos para la migración

1. En el equipo del servidor de administración original, detenga todos los servicios de Acronis.
   a. Abra **Servicios** y deshabilite el inicio de los servicios de Acronis, excepto para **Acronis Active Protection Service** y **Acronis Cyber Protection Service**.



   b. Abra **Regedit** y deshabilite **Acronis Active Protection Service** y **Acronis Cyber Protection Service** mediante la edición de sus claves:
      - En la clave `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AcronisCyberProtectionService`, abra el valor **Iniciar** y configure los datos del valor hasta el 4.
      - En la clave `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AcronisActiveProtectionService`, abra el valor **Iniciar** y configure los datos del valor hasta el 4.
2. Reinicie el equipo del servidor de administración y verifique que los servicios de Acronis deshabilitados no se ejecutan.

> **Nota**
> Es posible que los servicios **Acronis Scheduler Service Helper** y **Acronis TIB Mounter Monitor** sigan ejecutándose. Puede ignorarlos de forma segura.

3. [Si el componente de Cyber Protect Monitor está instalado en el equipo del servidor de administración] Salga de Acronis Cyber Protect Monitor.
4. En el símbolo del sistema de Windows, cambie el propietario de las carpetas `%ProgramData%\Acronis` y `%ProgramFiles%\Acronis`. Para ello, ejecute los siguientes comandos:

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

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

5. Edite los permisos de acceso de estas carpetas y sus subcarpetas mediante la ejecución de los siguientes comandos:

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

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

6. Copie las carpetas `%ProgramData%\Acronis` y `%ProgramFiles%\Acronis` en un recurso compartido de red al que pueda acceder el nuevo equipo del servidor de administración.
7. Apague el equipo del servidor de administración original.

A continuación, siga el procedimiento disponible en "Operaciones en el equipo de destino" (p. 166).

Operaciones en el equipo de destino

En esta fase, instale y configure un nuevo servidor de administración y migre los datos a este.

Antes de ejecutar las operaciones en el equipo de destino, asegúrese de completar el procedimiento en "Operaciones en el equipo de origen" (p. 165).

Pasos para migrar los datos al nuevo servidor de administración

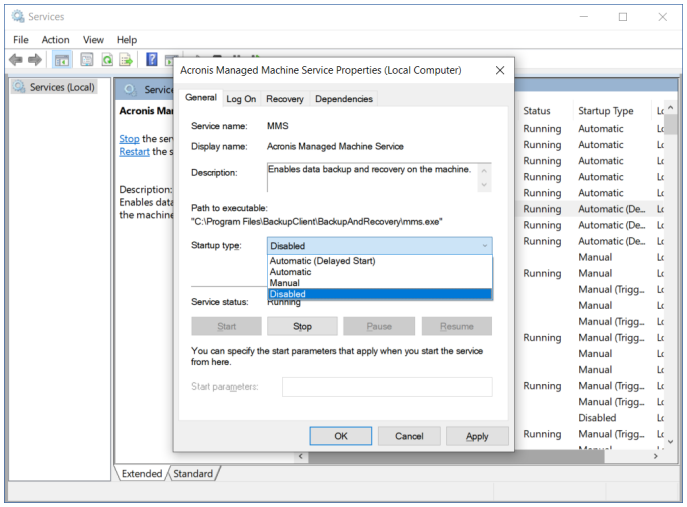
1. Establezca el nombre del host del equipo en el que instalará el nuevo servidor de administración. Este nombre debe ser el mismo que el del equipo con el servidor de administración original.
2. Cree una regla del firewall para bloquear todo el tráfico del puerto TCP 9877.
3. Ejecute el programa de instalación de Acronis Cyber Protect.
   a. Acepte los términos del acuerdo de licencia y la declaración de privacidad y, a continuación, haga clic en **Siguiente**.
   b. Haga clic en **Personalizar configuración de la instalación**.
   c. En **Qué instalar**, seleccione los siguientes componentes y haga clic en **Listo**.
      - Servidor de gestión
      - Componentes para la instalación remota
      - Bootable Media Builder
      - Herramienta de línea de comandos

d. En **Base de datos para el servidor de administración**, mantenga la opción predeterminada **Utilizar SQLite integrado**.

e. En **Cuenta de inicio de sesión para el servicio del servidor de administración**, utilice la misma opción que en el servidor de administración original.

4. Detenga los servicios de Acronis.

a. Abra **Servicios** y deshabilite el inicio de todos los servicios de Acronis.

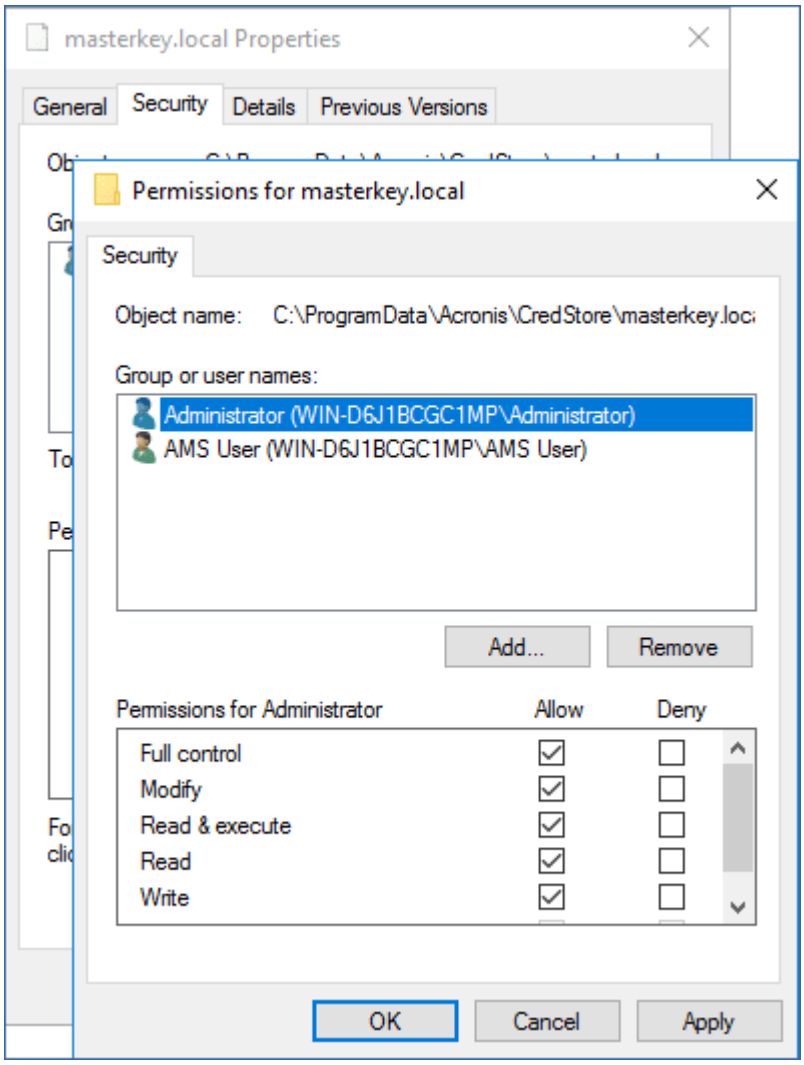


b. Reinicie el equipo y verifique que los servicios de Acronis deshabilitados no se están ejecutando.

5. Vaya a `%ProgramData%\Acronis\CredStore` y ajuste los permisos del archivo `masterkey.local` como sigue:

a. Otorgue la propiedad del archivo a la cuenta de usuario **Administrador**.

b. Otorgue a la cuenta de usuario **Administrador** permisos de **Control total**.



6. Vaya a `%ProgramData%\Acronis\AMS\AccessVault\config` y otorgue a la cuenta de usuario **Administrador** permisos de **Control total** para los siguientes archivos:
   - `%ProgramData%\Acronis\AMS\AccessVault\config\preferred`
   - `%ProgramData%\Acronis\AMS\AccessVault\config\preferred.json`
7. Reemplace las siguientes carpetas por las carpetas que copió del equipo del servidor de administración original al recurso compartido de red:
   - `%ProgramData%\Acronis`
   - `%ProgramFiles%\Acronis`

   Importante
   Sobrescriba las carpetas existentes sin eliminarlas primero.

   Nota
   Si ve un mensaje que dice que la carpeta `%ProgramFiles%\Acronis\ShellExtentions` no se puede reemplazar, puede omitir esta carpeta de forma segura.
8. Restaure los permisos para los siguientes archivos:

- `%ProgramData%\Acronis\CredStore\masterkey.local`: elimine la cuenta de usuario **Administrador** de la lista de usuarios con permisos.
- `%ProgramData%\Acronis\AMS\AccessVault\config\preferred`: otorgue a la cuenta de usuario **Administrador** solo el permiso de **Lectura**.
- `%ProgramData%\Acronis\AMS\AccessVault\config\preferred.json`: otorgue a la cuenta de usuario **Administrador** solo el permiso de **Lectura**.

9. Cree una intersección de directorios para la carpeta `NGMP\latest`.
   - En el símbolo del sistema de Windows, vaya a `%ProgramData%\Acronis\NGMP` y elimine la carpeta `más reciente`.

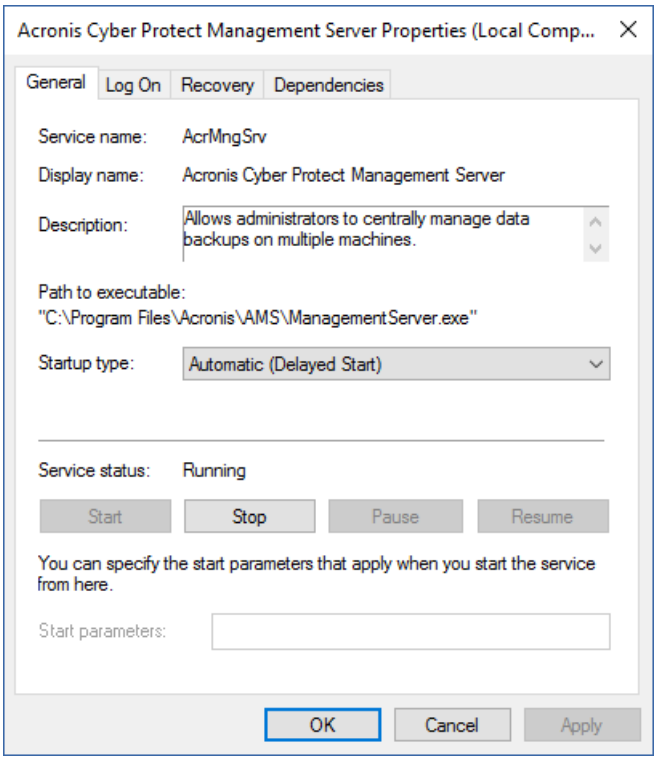
     ```
     cd %ProgramData%\Acronis\NGMP
     ```

     ```
     rmdir latest
     ```

   - Cree una intersección de directorios `más recientes` y vaya a la carpeta con el nombre de la versión actual de NGMP, por ejemplo:

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

10. Seleccione en el nuevo servidor de administración la base de datos de Microsoft SQL Server que utilizó el servidor de administración original.
    a. Abra **Regedit**.
    b. En la clave `HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\AMS\Settings`, modifique el valor `AmsDmlDbProtocol`. Para ello, cambie sus datos a `config://C:\ProgramData\Acronis\AMS\mssql\dml_mssql.config`.
11. Abra **Servicios** y habilite todos los servicios de Acronis deshabilitados.
    Establezca el tipo de inicio del **servidor de administración de Acronis Cyber Protect** en **Automático (Inicio diferido)** y el tipo de inicio del resto de servicios de Acronis en **Automático**.



12. En el firewall, permita todo el tráfico en el puerto TCP 9877.
13. Reinicie el equipo y verifique que todos los servicios de Acronis se ejecuten.
14. Ejecute el programa de instalación de Acronis Cyber Protect e instale los siguientes elementos:
    - Agente para Windows
    - [Opcional] Cyber Protect Monitor
15. Reinicie el equipo.

Implementación en la nube

Activación de la cuenta

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

- **Un enlace de activación de cuenta.** Haga clic en el enlace y establezca la contraseña de la cuenta. Recuerde su usuario, el cual aparece en la página de activación de la cuenta.
- **Un enlace a la página de inicio de la consola web de Cyber Protect.** Este enlace le permitirá acceder a la consola en el futuro. El usuario y la contraseña son los mismos que en el paso anterior.

Preparación

Paso 1

Elija el Agente teniendo en cuenta los elementos que va a incluir en la copia de seguridad. Para obtener más información acerca de los agentes, consulte "Componentes" (p. 63).

Paso 2

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

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

Si desea almacenar los programas de instalación localmente, descargue un paquete que contenga todos los agentes para la instalación en Windows por medio del enlace que hay en la parte inferior de la página **Añadir dispositivos**. Están disponibles los paquetes de 32 bits y 64 bits. Con estos paquetes se puede personalizar la lista de componentes que se instalarán. Estos paquetes también permiten la instalación sin interacción, por ejemplo, a través de la directiva de grupo. Se detalla este escenario avanzado en "Implementación de agentes mediante la directiva de grupo" (p. 220).

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

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

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

Paso 3

Antes de empezar la instalación, asegúrese de que los cortafuegos y otros componentes del sistema de seguridad de red (como, por ejemplo, un servidor proxy) permiten conexiones tanto de entrada como de salida mediante los siguientes puertos TCP:

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

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

  Los agentes usan estos puertos para comunicarse con el servidor de gestión.
- Puertos **44445** y **55556**

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

Si hay un servidor proxy habilitado en la red, consulte "Ajuste de la configuración del servidor proxy" (p. 173) para saber si debe configurar estos ajustes en cada equipo que ejecute un agente de protección.

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

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

- Puerto **443**

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

  El agente para VMware (en Windows y dispositivo virtual) se conecta a este puerto del servidor ESXi para establecer conexiones NFC con el fin de poder leer o escribir datos en discos de máquinas virtuales durante operaciones de copia de seguridad, recuperación y replicación de máquinas virtuales.
- Puerto **3333**

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

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

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

Paso 4

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

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

Nota
No tiene que abrirlos en el firewall.

El servicio Active Protection está escuchando en el puerto TCP **6109**. Compruebe que no esté en uso por otra aplicación.

Cambio de los puertos utilizados por el agente de protección

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

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

Ajuste de la configuración del servidor proxy

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

Puesto que el agente se registra en la cloud durante la instalación, debe proporcionarse la configuración del servidor proxy durante la instalación o antes de esta.

Para Windows

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

Utilice este procedimiento si desea ejecutar las siguientes tareas.

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

Para configurar los ajustes de proxy durante la instalación del agente, consulte "Instalación de agentes" (p. 177).

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

El archivo `%programdata%\Acronis\Agent\var\aakore\http-proxy.yaml` se crea al configurar los ajustes del servidor proxy mediante Cyber Protect Monitor. Para abrir este archivo, debe ser miembro del grupo Administradores en Windows.

Pasos para configurar los ajustes de proxy

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

```
Windows Registry Editor Version 5.00

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

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

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

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

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

14. Reinicie el agente con los siguientes comandos:

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

Para Linux

Para configurar la configuración del proxy durante la instalación del agente, ejecute el archivo de instalación con `--http-proxy-host=` `DIRECCIÓN` `--http-proxy-port=` `PUERTO` `--http-proxy-login=` `INICIO DE SESIÓN` `--http-proxy-password=` `parámetros de CONTRASEÑA`.

Use el siguiente procedimiento para actualizar los ajustes de proxy después de la instalación del agente de protección.

Pasos para configurar los ajustes de proxy

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

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

   - Si no especificó la configuración de proxy durante la instalación del agente, copie las siguientes líneas y péguelas en el archivo entre las etiquetas `<registry name="Global">...</registry>`.

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

3. Reemplace `DIRECCIÓN` por el nombre del host o la dirección IP del servidor proxy y `PUERTO` por el valor decimal del número de puerto.
4. Si su servidor proxy necesita que se autentifique, sustituya `INICIO DE SESIÓN` Y `CONTRASEÑA` por las credenciales del servidor proxy. De lo contrario, elimine estas líneas del archivo.
5. Guarde el archivo.

6. Abra el archivo `/opt/acronis/etc/aakore.yaml` en un editor de texto.
7. Busque la sección **env** o créela y añada las siguientes líneas:

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

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

```
sudo service aakore restart
```

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

```
sudo service acronis_mms restart
```

Para macOS:

Utilice este procedimiento si desea ejecutar las siguientes tareas.

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

Para configurar los ajustes de proxy durante la instalación del agente, consulte "Instalación de agentes" (p. 177).

Pasos para configurar los ajustes de proxy

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

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

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

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

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

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

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

12. Reinicie el agente con los siguientes comandos:

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

Para el dispositivo de arranque

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

Instalación de agentes

En Windows

1. Asegúrese de que el equipo está conectado a Internet.
2. Inicie sesión como administrador e inicie el programa de instalación.
3. [Opcional] Haga clic en **Personalizar configuración de la instalación** y realice los cambios necesarios para:
   - Cambiar los componentes que se vayan a instalar (concretamente, para deshabilitar la instalación de Cyber Protect Monitor y la herramienta de línea de comandos).
   - Pasos para cambiar el método de registro del equipo en el servicio de ciberprotección. Puede cambiar de **Usar la consola de Cyber Protect** (opción predeterminada) a **Usar credenciales** o **Usar token de registro**.
   - Cambiar la ruta de acceso de instalación.

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

4. Haga clic en **Instalar**.
5. [Solo al instalar Agente para VMware] Especifique la dirección y las credenciales de acceso del servidor vCenter Server o host ESXi independiente de cuyos equipos virtuales el agente realizará la copia de seguridad. Después, haga clic en **Listo**. Le recomendamos utilizar una cuenta que tenga asignado el rol de **Administrador**. En otro caso, proporcione una cuenta con los privilegios necesarios en el servidor vCenter Server oESXi.
6. [Solo al instalar en un controlador de dominio] Especifique la cuenta de usuario en la que se ejecutará el servicio de agente. Después, haga clic en **Listo**. Por razones de seguridad, el programa de instalación no crea automáticamente nuevas cuentas en un controlador de dominio.

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

   Para obtener más información sobre la instalación del agente en un controlador de dominio de sólo lectura, consulte este artículo de la base de conocimientos.
7. Si ha seguido el método de registro predeterminado **Usar consola de Cyber Protect** en el paso 3, espere a que aparezca la pantalla de registro y, a continuación, siga con el paso siguiente. De lo contrario, no se requieren más acciones.
8. Realice uno de los siguientes procedimientos:
   - Haga clic en **Registrar el equipo**. En la ventana del explorador que se abrirá, inicie sesión en la consola web de Cyber Protect, revise los detalles de registro y haga clic en **Confirmar registro**.
   - Haga clic en **Mostrar información de registro**. El programa de instalación mostrará el vínculo y el código de registro. Puede copiar esta información y llevar a cabo los pasos de registro en un equipo distinto. En ese caso, deberá escribir el código de registro en el formulario de registro. El código de registro tiene una validez de una hora.
     También puede acceder al formulario de registro haciendo clic en **Todos los dispositivos** > **Agregar**, desplazándose hacia abajo hasta **Registro por código** y haciendo clic en **Registrarse**.
9. **Nota**
   No salga del programa de instalación hasta confirmar el registro. Para iniciar el registro de

nuevo, reinicie el programa de instalación y haga clic en **Registrarse el equipo**.

Se asignará el equipo a la cuenta utilizada para iniciar sesión en la consola web de Cyber Protect.

En Linux

1. Asegúrese de que el equipo está conectado a Internet.
2. Ejecute el archivo de instalación como usuario raíz.

   Si hay un servidor proxy habilitado en la red, al ejecutar el archivo, especifique el nombre del host o la dirección IP del servidor y el puerto en el formato siguiente: `--http-proxy-host=DIRECCIÓN --http-proxy-port=PUERTO--http-proxy-login=NOMBRE DE USUARIO--http-proxy-password=CONTRASEÑA`.

   Si desea cambiar el método predeterminado de registro del equipo en el servicio de ciberprotección, ejecute el archivo de instalación con uno de los parámetros siguientes:
   - `--register-with-credentials`; para que se solicite un nombre de usuario y una contraseña durante la instalación
   - `--token=STRING`; para que se utilice un token de registro
   - `--skip-registration`; para omitir el registro
3. Seleccione las casillas de verificación de los agentes que desea instalar. Los agentes disponibles son los siguientes:
   - **Agente para Linux**
   - **Agente para Virtuozzo**

   Agente para Virtuozzo no se puede instalar sin Agente para Linux.
4. Si ha seguido el método de registro predeterminado en el paso 2, continúe con el paso siguiente. En caso contrario, introduzca el nombre de usuario y la contraseña para el servicio de ciberprotección o espere hasta que el equipo se registre mediante el token.
5. Realice uno de los siguientes procedimientos:
   - Haga clic en **Registrar el equipo**. En la ventana del explorador que se abrirá, inicie sesión en la consola web de Cyber Protect, revise los detalles de registro y haga clic en **Confirmar registro**.
   - Haga clic en **Mostrar información de registro**. El programa de instalación mostrará el vínculo y el código de registro. Puede copiar esta información y llevar a cabo los pasos de registro en un equipo distinto. En ese caso, deberá escribir el código de registro en el formulario de registro. El código de registro tiene una validez de una hora.

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

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

   Se asignará el equipo a la cuenta utilizada para iniciar sesión en la consola web de Cyber Protect.
7. Si el arranque seguro UEFI se habilita en el equipo, se le informará de que debe reiniciar el sistema tras la instalación. Asegúrese de que recuerda qué contraseña (la del usuario raíz o "acronis") debe utilizar.

   Nota
   Durante la instalación, se genera una clave nueva que se utiliza para firmar el módulo `snapapi` y se registra como clave del propietario del equipo (MOK). Es obligatorio reiniciar para poder registrar la clave. Si no se registra la clave, el agente no estará operativo. Si habilita el arranque seguro UEFI después de la instalación del agente, repita la instalación, incluido el paso 6.

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

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

En macOS

1. Asegúrese de que el equipo está conectado a Internet.
2. Haga doble clic sobre el archivo de instalación (.dmg).
3. Espere mientras el sistema operativo monta la imagen del disco de instalación.
4. Haga doble clic en **Instalar**.
5. Si en la red hay un servidor proxy habilitado, haga clic en **Agente de protección**, en la barra de menú, y luego en **Configuración del servidor proxy**. A continuación, especifique el nombre del host, la dirección IP, el puerto y las credenciales del servidor proxy.
6. Si se le pide, proporcione las credenciales del administrador.
7. Haga clic en **Continuar**.
8. Espere a que se muestre la pantalla de registro.
9. Realice uno de los siguientes procedimientos:
   - Haga clic en **Registrar el equipo**. En la ventana del explorador que se abrirá, inicie sesión en la consola web de Cyber Protect, revise los detalles de registro y haga clic en **Confirmar registro**.

- Haga clic en **Mostrar información de registro**. El programa de instalación mostrará el vínculo y el código de registro. Puede copiar esta información y llevar a cabo los pasos de registro en un equipo distinto. En ese caso, deberá escribir el código de registro en el formulario de registro. El código de registro tiene una validez de una hora.
  También puede acceder al formulario de registro haciendo clic en **Todos los dispositivos** > **Agregar**, desplazándose hacia abajo hasta **Registro por código** y haciendo clic en **Registrarse**.

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

Se asignará el equipo a la cuenta utilizada para iniciar sesión en la consola web de Cyber Protect.

Cómo cambiar la cuenta de inicio de sesión en equipos Windows

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

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

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

Privilegios necesarios para la cuenta de inicio de sesión

Los agentes de protección se ejecutan en un Managed Machine Service (MMS) de un equipo Windows. La cuenta con la que se ejecutará el agente debe tener derechos específicos para que el

agente funcione correctamente. Por lo tanto, al usuario de MMS se le deberían asignar los siguientes privilegios:

1. Incluirlo en los grupos **Operadores de copia de seguridad** y **Administradores**. En un controlador de dominio, el usuario debe incluirse en el grupo **Administradores del dominio**.
2. Se otorgan permisos de **Control total** sobre la carpeta `%PROGRAMDATA%\Acronis` (en Windows XP y en Server 2003, `%ALLUSERSPROFILE%\Application Data\Acronis`) y en sus subcarpetas.
3. Cada una de las tres cuentas tiene permiso de **Control total** en las claves de registro en la siguiente clave: `HKEY_LOCAL_MACHINE\SOFTWARE\Acronis`.
4. Asignarle los siguientes derechos de usuario:
   - Inicio de sesión como un servicio
   - Ajustar cantidades máximas de memoria para un proceso
   - Reemplazar símbolo de nivel de un proceso
   - Modificar los valores del entorno de firmware

Cómo asignar derechos de usuario

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

1. Inicie sesión en el equipo con una cuenta con privilegios administrativos.
2. Abra **Herramientas administrativas** del **Panel de control** (o haga clic en Win+R, escriba **herramientas de administración de control** y presione Intro) y abra **Política de seguridad local**.
3. Amplíe **Políticas locales** y haga clic en **Asignación de derechos de usuario.**
4. En el panel de la derecha, haga clic en **Inicio de sesión como un servicio** y seleccione **Propiedades**.
5. Haga clic en el botón **Añadir usuario o grupo...** para agregar un nuevo usuario.
6. En la ventana **Seleccionar usuarios, ordenadores, cuentas de servicio o grupos**, busque el usuario que quiera introducir y haga clic en **Aceptar**.
7. Haga clic en **Aceptar** en las propiedades **Inicio de sesión como un servicio** para guardar los cambios.

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

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

Instalación o desinstalación sin supervisión

Instalación o desinstalación sin supervisión en Windows

En esta sección se describe cómo instalar o desinstalar los agentes de protección en el modo de interacción en un equipo que ejecute Windows, o mediante Windows Installer (el programa `msiexec`). En un dominio de Active Directory, otra manera de realizar una instalación sin supervisión es a través de una directiva de grupo. Consulte "Implementación de agentes mediante la directiva de grupo" (p. 220).

Durante la instalación, puede utilizar un archivo conocido como una **transformación** (un archivo .mst). Una transformación es un archivo con parámetros de instalación. Como alternativa, puede especificar los parámetros de instalación directamente en la línea de comando.

Creación de la transformación .mst y extracción de los paquetes de instalación

1. Inicie sesión como administrador e inicie el programa de instalación.
2. Haga clic en **Crear archivos .mst y .msi para una instalación sin supervisión**.
3. En **Qué instalar**, seleccione los componentes que desea instalar y haga clic en **Listo**.
   Los paquetes de instalación de estos componentes se extraerán del programa de instalación.
4. En **Configuración de registro**, seleccione **Usar credenciales** o **Usar token de registro**. Para obtener más información sobre cómo generar un token de registro, consulte "Paso 1: Generar un token de registro" (p. 221).
5. [Solamente cuando instale en un controlador de dominio] En **Cuenta de inicio de sesión para el servicio de agente**, seleccione **Utilizar la siguiente cuenta**. Especifique la cuenta de usuario en la que se ejecutará el servicio de agente. Después, haga clic en **Listo**. Por razones de seguridad, el programa de instalación no crea automáticamente nuevas cuentas en un controlador de dominio.

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

   Para obtener más información sobre la instalación del agente en un controlador de dominio de sólo lectura, consulte este artículo de la base de conocimientos.
6. Compruebe o modifique otros ajustes de la instalación que se añadirá al archivo .mst y haga clic en **Continuar**.
7. Seleccione la carpeta en la que se generará la transformación .mst y los paquetes de instalación .msi y .cab se extraerán y, a continuación, haga clic en **Generar**.

Instalación del producto mediante la transformación .mst

En la línea de comando, ejecute el siguiente comando.

Plantilla de comando:

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

Donde:

- `<package name>` es el nombre del archivo .msi.
- `<transform name>` es el nombre de la transformación.

Ejemplo de comando:

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

Instalación o desinstalación del producto especificando parámetros manualmente

En la línea de comando, ejecute el siguiente comando.

Plantilla de comando (instalando):

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

Aquí, `<package name>` es el nombre del archivo .msi. Todos los parámetros disponibles y sus valores se describen en "Parámetros básicos" (p. 184).

Plantilla de comando (desinstalando):

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

La versión del paquete .msi debe ser la misma que la del producto que desee desinstalar.

Parámetros de instalación o desinstalación sin supervisión

Esta sección describe parámetros utilizados en una instalación o desinstalación sin supervisión en Windows. Además de estos parámetros, puede utilizar otros parámetros de `msiexec`, como se describe en https://msdn.microsoft.com/en-us/library/windows/desktop/aa367988(v=vs.85).aspx.

Parámetros de instalación

Parámetros básicos

`ADDLOCAL=<list of components>`

Los componentes que se van a instalar, separados con comas y sin espacios. Todos los componentes especificados deben extraerse del programa de instalación antes de realizar la instalación.

La lista completa de componentes es la siguiente:

Componente	Debe instalarse junto con	Número de bits	Nombre o descripción del componente
MmsMspComponents		32 bits / 64 bits	Componentes fundamentales de los agentes
BackupAndRecoveryAgent	MmsMspComponents	32 bits / 64 bits	Agente para Windows
ArxAgentFeature	BackupAndRecoveryAgent	32 bits / 64 bits	Agente para Exchange
ArsAgentFeature	BackupAndRecoveryAgent	32 bits / 64 bits	Agente para SQL
ARADAgentFeature	BackupAndRecoveryAgent	32 bits / 64 bits	Agente para Active Directory
ArxOnlineAgentFeature	MmsMspComponents	32 bits / 64 bits	Agente para Office 365
OracleAgentFeature	BackupAndRecoveryAgent	32 bits / 64 bits	Agent para Oracle
AcronisESXSupport	MmsMspComponents	64 bits	Agente para VMware ESX(i) (Windows)
HyperVAgent	MmsMspComponents	32 bits / 64 bits	Agente para Hyper-V
CommandLineTool		32 bits / 64 bits	Herramienta de línea de comandos
TrayMonitor	BackupAndRecoveryAgent	32 bits / 64 bits	Cyber Protect Monitor

`TARGETDIR=<path>`

La carpeta donde se instalará el producto. De forma predeterminada, esta carpeta es: `C:\Program Files\BackupClient`.

`REBOOT=ReallySuppress`

Si se especifica el parámetro, se prohíbe el reinicio del equipo.

`/l*v <log file>`

Si se especifica el parámetro, el registro de instalación en modo detallado se guardará en el archivo especificado. El archivo de registro se puede utilizar para analizar problemas de instalación.

`CURRENT_LANGUAGE=<language ID>`

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

Parámetros de registro

`REGISTRATION_ADDRESS`

Esta es la URL del servicio Cyber Protect. Puede usar este parámetro con los parámetros `REGISTRATION_LOGIN` y `REGISTRATION_PASSWORD` o bien con `REGISTRATION_TOKEN` .

- Cuando use `REGISTRATION_ADDRESS` con los parámetros `REGISTRATION_LOGIN` y `REGISTRATION_PASSWORD` , especifique la dirección que usa para **iniciar sesión en** el servicio Cyber Protect. Por ejemplo, `https://cloud.company.com`:

- Cuando use `REGISTRATION_ADDRESS` con el parámetro `REGISTRATION_TOKEN` , especifique la dirección exacta del centro de datos. Esta es la URL que ve **cuando ha iniciado sesión en** el servicio Cyber Protect. Por ejemplo, `https://eu2-cloud.company.com`.

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

`REGISTRATION_LOGIN` y `REGISTRATION_PASSWORD`

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

`REGISTRATION_PASSWORD_ENCODED`

Contraseña para la cuenta con la que se registrará el agente en el servicio Cyber Protect, codificada como base64. Para obtener más información sobre cómo codificar su contraseña, consulte: "Registro manual de equipos".

`REGISTRATION_TOKEN`

El token de registro es una serie de 12 caracteres separados en tres segmentos por guiones. Puede generar uno en la consola web como se describe en "Implementación de agentes mediante la directiva de grupo".

`REGISTRATION_REQUIRED={0,1}`

Define cómo terminará la instalación si falla el registro. Si el valor es `1`, la instalación también falla. El valor predeterminado es `0`, por lo que, si no especifica este parámetro, la instalación se lleva a cabo correctamente, aunque el componente no esté registrado.

Parámetros adicionales

Para definir la cuenta de inicio de sesión para el servicio de agente en Windows, use uno de los siguientes parámetros:

- `MMS_USE_SYSTEM_ACCOUNT={0,1}`

  Si el valor es `1`, el agente se ejecutará en la cuenta **Sistema local**.
- `MMS_CREATE_NEW_ACCOUNT={0,1}`

  Si el valor es `1`, el agente se ejecutará en una cuenta creada recientemente cuyo nombre es **Acronis Agent User**.
- `MMS_SERVICE_USERNAME=<user name>` y `MMS_SERVICE_PASSWORD=<password>`

  Use estos parámetros para especificar una cuenta existente en la que se ejecutará el agente.

Para obtener más información sobre las cuentas de inicio de sesión, consulte "Cómo cambiar la cuenta de inicio de sesión en equipos Windows".

`SET_ESX_SERVER={0,1}`

- Si el valor es `0`, el Agent for VMware que se esté instalando no se conectará al vCenter Server ni al servidor ESXi. Si el valor es `1`, especifique los siguientes parámetros:
  - `ESX_HOST=<host name>`

    El nombre del servidor o dirección IP del vCenter Server o servidor ESXi.
  - `ESX_USER=<user name>` y `ESX_PASSWORD=<password>`

    Credenciales para acceder al vCenter Server o al servidor ESXi.

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

Servidor proxy HTTP que utilizará el agente. Sin estos parámetros, no se utilizará ningún servidor proxy.

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

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

`HTTP_PROXY_ONLINE_BACKUP={0,1}`

Si el valor es `0`, o el parámetro no está especificado, el agente usará el servidor proxy únicamente para realizar copias de seguridad y recuperaciones desde el cloud. Si el valor es `1`, el agente también se conectará al servidor de gestión a través del servidor proxy.

Parámetros de desinstalación

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

Los componentes que se van a eliminar, separados con comas y sin espacios. Si el valor es `ALL`, se desinstalarán todos los componentes del producto.

Además, puede especificar el parámetro siguiente:

```
DELETE_ALL_SETTINGS={0, 1}
```

Si el valor es `1`, se eliminarán los registros, tareas y ajustes de configuración del producto.

Ejemplos

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

  ```
  msiexec.exe /i BackupClient64.msi /l*v my_log.txt /qn
  ADDLOCAL=MmsMspComponents,BackupAndRecoveryAgent,CommandLineTool,TrayMonitor
  TARGETDIR="C:\Program Files\BackupClient" REBOOT=ReallySuppress MMS_USE_SYSTEM_
  ACCOUNT=1 REGISTRATION_ADDRESS=https://cloud.company.com REGISTRATION_LOGIN=johndoe
  REGISTRATION_PASSWORD=johnspassword
  ```

- Instalación del Agente para Windows, la herramienta de línea de comandos y la monitorización de ciberprotección. Creación de una cuenta de inicio de sesión nueva para el servicio de agente en Windows. Registro del equipo en el servicio Cyber Protect empleando un token.

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

- Instalación del Agente para Windows, la herramienta de línea de comandos, Agent for Oracle y la monitorización de ciberprotección. Registro del equipo en el servicio Cyber Protect empleando un nombre de usuario y una contraseña codificada base64.

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

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

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

- Desinstalación de todos los agentes y eliminación de todos sus registros, tareas y ajustes de configuración.

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

Instalación o desinstalación sin supervisión en Linux

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

Pasos para instalar o desinstalar un agente de protección

1. Abra el terminal.

2. Realice uno de los siguientes procedimientos:

- Para iniciar la instalación especificando los parámetros de la línea de comando, ejecute el siguiente comando:

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

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

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

  Este enfoque puede ser útil si no quiere introducir información confidencial en la línea de comando. En este caso, puede especificar los ajustes de configuración en un archivo de texto independiente y asegurarse de que únicamente usted pueda acceder a él. Ponga cada parámetro en una línea nueva, seguido de los valores que desee, por ejemplo:

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

o

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

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

3. Si el arranque seguro UEFI se habilita en el equipo, se le informará de que debe reiniciar el sistema tras la instalación. Asegúrese de que recuerda qué contraseña (la del usuario raíz o "acronis") debe utilizar. Durante el reinicio del sistema, opte por la gestión de MOK (clave del propietario del equipo), seleccione **Registrar MOK** y, a continuación, registre la clave por medio de la contraseña recomendada.

Si habilita el arranque seguro UEFI después de la instalación del agente, repita la instalación, incluido el paso 3. En caso contrario, las copias de seguridad fallarán.

Parámetros de instalación o desinstalación sin supervisión

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

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

Parámetros de instalación

Parámetros básicos

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

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

Componente	Descripción de componentes
BackupAndRecoveryAgent	Agente para Linux
AgentForPCS	Agente para Virtuozzo
OracleAgentFeature	Agent para Oracle

Sin este parámetro, se instalarán todos los componentes anteriores.

Tanto Agente para Virtuozzo como Agent for Oracle requieren que el Agente para Linux también esté instalado.

El paquete de instalación .i686 contiene únicamente BackupAndRecoveryAgent.

`{-a|--auto}`

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

`{-t|--strict}`

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

`{-n|--nodeps}`

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

`{-d|--debug}`

Escribe el registro de instalación en modo detallado.

`--options-file=<location>`

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

`--language=<language ID>`

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

Parámetros de registro

Especifique alguno de los parámetros siguientes:

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

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

- `--token=<token>`

  El token de registro es una serie de 12 caracteres separados en tres segmentos por guiones. Puede generar uno en la consola web como se describe en "Implementación de agentes mediante la directiva de grupo".

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

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

  URL del servicio Cyber Protect.

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

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

- `--register-with-credentials`

Si se especifica este parámetro, se iniciará la interfaz gráfica del programa de instalación. Para finalizar el registro, introduzca el nombre de usuario y la contraseña de la cuenta con la que se registrará el agente en el servicio Cyber Protect. No puede ser una cuenta de administrador de partners.

- `--skip-registration`

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

Parámetros adicionales

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

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

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

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

`--tmp-dir=<location>`

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

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

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

`--skip-prereq-check`

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

`--force-weak-snapapi`

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

`--skip-svc-start`

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

Parámetros de información

`{-?|--help}`

Muestra descripción de los parámetros.

`--usage`

Muestra una breve descripción del uso del comando.

`{-v|--version}`

Muestra la versión del paquete de instalación.

`--product-info`

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

`--snapapi-list`

Muestra los módulos "snapapi" preparados disponibles.

`--components-list`

Muestra los componentes del programa de instalación.

Parámetros para funciones heredadas

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

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

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

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

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

Parámetros de desinstalación

`{-u|--uninstall}`

Desinstala el producto.

`--purge`

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

Ejemplos

- Instalación del Agente para Linux sin registrarlo.

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

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

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

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

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

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

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

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

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

Instalación sin supervisión e instalación en macOS

En esta sección se describe cómo instalar, registrar y desinstalar el agente de protección en el modo de interacción en un equipo que ejecute macOS mediante una línea de comando. Para obtener información sobre cómo descargar el archivo de instalación (.dmg), consulte "Añadir un equipo que ejecute macOS".

Para instalar Agente para Mac

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

   ```
   mkdir <dmg_root>
   ```

   Aquí, `<dmg_root>` es un nombre de su elección.
2. Monte el archivo .dmg.

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

   Aquí, `<dmg_file>` es el nombre del archivo de instalación. Por ejemplo, **AcronisAgentMspMacOSX64.dmg**.
3. Ejecute el programa de instalación.

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

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

   ```
   hdiutil detach <dmg_root>
   ```

Ejemplos

- ```
  mkdir mydirectory
  ```

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

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

  ```
  hdiutil detach mydirectory
  ```

Para registrar Agente para Mac

Realice uno de los siguientes procedimientos:

- Registre el agente en una cuenta específica con un nombre de usuario y una contraseña.
  ```

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

Donde:

La <dirección de servicio de Cyber Protect> es la dirección que usa **para iniciar sesión** en el servicio Cyber Protect. Por ejemplo:

El <user name> y la <password> son las credenciales para la cuenta en la que se registrará el agente. No puede ser una cuenta de administrador de partners.

- Registre el agente mediante un token de registro.

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

El token de registro es una serie de 12 caracteres separados en tres segmentos por guiones. Puede generar uno en la consola web de Cyber Protect como se describe en "Implementación de agentes mediante la directiva de grupo".

Cuando use un token de registro, debe especificar la dirección exacta del centro de datos. Esta es la URL que ve **cuando ha iniciado sesión en** el servicio Cyber Protect. Por ejemplo:

Importante

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

Ejemplos

Registro con un nombre de usuario y una contraseña.

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

Registro con un token.

-
```
sudo /Library/Application\
Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent -o register -t cloud -a
```

```
https://eu2-cloud company.com --token D91D-DC46-4F0B
```

Para desinstalar Agente para Mac

Ejecute el siguiente comando:

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

Para eliminar todos los registros, tareas y ajustes de configuración durante la desinstalación, ejecute el siguiente comando:

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

Registro y anulación de registro manual de equipos

Los equipos se registran automáticamente en el servicio de Cyber Protect cuando instala en ellas el agente de protección. Cuando desinstale el agente de protección, se anulará automáticamente el registro de los equipos y desaparecerán de la consola web de Cyber Protect.

También puede registrar un equipo manualmente mediante la interfaz de líneas de comando. Es posible que deba usar el registro manual, por ejemplo, si falla el registro automático o si quiere registrar un equipo existente en una cuenta nueva.

Puede encontrar la herramienta de registro en las siguientes ubicaciones:

- Windows: `Archivos de Programa\Acronis\RegisterAgentTool\register_agent.exe`
- Linux: `/usr/lib/Acronis/RegisterAgentTool/RegisterAgent`
- macOS: `/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent`

Para registrar un equipo con un nombre de usuario y una contraseña

En Windows

En la línea de comando, ejecute el siguiente comando:

```
<path to the registration tool> -o register -t cloud -a <service address> -u <user name>
-p <password>
```

Por ejemplo:

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

En Linux

En la línea de comando, ejecute el siguiente comando:

```
<path to the registration tool> -o register -t cloud -a <service address> -u <user name>
-p <password>
```

Por ejemplo:

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

En macOS

En la línea de comando, ejecute el siguiente comando:

```
<path to the registration tool> -o register -t cloud -a <service address> -u <user name>
-p <password>
```

Por ejemplo:

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

La <service address> es la URL que usa **para iniciar sesión en** el Cyber Protectservicio. Por ejemplo, `https://cloud.company.com`.

El <user name> y la <password> son las credenciales de la cuenta bajo la que se registrará el agente. No puede tratarse de una cuenta de administrador del partner. Si la contraseña contiene caracteres especiales o espacios en blanco, consulte "Contraseñas con caracteres especiales o espacios en blanco" (p. 162).

Pasos para registrar un equipo mediante un token de registro:

En Windows

En la línea de comando, ejecute el siguiente comando:

```
<path to the registration tool> -o register -t cloud -a <service address> --token
<registration token>
```

Por ejemplo:

```
<path to the registration tool> -o register -t cloud -a https://au1-cloud.company.com --
token 3B4C-E967-4FBD
```

En Linux

En la línea de comando, ejecute el siguiente comando:

```
<path to the registration tool> -o register -t cloud -a <service address> --token
<registration token>
```

Por ejemplo:

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

En macOS

En la línea de comando, ejecute el siguiente comando:

```
<path to the registration tool> -o register -t cloud -a <service address> --token
<registration token>
```

Por ejemplo:

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

Virtual Appliance

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

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

   Por ejemplo:

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

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

Nota

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

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

El token de registro es una serie de 12 caracteres, separados en tres segmentos por guiones. Para más información sobre cómo generar uno, consulte "Pasos para generar un token de registro" (p. 221).

Pasos para desregistrar un equipo

En Windows

En la línea de comando, ejecute el siguiente comando:

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

Por ejemplo:

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

En Linux

En la línea de comando, ejecute el siguiente comando:

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

Por ejemplo:

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

En macOS

En la línea de comando, ejecute el siguiente comando:

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

Por ejemplo:

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

Virtual Appliance

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

   ```
   register_agent -o unregister
   ```

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

Implementando Agent para oVirt (dispositivo virtual)

Para obtener información acerca del despliegue y configuración de Agente para oVirt (dispositivo virtual), consulte la documentación de Cyber Protection Cloud.

Implementación del Agente para Virtuozzo Hybrid Infrastructure (dispositivo virtual)

Para obtener información acerca del despliegue y configuración de Agente para Virtuozzo Hybrid Infrastructure (dispositivo virtual), consulte la documentación de Cyber Protection Cloud.

Autodetección de equipos

Con la autodetección, puede:

- Automatizar la instalación de agentes de protección y el registro de máquinas en el servidor de gestión mediante la detección de equipos en su dominio de Active Directory o su red local.
- Instalar y actualizar agentes de protección en varios equipos.
- Usar la sincronización con Active Directory para reducir los esfuerzos a la hora de aprovisionar recursos y gestionar equipos en un dominio de Active Directory grande.

Requisitos previos

Para llevar a cabo la autodetección, necesita al menos un equipo con un agente de protección instalado en su red local o en el dominio de Active Directory. Este agente se usa como agente de detección.

Importante
Solo los agentes instalados en equipos Windows pueden ser agentes de detección. Si no hay ningún agente de detección en su entorno, no podrá utilizar la opción **Varios dispositivos** en el panel **Añadir dispositivos**.

La instalación remota de agentes solo se admite en los equipos que ejecutan Windows (no es compatible con Windows XP). Para realizar la instalación remota en un equipo donde se ejecute Windows Server 2012 R2, debe tener la actualización KB2999226 de Windows instalada en ese equipo.

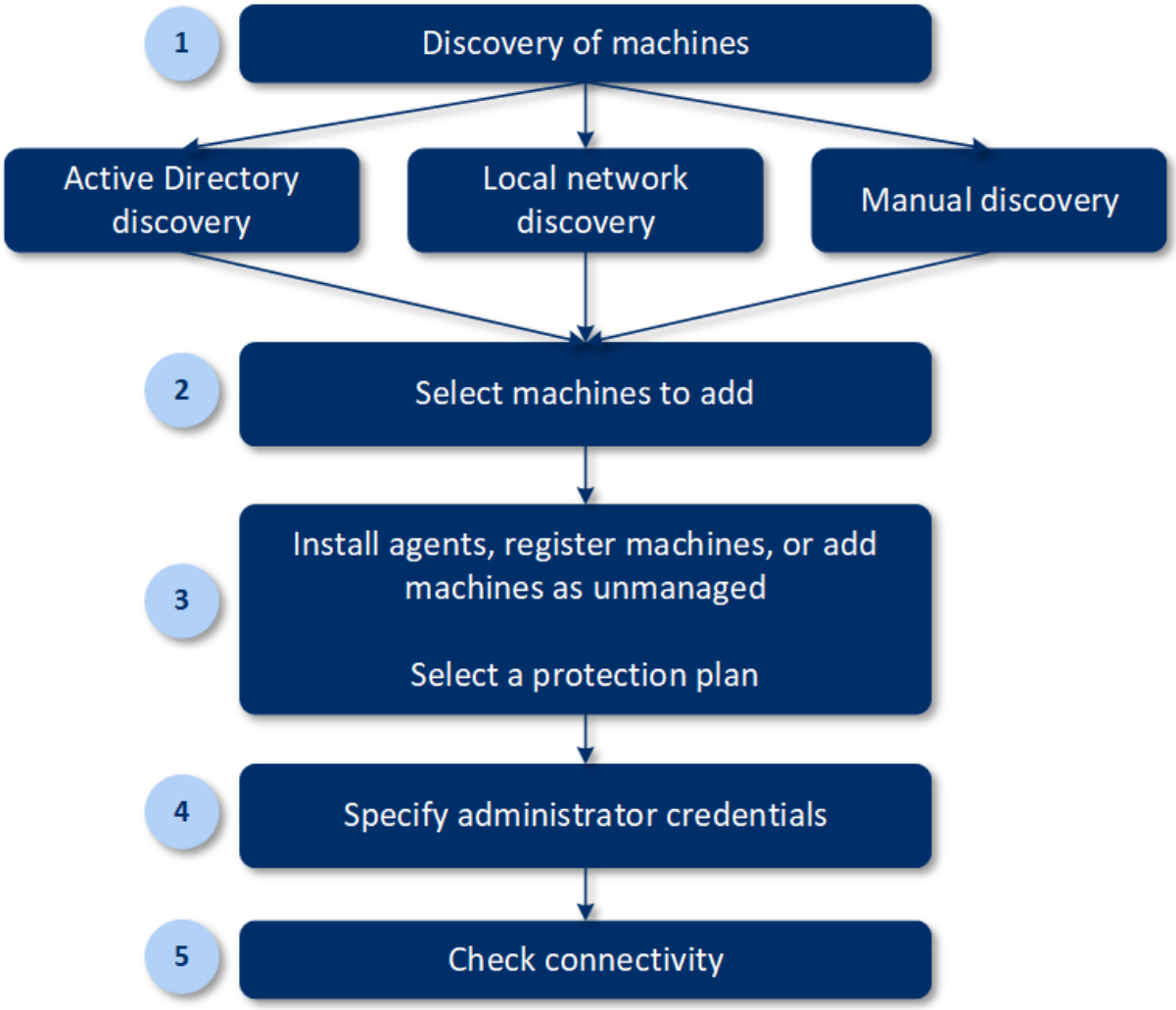
Cómo funciona la autodetección

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

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

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

El siguiente diagrama resume el proceso de autodetección.



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

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

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

- Registrar los equipos en la consola web (si ya hay un agente de protección instalado).
- Añadir los equipos como **equipos sin gestionar** a la consola web sin instalar ningún agente de protección.

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

4. Proporcione las credenciales de administrador para los equipos seleccionados.
5. Seleccione el nombre o la dirección IP del servidor de administración que el agente utilizará para acceder a ese servidor.

   De forma predeterminada, se selecciona el nombre del servidor. Puede que deba seleccionar la dirección IP en su lugar si su servidor de administración tiene más de una interfaz de red o si está experimentando problemas de DNS que provocan que el registro del agente falle.
6. Compruebe que puede conectarse a los equipos con las credenciales proporcionadas.

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

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

Autodetección y detección manual

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

Pasos para detectar equipos

1. En la consola web, vaya a **Dispositivos** > **Todos los dispositivos**.
2. Haga clic en **Agregar**.
3. En **Varios dispositivos**, haga clic en **Solo Windows**. Se abre el asistente de autodetección.
4. [Si hay unidades en su organización]. Seleccione una unidad. A continuación, en **Agente de detección**, podrá seleccionar los agentes asociados a la unidad seleccionada y sus unidades secundarias.
5. Seleccione el agente de detección que llevará a cabo el análisis para detectar equipos.
6. Seleccione el método de detección:
   - **Buscar en Active Directory**. Asegúrese de que el equipo con el agente de detección esté en el miembro del dominio de Active Directory.
   - **Analizar red local**. Si el agente de detección seleccionado no encuentra ningún equipo, seleccione otro agente de detección.

- **Especificar manualmente o importar desde un archivo**. Defina manualmente los equipos que quiere añadir o impórtelos desde un archivo de texto.

7. [Si se ha seleccionado el método de detección Active Directory] Seleccione cómo buscar equipos:
   - **En lista de unidades organizativas**. Seleccione el grupo de equipos que se va a añadir.
   - **Por consulta en dialecto LDAP**. Use la consulta en dialecto LDAP para seleccionar los equipos. La **base de búsqueda** define dónde buscar, mientras que la opción **Filtrar** le permite especificar el criterio de selección de los equipos.
8. [Si se ha seleccionado el método de detección red local o Active Directory] Use una lista para seleccionar los equipos que quiera añadir.

   [Si se ha seleccionado el método de detección manual] Especifique las direcciones IP o los nombres de servidor de los equipos, o bien importe la lista de equipos de un archivo de texto. El archivo debe contener las direcciones IP o los nombres de servidor, uno por línea. Aquí tiene un ejemplo de un archivo:

   ```
   156.85.34.10
   156.85.53.32
   156.85.53.12
   EN-L00000100
   EN-L00000101
   ```

   Cuando ya se han añadido las direcciones de los equipos manualmente o se han importado de un archivo, el agente intenta anclar los equipos añadidos y definir su disponibilidad.
9. Seleccione qué hacer después de la detección:
   - **Instalar agentes y registrar equipos**. Puede seleccionar qué componentes quiere instalar en los equipos si hace clic en **Seleccionar componentes**. Para obtener más información, consulte "Selección de componentes para la instalación". Puede instalar hasta 100 agentes de forma simultánea.

     En la pantalla **Seleccionar componentes**, defina la cuenta en la que se ejecutarán los servicios especificando **Cuenta de inicio de sesión para el servicio de agente**. Puede seleccionar una de las siguientes opciones:
     - **Usar cuentas de usuario del servicio** (opción predeterminada para el servicio de agente)

       Las cuentas de usuario del servicio son cuentas de sistema de Windows que se utilizan para ejecutar servicios. La ventaja de este ajuste es que las directivas de seguridad de dominios no afectan a los derechos de usuario de estas cuentas. De forma predeterminada, el agente se ejecuta desde la cuenta **Sistema local**.
     - **Cree una nueva cuenta**

       El nombre de cuenta del agente será Agent User.
     - **Utilice la siguiente cuenta**

       Si instala el agente en un controlador de dominios, el sistema le pedirá que especifique las cuentas actuales (o una misma cuenta) para cada agente. Por razones de seguridad, el sistema no crea automáticamente nuevas cuentas en un controlador de dominio.

     Si selecciona la opción **Crear una cuenta nueva** o **Utilice la siguiente cuenta**, asegúrese de que las directivas de seguridad de dominio no afecten a los derechos de las cuentas

relacionadas. Si se niegan los derechos de usuario para una cuenta durante la instalación, el componente podría no funcionar correctamente o no funcionar en absoluto.

- **Registrar equipos con agentes instalados**. Esta opción se usa si el agente ya está instalado en los equipos y solo tiene que registrarlos en Cyber Protect. Si no se encuentra ningún agente en los equipos, se añadirán como equipos **sin gestionar**.
- **Agregar como equipos sin gestionar**. El agente no se instalará en los equipos. Podrá verlos en la consola web e instalar o registrar el agente posteriormente.

[Si se ha seleccionado la acción posterior a la detección **Instalar agentes y registrar equipos**] **Reiniciar el equipo si es necesario:** si esta opción está habilitada, el equipo se reiniciará tantas veces como sea necesario para realizar la instalación.

Se puede requerir que se reinicie el equipo en uno de los siguientes casos:

- Se ha completado la instalación de los requisitos previos, pero es necesario reiniciar para continuar con la instalación.
- Se ha completado la instalación, pero es necesario reiniciar porque algunos archivos se bloquean durante la instalación.
- Se ha completado la instalación, pero es necesario reiniciar porque hay otro software previamente instalado.

[Si se ha seleccionado **Reiniciar el equipo si es necesario**] **No reinicie el equipo si está abierta la sesión de un usuario**: si esta opción está habilitada, el equipo no se reiniciará automáticamente en caso de que esté abierta la sesión del usuario en el sistema. Por ejemplo, si un usuario está trabajando cuando la instalación requiera que se reinicie el equipo, el sistema no se reiniciará.

Si se han instalado los requisitos previos, pero no se ha reiniciado el equipo porque estaba abierta la sesión de un usuario, para completar la instalación del agente tendrá que reiniciar el equipo e iniciar de nuevo la instalación.

Si se ha instalado el agente, pero no se ha reiniciado el equipo, tendrá que reiniciarlo.

[Si hay unidades en su organización] **Unidad en la que se registran los equipos**: seleccione la unidad en la que se registrarán los equipos.

Si ha seleccionado una de las dos primeras acciones posteriores a la detección, también existe una opción para aplicar el plan de protección a los equipos. Si tiene varios planes de protección, puede seleccionar el que quiera usar.

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

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

11. Seleccione el nombre o la dirección IP del servidor de administración que el agente utilizará para acceder a ese servidor.

De forma predeterminada, se selecciona el nombre del servidor. Puede que deba seleccionar la dirección IP en su lugar si su servidor de administración tiene más de una interfaz de red o si está experimentando problemas de DNS que provocan que el registro del agente falle.

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

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

Selección de componentes para la instalación

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

Componente	Descripción
Componentes obligatorios	
Agente para Windows	Este agente realiza copias de seguridad de discos, volúmenes y archivos, y se instalará en equipos Windows. Siempre estará instalado, no se seleccionará.
Componentes adicionales	
Agente para Hyper-V	Este agente realiza copias de seguridad de equipos virtuales Hyper-V y se instalará en servidores Hyper-V. Se instalará si se selecciona y detecta el rol Hyper-V en un equipo.
Agente para SQL	Este agente realiza copias de seguridad de bases de datos SQL Server y se instalará en equipos que ejecuten Microsoft SQL Server. Se instalará si se selecciona y detecta su aplicación en un equipo.
Agente para Exchange	Este agente realiza copias de seguridad de bases de datos y buzones de correo electrónico de Exchange y se instalará en equipos con la función Buzón de Microsoft Exchange Server. Se instalará si se selecciona y detecta su aplicación en un equipo.
Agente para Active Directory	Este agente realiza copias de seguridad de los datos de los servicios de dominio de Active Directory y se instalará en controladores de dominio. Se instalará si se selecciona y detecta su aplicación en un equipo.
Agente para VMware (Windows)	Este agente realiza copias de seguridad de equipos virtuales VMware y se instalará en equipos Windows que tengan acceso de red a vCenter Server. Se instalará si se selecciona.
Agente para Office 365	Este agente realiza copias de seguridad de los buzones de correo de Microsoft 365 en un destino local y se instalará en máquinas Windows. Se instalará si se selecciona.
Agent para Oracle	Este agente realiza copias de seguridad de bases de datos Oracle y

	se instalará en equipos que ejecuten Oracle Database. Se instalará si se selecciona.
Cyber Protect Monitor	Este componente permite a un usuario supervisar las tareas en ejecución en el área de notificación y se instalará en equipos Windows. Se instalará si se selecciona.
Herramienta de línea de comandos	Cyber Protect admite la interfaz de la línea de comandos con la utilidad acrocmd; acrocmd no contiene ninguna herramienta que ejecute los comandos de forma física. Solo proporciona la interfaz de la línea de comandos para los componentes de Cyber Protect: agentes y el servidor de gestión. Se instalará si se selecciona.
Bootable Media Builder	Este componente permite a los usuarios crear un dispositivo de arranque y, si se selecciona, se instalará en equipos Windows.

Gestión de equipos detectados

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

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

Nombre	Descripción
Nombre	El nombre del equipo. La dirección IP se mostrará si no se puede detectar el nombre del equipo.
Dirección IP	La dirección IP del equipo.
Tipo de detección	El método de detección empleado para detectar el equipo.
Unidad organizativa	La unidad organizativa de Active Directory a la que pertenece el equipo. Esta columna se muestra si ve la lista de equipos en **Equipos sin gestionar** > **Active Directory**.
Sistema operativo	El sistema operativo instalado en el equipo.

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

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

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

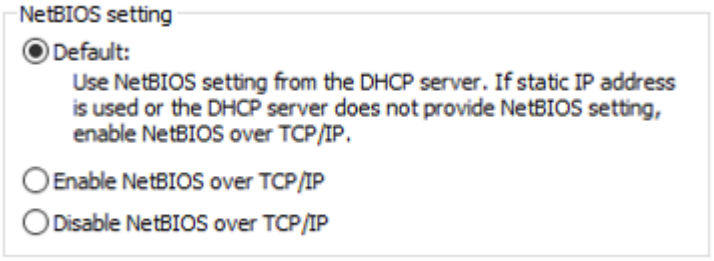
Cuando el agente de protección esté instalado en los equipos, estos aparecerán en la sección **Dispositivos** > **Equipos con agentes**.

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

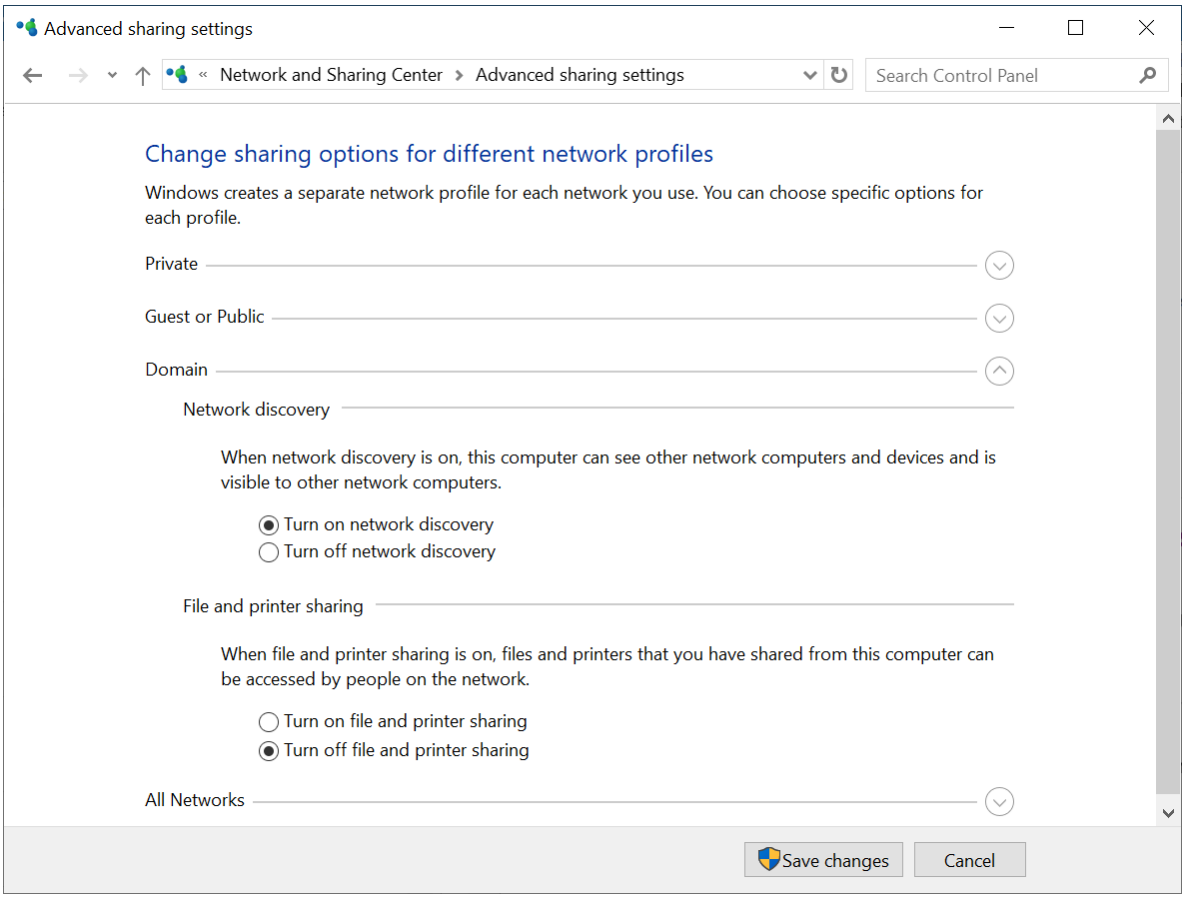
Solución de problemas

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

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



- En **Panel de control** > **Centro de redes y uso compartido** > **Configuraciones avanzadas de uso compartido**, active la detección de redes.



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

Implementación del Agente para VMware (dispositivo virtual) desde una plantilla de OVF

Antes de empezar

Requisitos del sistema para el agente

De forma predeterminada, se asignan al dispositivo virtual 4 GB de RAM y 2 vCPU, que son óptimos y suficientes para llevar a cabo la mayoría de las operaciones.

Para mejorar el rendimiento de copia de seguridad y evitar fallos relacionados con la memoria RAM insuficiente, le recomendamos que aumente estos recursos a 16 GB de RAM y 4 vCPU en los casos que sean más exigentes. Por ejemplo, aumente los recursos asignados cuando espere que la transferencia de datos de la copia de seguridad exceda los 100 MB por segundo o si realiza una copia de seguridad de varias máquinas virtuales simultáneamente con discos duros grandes (500 GB o más).

Las unidades de disco virtual del propio dispositivo no ocupan más de 6 GB. No importa si el formato del disco es ligero o denso, ya que esto no afecta al rendimiento del dispositivo.

Nota
Las API de vStorage deben estar instaladas en el host ESXi para habilitar las copias de seguridad de máquinas virtuales. Consulte https://kb.acronis.com/content/14931.

¿Cuántos agentes necesito?

Aunque un dispositivo virtual puede proteger todo un entorno vSphere, lo mejor es implementar un dispositivo virtual por clúster vSphere (o por host, si no hay clústeres). Esto provoca que las copias de seguridad sean más rápidas porque el dispositivo puede adjuntar los discos de los que se ha realizado la copia mediante el transporte HotAdd y, por tanto, la transferencia de datos de la copia de seguridad se dirige desde un disco local a otro.

Es normal usar tanto el dispositivo virtual como el agente para VMware (Windows) a la vez, siempre que estén conectados al mismo vCenter Server *o* a diferentes hosts ESXi. Evite los casos en los que un agente se conecte a un ESXi directamente y otro se conecte al vCenter Server que gestione este ESXi.

No le recomendamos usar un almacenamiento conectado localmente (es decir, almacenar copias de seguridad en discos virtuales añadidos al dispositivo virtual) si tiene más de un agente. Para obtener más detalles, consulte Utilización de un almacenamiento conectado localmente.

Deshabilitar el DRS automático para el agente

Si el dispositivo virtual se implementa en un clúster vSphere, asegúrese de deshabilitar el vMotion automático. En la configuración del clúster de DRS, habilite los niveles de automatización del equipo virtual individual y, a continuación, establezca la opción **Nivel de automatización** del dispositivo virtual en **Deshabilitado**.

Implementación de la plantilla OVF

Ubicación de la plantilla del OVF

La plantilla del formato de virtualización abierta (OVF, por sus siglas en inglés) está formada por un archivo .ovf y dos .vmdk.

En implementaciones locales

Cuando se haya instalado el servidor de gestión, el paquete OVF del dispositivo virtual estará en la carpeta **%ProgramFiles%\Acronis\ESXAppliance** (en Windows) o **/usr/lib/Acronis/ESXAppliance** (en Linux).

En implementaciones en el cloud

1. Haga clic en**Todos los dispositivos** > **Añadir** > **VMware ESXi** > **Dispositivo virtual (OVF)**.
   El archivo .zip se descarga en su equipo.
2. Descomprímalo.

Implementación de la plantilla OVF

1. Asegúrese de que se puede acceder a los archivos de plantilla de OVF desde el equipo que ejecuta el vSphere Client.
2. Abra vSphere Client e inicie sesión en vCenter Server.
3. Implemente la plantilla de OVF.
   - Al configurar el almacenamiento, seleccione el almacén de datos compartido si existe. No importa si el formato del disco es ligero o denso, ya que esto no afecta al rendimiento del dispositivo.
   - Al configurar las conexiones de red en implementaciones en el cloud, asegúrese de seleccionar una red que permita la conexión a Internet para que el agente pueda registrarse adecuadamente en el cloud. Al configurar las conexiones de red en implementaciones locales, seleccione una red que incluya el servidor de gestión.

Configuración del dispositivo virtual

1. **Inicio del dispositivo virtual**
   En vSphere Client, muestre el **Inventario**, haga clic con el botón derecho sobre el nombre del dispositivo virtual y, a continuación, seleccione **Activar** > **Encender**. Seleccione la pestaña **Consola.**
2. **Servidor proxy**
   Si hay un servidor proxy habilitado en la red:
   a. Para iniciar el shell de comandos, presione Ctrl+Máyus+F2 en la interfaz de usuario del dispositivo virtual.
   b. Abra el archivo **/etc/Acronis/Global.config** en un editor de texto.
   c. Realice uno de los siguientes procedimientos:
      - Si especificó la configuración del servidor proxy durante la instalación del agente, busque la sección siguiente:

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

- En caso contrario, copie les líneas anteriores y péguelas en el archivo entre las etiquetas `<registry name="Global">...</registry>`.

d. Reemplace `ADDRESS` por el nombre del host o la dirección IP del servidor proxy y `PORT` por el valor decimal del número de puerto.

e. Si su servidor proxy necesita que se autentifique, sustituya `LOGIN` Y `PASSWORD` por las credenciales del servidor proxy. De lo contrario, elimine estas líneas del archivo.

f. Guarde el archivo.

g. Abra el archivo **/opt/acronis/etc/aakore.yaml** en un editor de texto.

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

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

i. Sustituya `proxy_login` y `proxy_password` por las credenciales del servidor proxy y `proxy_address:port` por la dirección y el número de puerto del servidor proxy.

j. Ejecute el comando de **reboot**.

De lo contrario, omita este paso.

3. **Configuraciones de red**

   La conexión de red del agente se configura automáticamente con el Protocolo de configuración de host (DHCP). Para cambiar la configuración predeterminada, en **Opciones del agente**, **eth0**, haga clic en **Cambiar** y especifique las configuraciones de red deseadas.

4. **vCenter/ESX(i)**

   En **Opciones del agente**, en **vCenter/ESX(i)**, haga clic en **Cambiar** y especifique el nombre o la dirección IP de vCenter Server. El agente podrá realizar la copia de seguridad y recuperar cualquier equipo virtual gestionado por vCenter Server.

   Si no utiliza un vCenter Server, especifique el nombre o la dirección IP del servidor ESXi cuyos equipos virtuales desea incluir en la copia de seguridad y recuperar. Normalmente, las copias de seguridad se ejecutan más rápido cuando el agente realiza las copias de seguridad de equipos virtuales alojados en su propio servidor.

   Especifique las credenciales que el agente utilizará para conectarse a vCenter Server o ESXi. Le recomendamos utilizar una cuenta que tenga asignado el rol de **Administrador**. En otro caso, proporcione una cuenta con los privilegios necesarios en el servidor vCenter Server oESXi.

   Puede hacer clic en **Verificar la conexión** para asegurarse de que las credenciales de acceso son las correctas.

5. **Servidor de gestión**

   a. En **Opciones del agente** > **Servidor de gestión**, haga clic en **Cambiar**.

   b. En **Nombre del servidor/IP**, realice uno de los siguientes procedimientos:

   - Para llevar a cabo una implementación local, seleccione **Local**. Especifique el nombre del servidor o la dirección IP del equipo donde está instalado el servidor de gestión.

- Para llevar a cabo una implementación en el cloud, seleccione **Cloud**. El software muestra la dirección del servicio de ciberprotección. No cambie esta dirección a menos que se le indique lo contrario.

c. En **Nombre de usuario** y **Contraseña**, realice una de las siguientes acciones:
   - Para una implementación local, especifique el nombre de usuario y la contraseña de un administrador del servidor de gestión.
   - Para una implementación en la nube, indique el nombre de usuario y la contraseña para el servicio de ciberprotección. El agente y los equipos virtuales que este gestiona se registrarán en esta cuenta.

6. **Zona horaria**

   En **Equipo virtual**, en **Zona horaria**, haga clic en **Cambiar**. Seleccione la zona horaria de su ubicación para asegurar que las operaciones planificadas se ejecutan en el momento apropiado.

7. **[Opcional] Almacenamientos locales**

   Puede conectar un disco adicional al dispositivo virtual para que Agente para VMware pueda realizar la copia de seguridad en este almacenamiento conectado localmente.

   Añada el disco al editar los ajustes del equipo virtual y haga clic en **Actualizar**. El enlace **Crear almacenamiento** está ahora disponible. Haga clic en este enlace, seleccione el disco y, a continuación, especifique una etiqueta para este.

Implementación de Agent para Scale Computing HC3 (dispositivo virtual)

Antes de empezar

Este dispositivo es un equipo virtual preconfigurado que se implementa en el clúster de Scale Computing HC3. Contiene un agente de protección que le permite administrar la ciberprotección de todos los equipos virtuales del clúster.

Requisitos del sistema para el agente

Al implementar el dispositivo virtual, puede elegir entre distintas combinaciones de vCPU y RAM. La combinación de 2 vCPU y 4 GB de RAM es óptima y suficiente para llevar a cabo la mayoría de las operaciones. Le recomendamos que aumente estos recursos a 4 vCPU y 8 GB de RAM si se espera que el ancho de banda de la transferencia de datos de la copia de seguridad supere los 100 Mb por segundo (por ejemplo, en redes de 10 Gbits) a fin de mejorar el rendimiento de copia de seguridad.

Las unidades de disco virtual del propio dispositivo no ocupan más de 6 GB.

¿Cuántos agentes necesito?

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

Si tiene más de un agente en un clúster, los equipos virtuales se distribuyen automáticamente entre ellos de forma equitativa, de modo que cada agente gestione el mismo número de equipos.

La redistribución automática se realiza cada vez que un desequilibrio de cargas entre los agentes llega al 20 por ciento. Puede suceder, por ejemplo, al añadir o eliminar un equipo o un agente. Por ejemplo, se da cuenta que necesita más agentes para ayudar al rendimiento e implementa un dispositivo virtual adicional en el clúster. El servidor de gestión asignará los equipos más adecuados al nuevo agente. La carga de los agentes anteriores se reducirá. Cuando retira un agente del servidor de gestión, los equipos asignados al agente se distribuyen entre los agentes restantes. Sin embargo, esto no sucederá si un agente se daña o elimina manualmente del clúster de Scale Computing HC3. La redistribución comenzará solo después de eliminar dicho agente de la interfaz web de Cyber Protect.

Puede ver el resultado de la distribución automática:

- En la columna **Agente** para cada equipo virtual en la sección **Todos los dispositivos**
- En la sección **Equipos virtuales asignados** del panel **Detalles** cuando un agente está seleccionado en **Configuración** > **Agentes**

Implementar el dispositivo virtual

1. Inicie sesión en su cuenta de Cyber Protect.
2. Haga clic en **Dispositivos** > **Todos los dispositivos** > **Añadir** > **Scale Computing HC3**.
3. Seleccione el número de dispositivos virtuales que desea implementar.
4. Especifique la dirección IP o el nombre del servidor en el clúster de Scale Computing HC3.
5. Especifique las credenciales de una cuenta que tenga el rol **Crear/editar equipo virtual** asignado en este clúster.
6. Especifique una red compartida que se utilizará para el almacenamiento temporal del archivo de imagen del dispositivo virtual. Se requiere un mínimo de 2 GB de espacio libre.
7. Especifique las credenciales de una cuenta que tenga acceso de lectura y escritura a esta red compartida.
8. Haga clic en **Implementar**.

Cuando se complete la implementación, configure el dispositivo virtual.

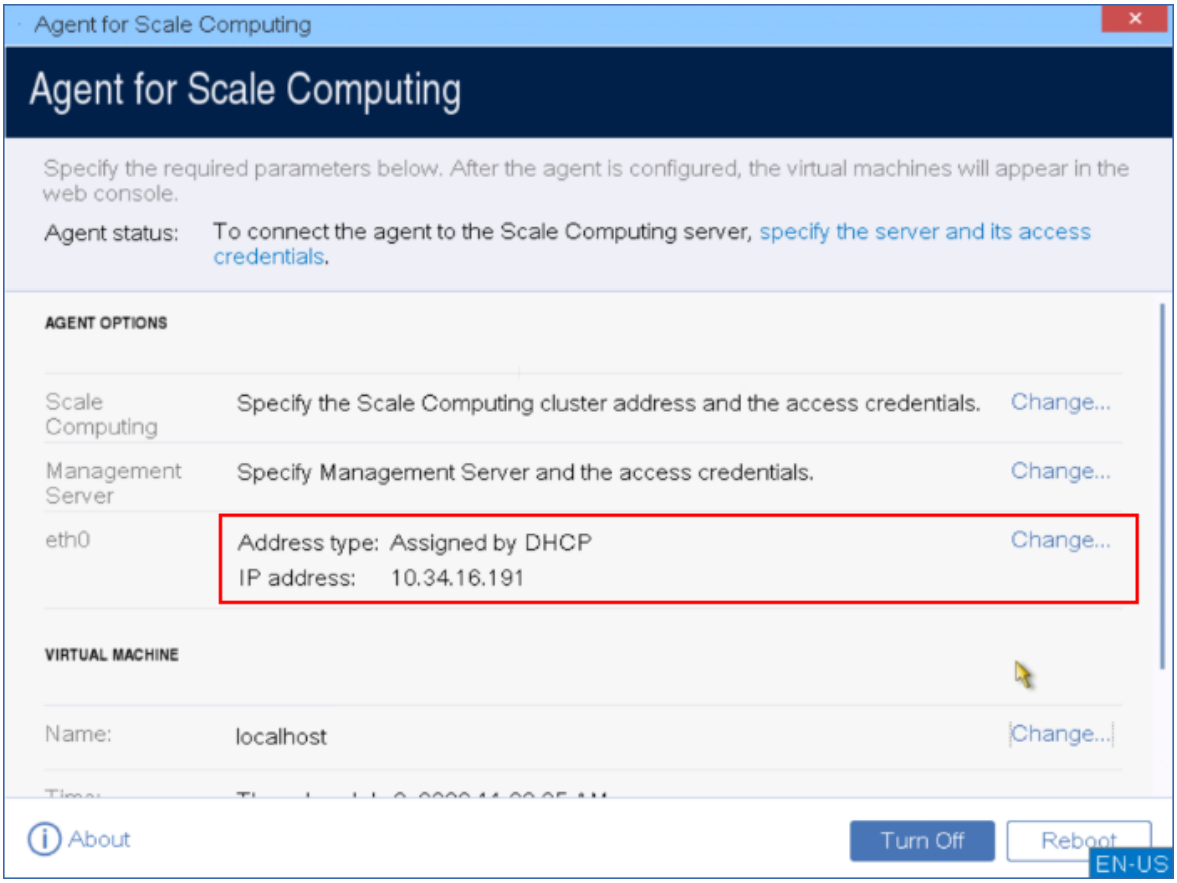
Configuración del dispositivo virtual

Después de implementar el dispositivo virtual, debe configurarlo de modo que pueda alcanzar tanto el clúster de Scale Computing HC3 que protegerá como el servidor de gestión de Cyber Protect.

Para configurar la aplicación virtual

1. Inicie sesión en su cuenta de Scale Computing HC3.
2. Seleccione el equipo virtual con el agente que necesite configurar y haga clic en **Consola**.

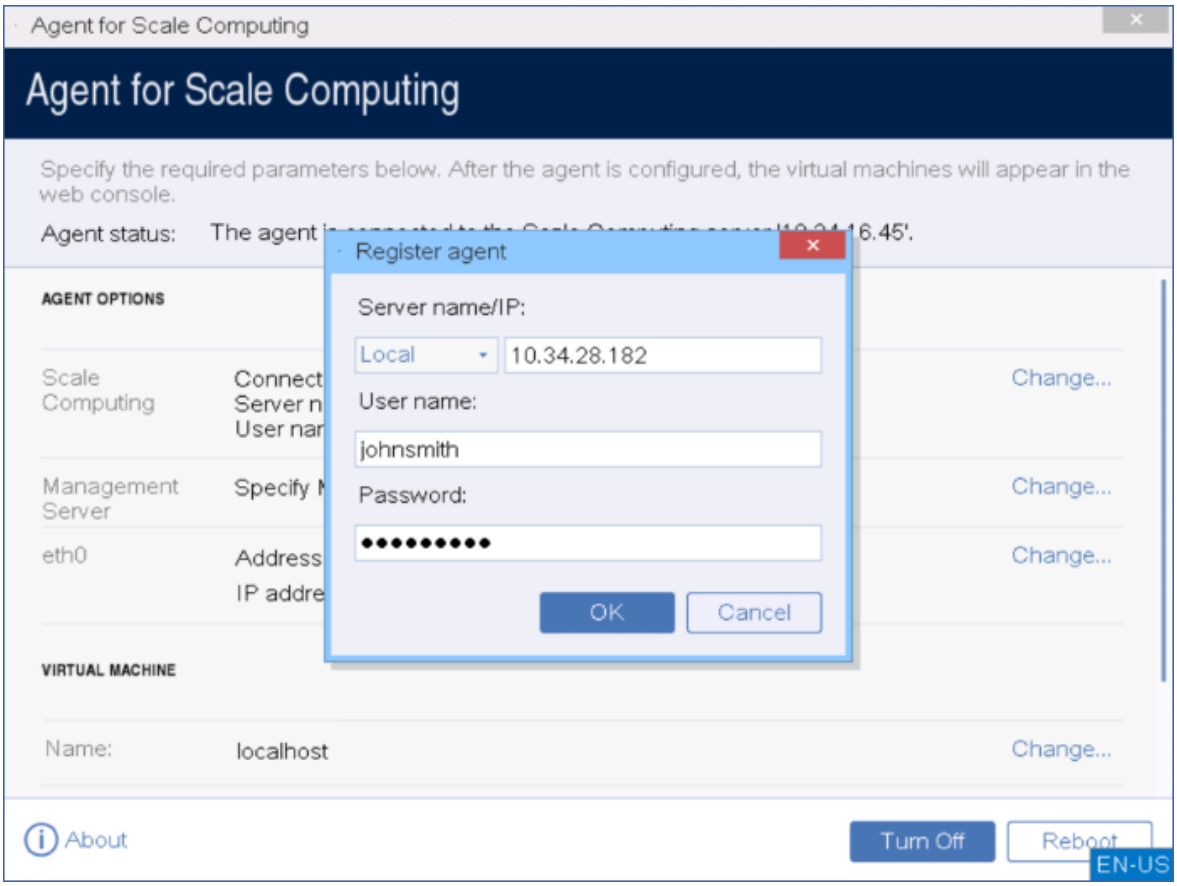
3. Configure las interfaces de red del dispositivo. Puede haber una o más interfaces a configurar, en función del número de redes que utilice el dispositivo. Asegúrese de que las direcciones DHCP asignadas automáticamente (de haberlas) sean válidas dentro de las redes que utiliza su equipo virtual, o bien asígnelas de forma manual.



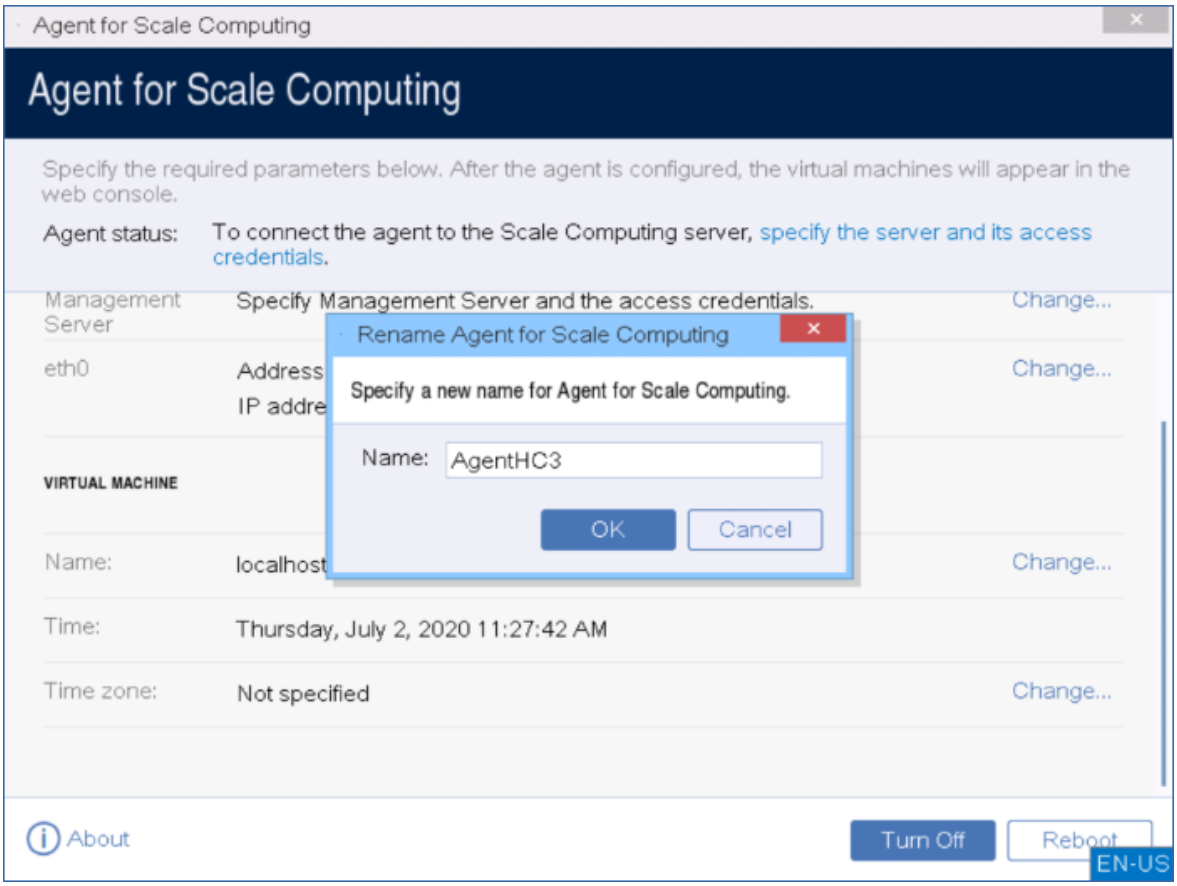
4. Especifique la dirección y las credenciales del clúster de Scale Computing HC3:
   - El nombre del DNS o la dirección IP del clúster.
   - En los campos **Nombre de usuario** y **Contraseña**, introduzca las credenciales de la cuenta de Scale Computing HC3 que tenga asignada la función adecuada.

   Puede hacer clic en **Verificar la conexión** para asegurarse de que las credenciales de acceso son las correctas.

5. Especifique la dirección del servidor de gestión de Cyber Protect y las credenciales para acceder a él.



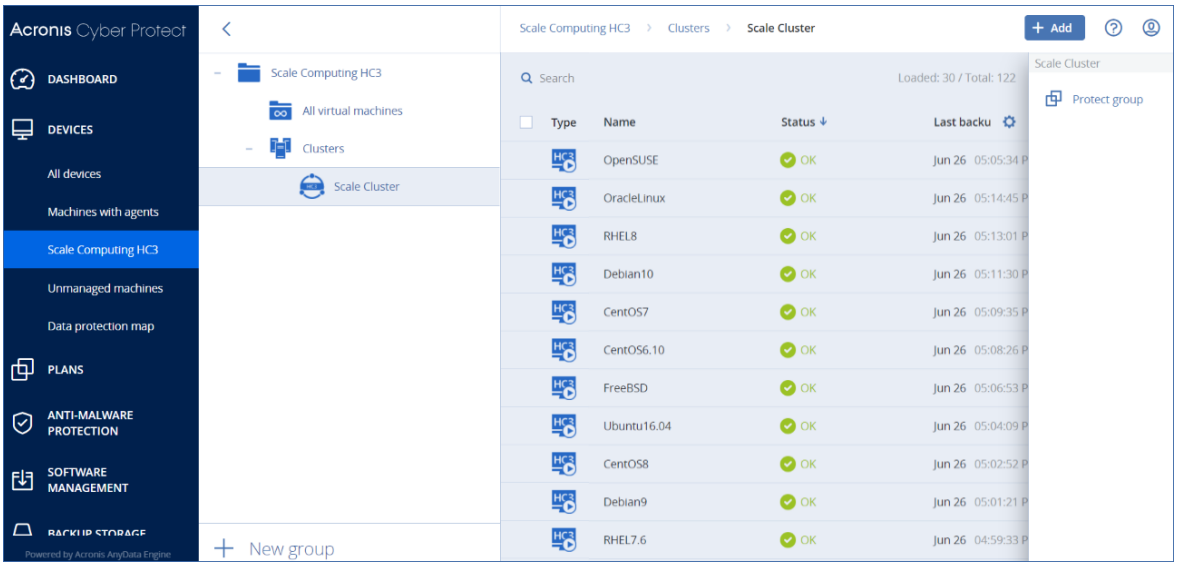
6. [Opcional] Especifique un nombre para el agente. Este nombre aparecerá en la consola web de Cyber Protect.



7. [Opcional] Seleccione la zona horaria de su ubicación para asegurar que las operaciones planificadas se ejecutan en el momento apropiado.

Pasos para proteger los equipos virtuales en el clúster de Scale Computing HC3

1. Inicie sesión en su cuenta de Cyber Protect.
2. Vaya a **Dispositivos** > **Scale Computing HC3**> <your cluster>, o busque sus equipos en **Dispositivos** > **Todos los dispositivos**.
3. Seleccione los equipos deseados y aplíqueles un plan de protección.



Agent para Scale Computing HC3: roles obligatorios

Esta sección describe los roles necesarios para realizar operaciones con equipos virtuales Scale Computing HC3 y, además, para la implementación de dispositivos virtuales.

Operación	Rol
Copias de seguridad de un equipo virtual	Copia de seguridad Crear/editar equipo virtual Borrar equipo virtual
Recuperación en un equipo virtual existente	Copia de seguridad Crear/editar equipo virtual Control de energía del equipo virtual Borrar equipo virtual Configuración del clúster
Recuperación en un nuevo equipo virtual	Copia de seguridad Crear/editar equipo virtual Control de energía del equipo virtual Borrar equipo virtual Configuración del clúster
Implementación de un dispositivo virtual	Crear/editar equipo virtual

Implementación de agentes mediante la directiva de grupo

Puede instalar (o implementar) de manera central el Agente para Windows en los equipos que pertenecen a un dominio de Active Directory usando la directiva de grupo.

En esta sección, encontrará cómo instalar un objeto de directiva de grupo para implementar agentes en un dominio completo o en la unidad organizacional de los equipos.

Siempre que un equipo inicie sesión en el dominio, el objeto de directiva de grupo resultante garantizará que el agente se encuentre instalado y registrado.

Requisitos previos

Antes de que proceda a la implementación de un Agente, asegúrese de que:

- Tiene un dominio de Active Directory con un controlador de dominio ejecutando Microsoft Windows Server 2003 o una versión posterior.
- Es miembro del grupo **Administradores del dominio** en el dominio.
- Ha descargado el programa de instalación **Todos los agentes para la instalación en Windows**. El enlace de descarga está disponible en la página **Añadir dispositivos** de la consola web de Cyber Protect.

Paso 1: Generar un token de registro

Un token de registro transmite su identidad al programa de instalación sin almacenar el nombre de usuario ni la contraseña para la consola web de Cyber Protect. Esto le permite registrar cualquier número de equipos usando su cuenta. Para más seguridad, los tokens tienen una duración limitada.

Pasos para generar un token de registro

1. Inicie sesión en la consola web de Cyber Protect usando las credenciales de la cuenta a la que los equipos deberían estar asignados.
2. Haga clic en **Todos los dispositivos** > **Añadir**.
3. Desplácese hasta **Token de registro** y haga clic en **Generar**.
4. Especifique la duración del token y haga clic en **Generar token**.
5. Copie el token o escríbalo. Asegúrese de guardar el token si necesita volver a usarlo.
   Puede hacer clic en **Administrar tokens activos** para ver y administrar los tokens ya generados. Tenga en cuenta que, por motivos de seguridad, en esta tabla no se muestran los valores de los tokens completos.

Paso 2: Creación de la transformación .mst y extracción del paquete de instalación

1. Conéctese como administrador en cualquier equipo del dominio.
2. Cree una carpeta compartida que contendrá los paquetes de instalación. Asegúrese de que los usuarios del dominio puedan acceder a la carpeta compartida, por ejemplo, manteniendo la configuración de uso compartido predeterminada para **Todos**.
3. Inicie el programa de instalación.
4. Haga clic en **Crear archivos .mst y .msi para una instalación sin supervisión**.
5. Compruebe o modifique la configuración de instalación que se añadirá al archivo .mst. Al especificar el método de conexión al servidor de gestión, seleccione **Usar un token de registro** y especifique el token generado.
6. Haga clic en **Continuar**.
7. En **Guardar los archivos en**, especifique la ruta para el archivo que haya creado.
8. Haga clic en **Generar**.

Como consecuencia, se generará la transformación .mst y los paquetes de instalación .msi y .cab se extraerán a la carpeta que creó.

Paso 3: Configuración de objetos de directiva de grupo

1. Conéctese al controlador de dominio como un administrador de dominio y, si el dominio tiene más de un controlador de dominio, conéctese a cualquiera de ellos como un administrador de dominio.
2. Si tiene pensado implementar un Agente en una unidad organizacional, asegúrese de que la unidad organizacional existe en el dominio. De lo contrario, omita este paso.
3. En el menú **Inicio** , seleccione **Herramientas administrativas** y haga clic en **Equipos y usuarios de Active Directory** (en Windows Server 2003) o en **Gestión de Directiva de grupo** (en Windows Server 2008 y versiones posteriores).
4. En Windows Server 2003:
   - Haga clic con el botón derecho en el nombre del dominio o unidad organizativa y después haga clic en **Propiedades**. En el cuadro de diálogo, haga clic en la pestaña **Directiva de grupo** y después en **Nueva**.

   En Windows Server 2008 y versiones posteriores:
   - Haga clic con el botón derecho del ratón sobre el dominio o unidad organizativa y después haga clic en **Crear un GPO en este dominio y vincularlo aquí**.
5. Llame al nuevo objeto de directiva de grupo **Agente para Windows.**
6. Abra el objeto de directiva de grupo de **Agente para Windows** para editar de la siguiente manera:
   - En Windows Server 2003, haga clic en el objeto de directiva de grupo y, a continuación, haga clic en **Editar**.
   - En Windows Server 2008 y versiones posteriores, debajo de **Objetos de directiva de grupo**, haga clic con el botón derecho en Objeto de directiva de grupo y, después, haga clic en **Editar**.
7. En el complemento del editor de objeto de directiva de grupo, expanda **Configuración del equipo**.
8. En Windows Server 2003 y Windows Server 2008:
   - Expanda **Configuración de software**.

   En Windows Server 2012 y versiones posteriores:
   - Expanda **Directivas** > **Configuración de software**.
9. Haga clic con el botón derecho sobre **Instalación de software**, después seleccione **Nueva** y haga clic en **Paquete**.
10. Seleccione el paquete de instalación .msi del agente en la carpeta compartida que creó anteriormente y haga clic en **Abrir**.
11. En el cuadro de diálogo **Implementar software**, haga clic en **Avanzado** y después en **Aceptar**.
12. En la pestaña **Modificaciones**, haga clic en **Añadir** y seleccione la transformación .mst que creó anteriormente.
13. Haga clic en **Aceptar** para cerrar el cuadro de diálogo **Implementar software**.

Actualización de dispositivos virtuales

Implementaciones locales

Para actualizar un dispositivo virtual (Agente para VMware o Agente para Scale Computing HC3) con una versión inferior a la 15.24426 (lanzada en septiembre de 2020), siga el procedimiento disponible en "Actualizar agentes" (p. 224).

Pasos para actualizar la versión 15.24426 o posterior del dispositivo virtual

1. Descargue el paquete de actualización según se describe en http://kb.acronis.com/latest.
2. Guarde los archivos `tar.bz` en el siguiente directorio del equipo del servidor de gestión:
   - Windows: `C:\Program Files\Acronis\VirtualAppliances\va-updates`
   - Linux: `/usr/lib/Acronis/VirtualAppliances/va-updates`
3. En la consola web de Cyber Protect, haga clic en **Configuración** > **Agentes**.
   El software muestra la lista de equipos. Los equipos con dispositivos virtuales obsoletos tienen un signo de exclamación naranja.
4. Seleccione los equipos en los que desea actualizar los dispositivos virtuales. Estos equipos deben estar conectados.
5. Haga clic en **Actualizar Agente**.
6. Seleccione el agente de implementación.
7. Especifique las credenciales de una cuenta con privilegios administrativos en el equipo de destino.
8. Seleccione el nombre o la dirección IP que el agente utilizará para acceder al servidor de gestión.
   De forma predeterminada, se elige el nombre del servidor. Es posible que tenga que cambiar este ajuste si el servidor DNS no puede resolver el nombre a la dirección IP, lo que ocasiona un error durante el registro del dispositivo virtual.

El progreso de la actualización aparece en la pestaña **Actividades**.

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

Implementación en la nube

Para obtener más información sobre cómo actualizar un dispositivo virtual en el despliegue en la nube, consulte Actualización de agentes en la documentación de la nube.

Actualizar agentes

Requisitos previos

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

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

Puede actualizar agentes con la consola web de Cyber Protect o repitiendo su instalación de cualquier modo disponible. Para actualizar varios agentes simultáneamente, siga el procedimiento indicado a continuación.

Pasos para actualizar agentes con la consola web de Cyber Protect

1. [Solo en implementaciones locales] Actualice el servidor de gestión.
2. [Solo en implementaciones locales] Asegúrese de que los paquetes de instalación estén presentes en el equipo con el servidor de gestión. Para ver los pasos exactos, consulte "Adición de un equipo que ejecute Windows" > "Paquetes de instalación".
3. En la consola web de Cyber Protect, haga clic en **Configuración** > **Agentes**.
   El software muestra la lista de equipos. Los equipos con versiones de agentes obsoletas tienen un signo de exclamación naranja.
4. Seleccione los equipos en los que desea actualizar los agentes. Los equipos deben estar conectados.
5. Haga clic en **Actualizar Agente**.
6. Seleccione el agente de implementación.
7. Especifique las credenciales de una cuenta con privilegios administrativos en el equipo de destino.
8. Seleccione el nombre o la dirección IP del servidor de administración que el agente utilizará para acceder a ese servidor.
   De forma predeterminada, se selecciona el nombre del servidor. Puede que deba seleccionar la dirección IP en su lugar si su servidor de administración tiene más de una interfaz de red o si está experimentando problemas de DNS que provocan que el registro del agente falle.
9. [Solo en implementaciones locales] El progreso de la actualización aparece en la pestaña **Actividades**.

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

Pasos para actualizar las definiciones de Cyber Protect en un equipo

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

Pasos para asignar el rol de actualizador a un agente

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

Pasos para borrar los datos de la caché en un agente

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

Actualización de agentes en cargas de trabajo protegidas por BitLocker

Las actualizaciones de agentes que introducen cambios en Startup Recovery Manager interfieren con BitLocker en cargas de trabajo en las que tanto BitLocker como Startup Recovery Manager están habilitados. En este caso, después de un reinicio, se requiere la clave de recuperación de BitLocker. Para mitigar este problema, suspenda o deshabilite BitLocker antes de actualizar el agente.

Puede comprobar si una actualización introduce cambios en Startup Recovery Manager en las notas de versión de cada nueva versión de Acronis Cyber Protect.

Pasos para instalar la actualización

1. En la carga de trabajo en la que actualizará el agente, suspenda o desactive BitLocker.
2. Actualice el agente.
3. Reinicie la carga de trabajo.
4. Active BitLocker.

Actualización a Acronis Cyber Protect 15

Puede actualizar un producto anterior a Acronis Cyber Protect 15 de las siguientes formas:

- Directamente, sin desinstalar el producto anterior.
  Esta opción solo está disponible en Acronis Backup 12.5, actualización 5 (compilación 16180) y posteriores.
- Desinstalando un producto anterior e instalando una copia nueva de Acronis Cyber Protect 15.
  Esta opción está disponible para todos los productos aptos. Para obtener más información sobre estos productos, consulte este artículo de la base de conocimientos.

Nota
Le recomendamos que realice copias de seguridad de su sistema antes de actualizarlo. De este modo, podrá volver a la configuración original en caso de fallo en la actualización.

Para iniciar la actualización, ejecute el programa de instalación y siga las instrucciones en pantalla.

El servidor de gestión de Acronis Cyber Protect 15 es compatible con versiones anteriores y con agentes de la versión 12.5. Sin embargo, dichos agentes no son compatibles con las Funciones de Cyber Protect.

La actualización de agentes no interfiere con los conjuntos de copias de seguridad existentes y su configuración.

Desinstalación del producto

Si desea quitar componentes de producto individuales de un equipo, ejecute el programa de instalación, elija modificar el producto y desmarque la selección de los componentes que desea quitar. Los enlaces a los programas de instalación están presentes en la página **Descargas** (haga clic en el icono de cuenta en la esquina superior derecha > **Descargas**).

Si desea quitar todos los componentes de producto de un equipo, siga los pasos que se describen a continuación.

Advertencia.
En implementaciones locales, tenga mucho cuidado al seleccionar los componentes que desee desinstalar.

Si desinstala el servidor de gestión por error, la consola web de Cyber Protect dejará de estar disponible y ya no podrá realizar copias de seguridad ni recuperaciones en las máquinas que estaban registradas en el servidor de gestión desinstalado.

En Windows

1. Inicie sesión como administrador.
2. Vaya a **Panel de control** y luego seleccione **Programas y características** (**Añadir o quitar programas** en Windows XP) >**Acronis Cyber Protect** > **Desinstalar**.
3. [Opcional] Seleccione la casilla de verificación **Eliminar los registros y las opciones de configuración**.

   No marque esta casilla de verificación si va a desinstalar un agente, pero tiene previsto volverlo a instalar. Si selecciona la casilla de verificación, el equipo podría duplicarse en la consola web de Cyber Protect y las copias de seguridad del antiguo equipo podrían no asociarse al nuevo equipo.
4. Confirme su decisión.

En Linux

1. Como usuario raíz, ejecute **/usr/lib/Acronis/BackupAndRecovery/uninstall/uninstall**.
2. [Opcional] Seleccione la casilla de verificación **Limpiar todos los rastros del producto (Eliminar los registros, tareas, bóvedas y opciones de configuración del producto)**.
   No marque esta casilla de verificación si va a desinstalar un agente, pero tiene previsto volverlo a instalar. Si selecciona la casilla de verificación, el equipo podría duplicarse en la consola web de Cyber Protect y las copias de seguridad del antiguo equipo podrían no asociarse al nuevo equipo.
3. Confirme su decisión.

En macOS

1. Haga doble clic sobre el archivo de instalación (.dmg).
2. Espere mientras el sistema operativo monta la imagen del disco de instalación.
3. Dentro de la imagen, haga doble clic en **Desinstalar**.
4. Si se le pide, proporcione las credenciales del administrador.
5. Confirme su decisión.

Eliminación de Agent for VMware (Virtual Appliance)

1. Abra vSphere Client e inicie sesión en vCenter Server.
2. Si el dispositivo virtual está encendido, haga clic sobre él con el botón derecho y luego elija **Activar** > **Apagar**. Confirme su decisión.
3. Si el dispositivo virtual utiliza un almacenamiento conectado localmente en un disco virtual, y desea conservar los datos en ese disco, realice lo siguiente:
   a. Haga clic con el botón derecho en el dispositivo virtual y, a continuación, haga clic en **Editar configuración**.
   b. Seleccione el disco con el almacenamiento y después haga clic en **Eliminar**. En **Opciones de eliminación**, haga clic en **Eliminar del equipo virtual**.
   c. Haga clic en **Aceptar**.

   Como resultado, el disco permanece en el almacén de datos. Puede conectar el disco a otro dispositivo virtual.
4. Haga clic con el botón derecho en el dispositivo virtual y haga clic en **Eliminar del disco**. Confirme su decisión.

Eliminando equipos de la consola web de Cyber Protect

Después de desinstalar un agente, se eliminará el registro del servidor de gestión y la máquina en la que estaba instalado el agente se eliminará automáticamente de la consola web de Cyber Protect.

Sin embargo, si se pierde la conexión al servidor de gestión durante esta operación, por ejemplo, debido a un problema de red, el agente podría desinstalarse pero la máquina podría seguir mostrándose en la consola web. En este caso, deberá eliminar la máquina de la consola web de forma manual.

Pasos para eliminar una máquina de la consola web de forma manual

1. En la consola web de Cyber Protect, vaya a **Configuración** > **Agentes**.
2. Seleccione la máquina en la que está instalado el agente.
3. Haga clic en **Eliminar**.

Acceso a la consola web de Cyber Protect

Para acceder a la consola web de Cyber Protect, introduzca la dirección de la página de inicio de sesión en la barra de direcciones del navegador web y luego inicie sesión como se indica a continuación.

Implementación local

La dirección de la página de inicio de sesión es la dirección IP o el nombre del equipo donde se ha instalado el servidor de gestión.

Se admiten los protocolos HTTP y HTTPS en el mismo puerto TCP, que puede configurarse durante la instalación del servidor de gestión. El puerto predeterminado es 9877.

Puede configurar el servidor de gestión para prohibir el acceso a la consola web de Cyber Protect mediante HTTP y utilizar un certificado SSL de terceros.

En Windows

Si el servidor de gestión está instalado en Windows, hay dos formas de iniciar sesión en la consola web de Cyber Protect.

- Haga clic en **Iniciar sesión** para iniciar sesión como el usuario actual de Windows.
  Es la forma más fácil de iniciar sesión desde el mismo equipo en el que está instalado el servidor de gestión.
  Si el servidor de gestión está instalado en otro equipo, este método funciona en las condiciones siguientes:
  - El equipo desde el que está iniciando sesión está en el mismo dominio de Active Directory que el del servidor de gestión.
  - Ha iniciado sesión como usuario del dominio.

  Le recomendamos que configure su navegador web para que admita la autenticación integrada de Windows. Si no lo hace, el navegador le solicitará un nombre de usuario y una contraseña. No obstante, puede deshabilitar esta opción.
- Haga clic en **Introducir el nombre de usuario y la contraseña** y, a continuación, escriba el nombre de usuario y la contraseña.

En cualquier caso, su cuenta debe figurar en la lista de administradores del servidor de gestión. De manera predeterminada, esta lista contiene el grupo de **administradores** del equipo que ejecuta el servidor de gestión. Para obtener más información, consulte la sección "Administradores y unidades".

Pasos para deshabilitar el Inicio de sesión como opción actual del usuario de Windows

1. En el equipo en el que esté instalado el servidor de gestión, vaya a `C:\Program Files\Acronis\AccountServer`.
2. Abra el archivo **account_server.json** para editarlo.

3. Vaya a la sección "conectores" y borre las siguientes líneas:

```
{
"type": "sspi",
"name": "1 Windows Integrated Logon",
"id": "sspi",
"config": {}
},
```

4. Vaya a la sección "suma de comprobación" y cambie el valor de la suma como se indica a continuación:

```
"sum": "FWY/8e8C6c0AgNl0BfCrjgT4v2uj7RQNmaIYbwbjpzU="
```

5. Reinicie Acronis Service Manager Service como se indica en "Uso de un certificado emitido por una autoridad de certificación de confianza".

En Linux

Si el servidor de gestión está instalado en Linux, especifique el nombre de usuario y la contraseña de una cuenta que aparezca en la lista de los administradores del servidor de gestión. De forma predeterminada, esta lista contiene únicamente el usuario **raíz** en el equipo que ejecuta el servidor de gestión. Para obtener más información, consulte la sección "Administradores y unidades".

Implementación en la nube

La dirección de la página de inicio de sesión es https://backup.acronis.com/. El nombre de usuario y la contraseña serán los mismos que los de su cuenta de Acronis.

Si su cuenta la creó el administrador de copias de seguridad, deberá activar la cuenta y establecer la contraseña haciendo clic en el enlace del correo electrónico de activación.

Cambio de idioma

Una vez que haya iniciado la sesión, puede cambiar el idioma de la interfaz web haciendo clic en el icono de la cuenta que hay en la esquina superior derecha.

Configuración de un navegador web para autenticación integrada de Windows

Si accede a la consola web de Cyber Protect desde un equipo Windows y un navegador web compatible, puede utilizar la autenticación integrada de Windows. Sin la autenticación integrada de Windows, debe especificar un nombre de usuario y una contraseña para acceder a la consola web de Cyber Protect.

Cómo configurar Edge, Opera o Chrome

- Si accede a la consola web de Cyber Protect desde un equipo en el mismo dominio de Active Directory que el equipo que ejecuta el servidor de administración, añada la página de inicio de sesión de la consola a la lista de sitios de la **intranet local**. Consulte cómo hacerlo en "Incorporación de la consola a la lista de sitios de la intranet local" (p. 231).
- Si los equipos no están en el mismo dominio de Active Directory, añada la página de inicio de sesión de la consola a la lista de **sitios de confianza** y active la opción **Inicio de sesión automático con el nombre de usuario y la contraseña actuales**. Consulte cómo hacerlo en "Incorporación de la consola a la lista de sitios de confianza" (p. 233).

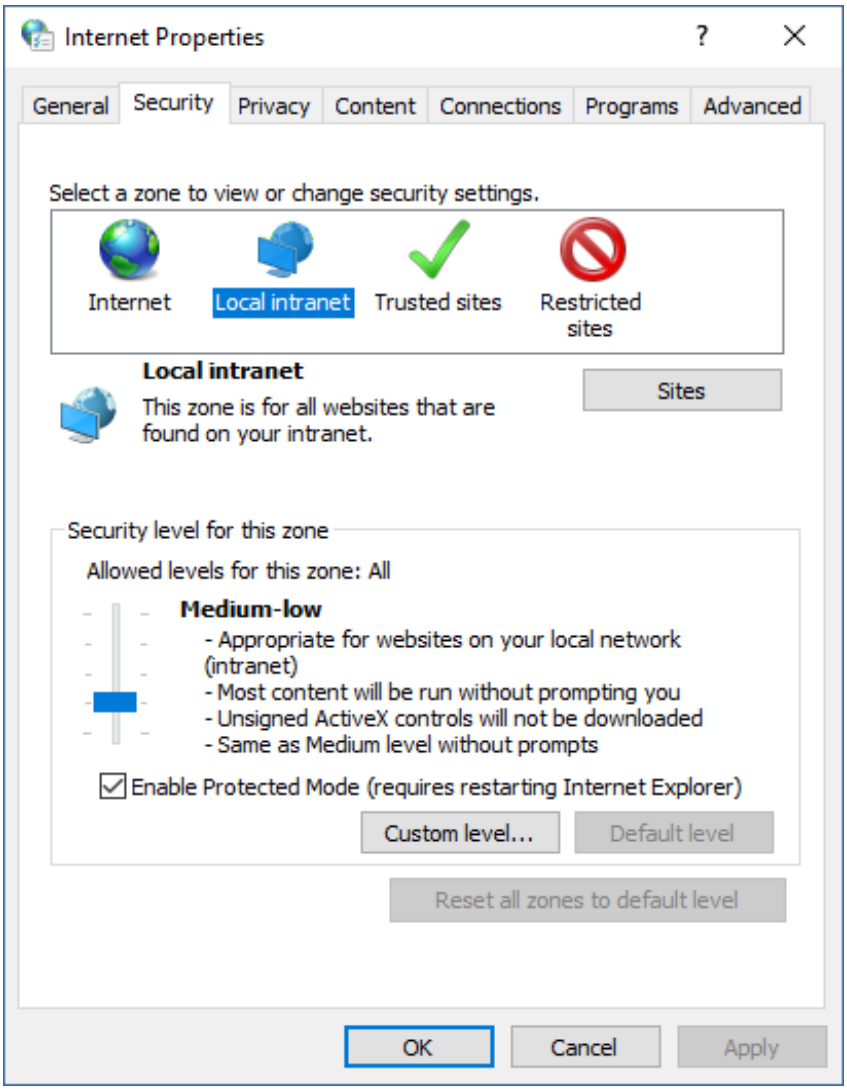
Nota
También puede configurar los navegadores mediante una directiva de grupo en el dominio de Active Directory.

Cómo configurar Firefox

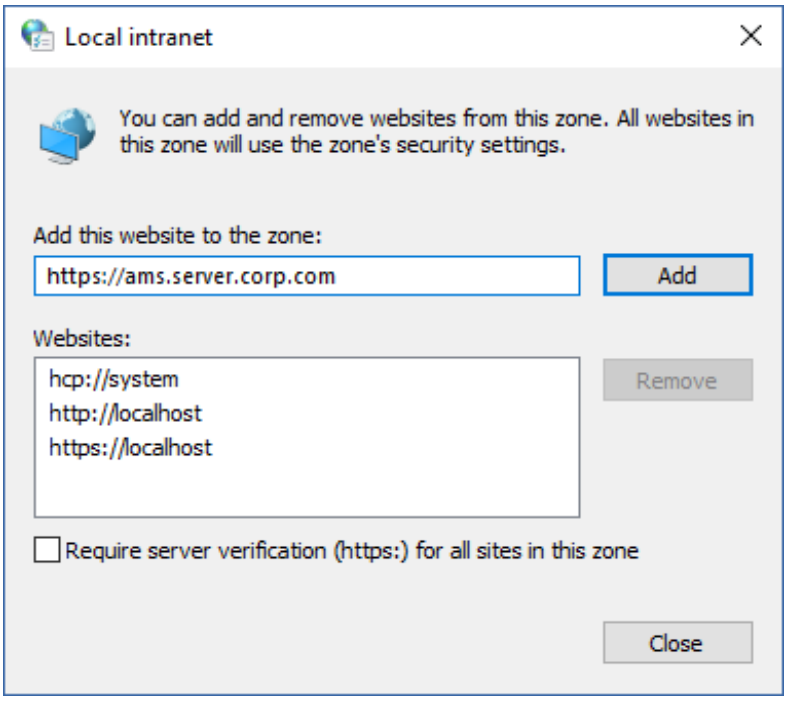
1. En la barra de direcciones de Firefox, introduzca `about:config` y pulse Intro.
2. Haga clic en **Aceptar el riesgo y Continuar**.
3. En el campo de búsqueda, introduzca `network.negotiate-auth.trusted-uris`.
4. Haga doble clic en la preferencia `network.negotiate-auth.trusted-uris` y, a continuación, introduzca la dirección de la página de inicio de la consola web de Cyber Protect.
5. En el campo de búsqueda, introduzca `network.automatic-ntlm-auth.trusted-uris`.
6. Haga doble clic en la preferencia `network.automatic-ntlm-auth.trusted-uris` y, a continuación, introduzca la dirección de la página de inicio de la consola web de Cyber Protect.
7. Cierre la ventana `about:config`.

Incorporación de la consola a la lista de sitios de la intranet local

1. Vaya al **Panel de control** > **Opciones de Internet**.
2. En la pestaña **Seguridad**, seleccione **Intranet local**.



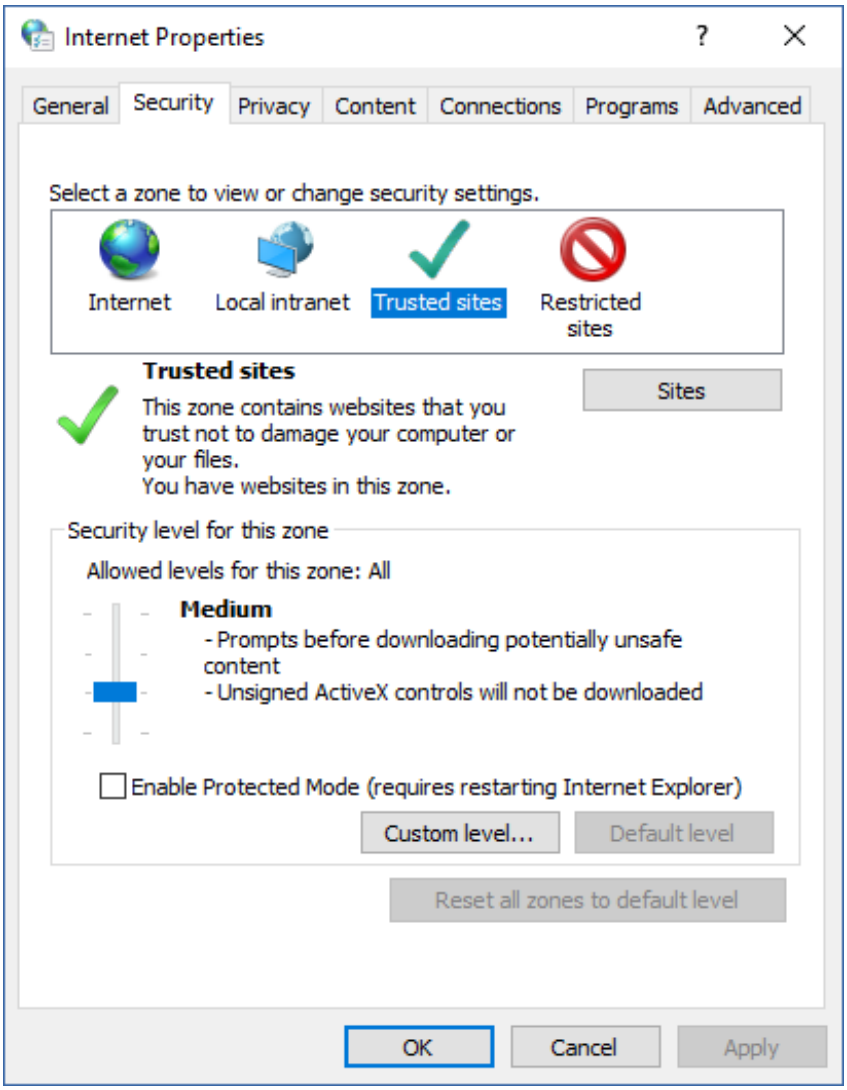
3. Haga clic en **Sitios**.
4. En **Añadir este sitio web a la zona**, introduzca la dirección de la página de inicio de sesión de la consola web de Cyber Protect y, a continuación, haga clic en **Añadir**.



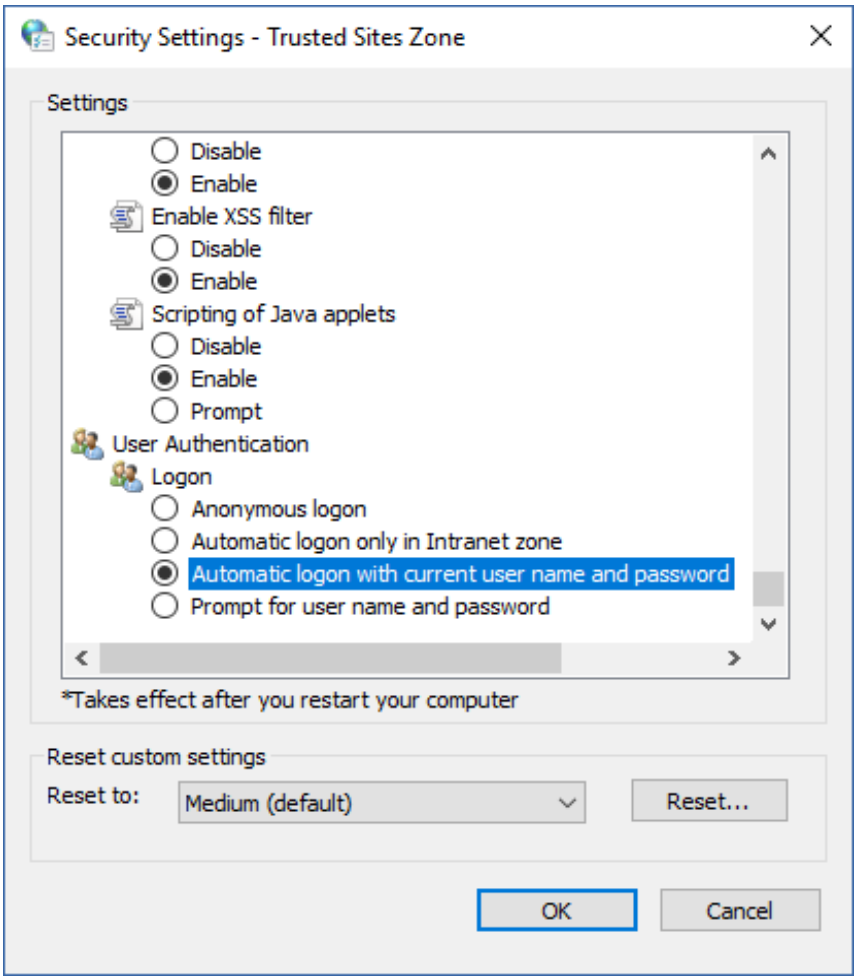
5. Haga clic en **Cerrar**.
6. Haga clic en **Aceptar**.

Incorporación de la consola a la lista de sitios de confianza

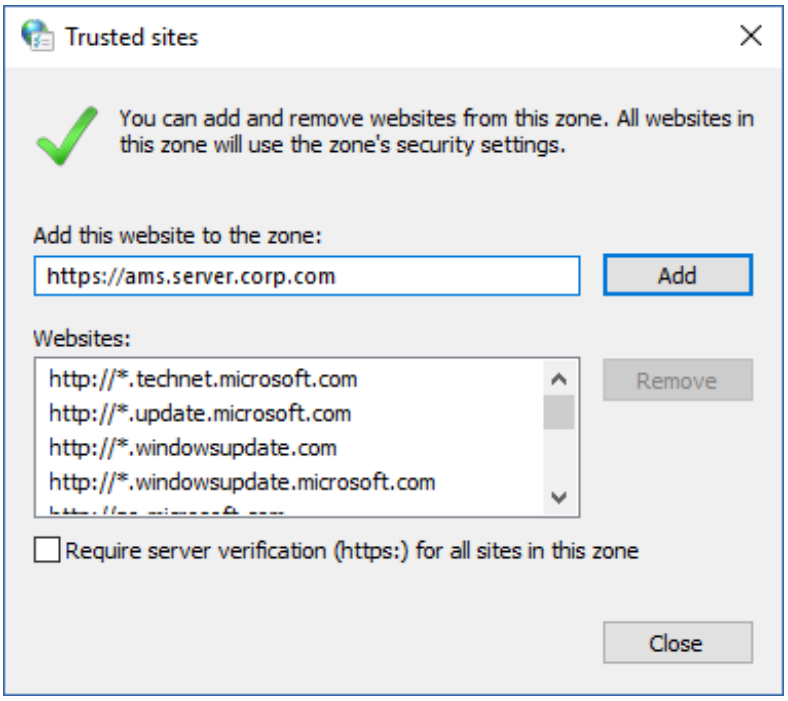
1. Vaya al **Panel de control** > **Opciones de Internet**.
2. En la pestaña **Seguridad**, seleccione **Sitios de confianza** y, a continuación, haga clic en **Nivel personalizado**.



3. En **Iniciar sesión**, seleccione **Inicio de sesión automático con el usuario y la contraseña actuales** y, a continuación, haga clic en **Aceptar**.



4. En la pestaña **Seguridad**, con la opción **Sitios de confianza** todavía seleccionada, haga clic en **Sitios**.
5. En **Añadir este sitio web a la zona**, introduzca la dirección de la página de inicio de sesión de la consola web de Cyber Protect y, a continuación, haga clic en **Añadir**.



6. Haga clic en **Cerrar**.
7. Haga clic en **Aceptar**.

Permitir solo conexiones HTTPS a la consola web

Nota
El acceso a la consola web de Cyber Protect a través de HTTPS solo está disponible si utiliza certificados en formato PEM. Si utiliza certificados PFX, conviértalos en archivos PEM.

Por motivos de seguridad, puede evitar que los usuarios accedan a la consola web de Cyber Protect a través del protocolo HTTP y permitir solo conexiones HTTPS.

Pasos para permitir solo conexiones HTTPS a la consola web

1. En el equipo que ejecuta el servidor de gestión, abra el siguiente archivo de configuración con un editor de texto:
   - En Windows: `%ProgramData%\Acronis\ApiGateway\api_gateway.json`
   - En Linux: `/var/lib/Acronis/ApiGateway/api_gateway.json`
2. Busque la siguiente sección:

```
"tls": {
  "auto_redirect" : false,
  "cert_file": "cert.pem",
```

3. Cambie el valor de `"auto_redirect"` de `false` a `true`.
   Si falta la línea `"auto_redirect"`, añádala de forma manual:

```
"auto_redirect": true,
```

4. Guarde el archivo `api_gateway.json`.

Importante
Tenga cuidado de no eliminar accidentalmente comas, paréntesis o comillas en el archivo de configuración.

5. Reinicie Acronis Service Manager Service como se indica continuación.

Pasos para reiniciar el servicio del administrador de servicios de Acronis en Windows

En Windows

1. En el menú **Inicio**, haga clic en **Ejecutar** y luego escriba **cmd**.
2. Haga clic en **Aceptar**.
3. Ejecute los siguientes comandos:

```
net stop asm
net start asm
```

En Linux

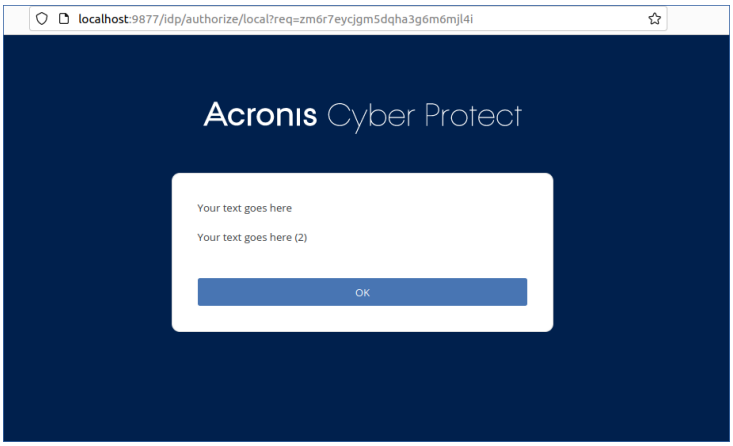
1. Abra el **Terminal**.
2. Ejecute el comando siguiente en cualquier directorio:

```
sudo service acronis_asm restart
```

Añadir un mensaje personalizado a la consola web

Puede añadir un mensaje personalizado a la consola web de Cyber Protect.

Este mensaje se mostrará antes de cada intento de inicio de sesión.



Requisitos previos

Si se aplica algún plan de protección al equipo en el que se ejecuta el servidor de administración, asegúrese de que la función de autoprotección esté deshabilitada. De lo contrario, no podrá editar el archivo de configuración.

Para obtener más información sobre cómo deshabilitar o habilitar la función de autoprotección, consulte "Autoprotección" (p. 575).

Pasos para añadir un mensaje personalizado a la consola web

En Windows

1. Inicie sesión en el equipo en el que está instalado el servidor de administración. Su cuenta debe tener derechos de administrador.
2. Vaya a `%Program Files%\Acronis\AccountServer`.
3. [Opcional] Haga una copia de seguridad del archivo `AccountServer.zip`.
4. Vaya a `%Program Files%\Acronis\AccountServer\AccountServer.zip\static\locale`.
5. Extraiga el archivo JSON que corresponda al idioma que utilice en la consola web de Cyber Protect. Por ejemplo, si utiliza el inglés, extraiga el archivo `en.json`.

   Nota
   Para editar el archivo, debe extraerlo y no solo abrirlo haciendo doble clic.

6. Abra el archivo extraído para editarlo. Puede utilizar un editor de texto, como Notepad o Notepad++.
7. Vaya a la siguiente línea y añada una coma al final:

   ```
   "APP_LOGINFORM_LOGIN_BUTTON": "Log in",
   ```

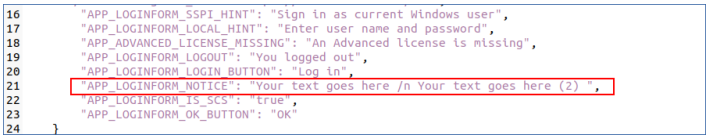
8. En la línea `"APP_LOGINFORM_LOGIN_BUTTON": "Log in"`, añada estas líneas:

   ```
   "APP_LOGINFORM_NOTICE": "<Type your custom message here>",
   ```

   ```
   "APP_LOGINFORM_IS_SCS": "true",
   ```

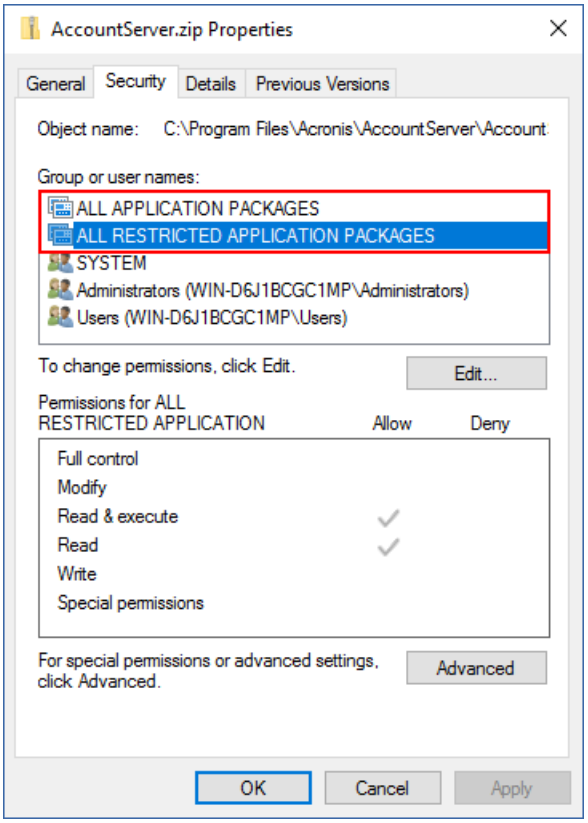
   ```
   "APP_LOGINFORM_OK_BUTTON": "OK"
   ```

   Por ejemplo:

9. Guarde los cambios y vuelva a ubicar el archivo JSON editado en `%Program Files%\Acronis\AccountServer\AccountServer.zip\static\locale`.

10. Haga clic en con el botón derecho en el archivo `AccountServer.zip` y vaya a **Propiedades** > **Seguridad** para verificar que se han añadido `TODOS LOS PAQUETES DE APLICACIONES` y `TODOS LOS PAQUETES DE APLICACIONES RESTRINGIDAS` a **Nombres de grupo o usuario** con derechos para **Leer** y **Leer y ejecutar**.



Nota

Si faltan `TODOS LOS PAQUETES DE APLICACIONES RESTRINGIDAS`, elimine `TODOS LOS PAQUETES DE APLICACIONES` de la lista y añádalos de nuevo. `TODOS LOS PAQUETES DE APLICACIONES RESTRINGIDAS` aparecerá automáticamente cuando añada `TODOS LOS PAQUETES DE APLICACIONES`.

11. Reinicie **Acronis Service Manager Service** como se indica en "Pasos para reiniciar el servicio del administrador de servicios de Acronis" (p. 243).

En Linux

1. Inicie sesión en el equipo en el que está instalado el servidor de administración.
2. Vaya a `/usr/lib/Acronis/AccountServer`.
3. Asegúrese de tener permisos de escritura para el archivo `AccountServer.zip`.
4. [Opcional] Haga una copia de seguridad del archivo `AccountServer.zip`.
5. Vaya a `/usr/lib/Acronis/AccountServer/static/locale`.
6. Extraiga el archivo JSON que corresponda al idioma que utilice en la consola web de Cyber Protect. Por ejemplo, si utiliza el inglés, extraiga el archivo `en.json`.

7. Abra el archivo extraído para editarlo.
8. Vaya a la siguiente línea y añada una coma al final:

```
"APP_LOGINFORM_LOGIN_BUTTON": "Log in",
```

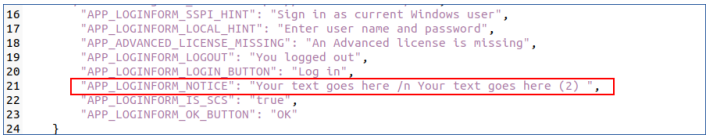
9. En la línea `"APP_LOGINFORM_LOGIN_BUTTON": "Log in"`, añada estas líneas:

```
"APP_LOGINFORM_NOTICE": "<Type your custom message here>",
```

```
"APP_LOGINFORM_IS_SCS": "true",
```

```
"APP_LOGINFORM_OK_BUTTON": "OK"
```

Por ejemplo:



10. Guarde los cambios y ubique de nuevo el archivo JSON editado en `/usr/lib/Acronis/AccountServer/static/locale`.
11. Reinicie **Acronis Service Manager Service** como se indica en "Pasos para reiniciar el servicio del administrador de servicios de Acronis" (p. 243).

Configuración del certificado SSL

Esta sección describe:

- Cómo configurar un agente de protección que utiliza un certificado Secure Socket Layer (SSL) autofirmado generado por el servidor de gestión.
- Cómo cambiar el certificado SSL autofirmado generado por el servidor de gestión por un certificado emitido por una autoridad de certificación de confianza, como GoDaddy, Comodo o GlobalSign. Si realiza este cambio, cualquier equipo considerará que el certificado utilizado por el servidor de gestión es de confianza. La alerta de seguridad del navegador no aparecerá cuando inicie sesión en la consola web de Cyber Protect mediante el protocolo HTTPS.

Opcionalmente, puede configurar el servidor de administración, así como prohibir el acceso a la consola web de Cyber Protect mediante HTTP y redirigir a todos los usuarios a la versión HTTPS. Para obtener más información, consulte "Permitir solo conexiones HTTPS a la consola web" (p. 236).

Nota
El acceso a la consola web de Cyber Protect a través de HTTPS solo está disponible si utiliza certificados en formato PEM. Si utiliza certificados PFX, conviértalos en archivos PEM.

Utilizar un certificado autofirmado

Pasos para configurar un agente de protección en Windows

1. En el equipo con el agente, abra el Editor del registro.
2. Busque la siguiente clave del registro: **HKEY_LOCAL_MACHINE\Software\Acronis\BackupAndRecovery\Settings\CurlOptions.**
3. Establezca el valor **VerifyPeer** en **0**.
4. Asegúrese de que el valor **VerifyHost** se ha establecido en **0**.
5. Reinicie Managed Machine Service (MMS):
   a. En el **menú Inicio**, haga clic en **Ejecutar** y luego escriba **cmd**
   b. Haga clic en **Aceptar**.
   c. Ejecute los siguientes comandos:

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

Pasos para configurar un agente de protección en Linux

1. En el equipo con el agente, abra el archivo **/etc/Acronis/BackupAndRecovery.config** para editarlo**.**
2. Vaya a la clave **CurlOptions** y establezca el valor para **VerifyPeer** en **0.** Asegúrese de que el valor de **VerifyHost** también es **0.**
3. Guarde los cambios.
4. Reinicie Managed Machine Service (MMS) ejecutando el siguiente comando en cualquier directorio:

```
sudo service acronis_mms restart
```

Pasos para configurar un agente de protección en macOS

1. En el equipo con el agente, detenga Managed Machine Service (MMS):
   a. Vaya a **Aplicaciones** > **Utilidades** > **Terminal**.
   b. Ejecute el siguiente comando:

```
sudo launchctl stop acronis_mms
```

2. Abra el archivo **/Library/Application Support/Acronis/Registry/BackupAndRecovery.config** para editarlo.
3. Vaya a la clave **CurlOptions** y establezca el valor para **VerifyPeer** en **0**. Asegúrese de que el valor de **VerifyHost** también es **0**.
4. Guarde los cambios.
5. Inicie Managed Machine Service (MMS) ejecutando el siguiente comando en el Terminal:

```
sudo launchctl starts acronis_mms
```

Utilizar un certificado emitido por una autoridad de certificación de confianza

Pasos para configurar los ajustes del certificado SSL

1. Asegúrese de tener lo siguiente:

Si usa archivos de clave y de certificado	Si usa un archivo PFX
El archivo de certificado (en formato .pem)	El archivo PFX
El archivo con la clave privada para el certificado (por lo general, en formato .key)	
La contraseña de clave privada (si la clave está protegida con contraseña)	La contraseña del archivo PFX, si está protegido con contraseña

Importante
Todos los alias del servidor de administración deben incluirse en el certificado como Subject Alternative Names (SAN).

2. Copie los archivos al equipo que ejecute el servidor de gestión.
3. En este equipo, abra el siguiente archivo de configuración con un editor de texto:
   - En Windows: `%ProgramData%\Acronis\ApiGateway\api_gateway.json`
   - En Linux: `/var/lib/Acronis/ApiGateway/api_gateway.json`
4. Busque la siguiente sección:

```
"tls": {
    "cert_file": "cert.pem",
    "key_file": "key.pem",
    "passphrase": "",
```

5. Entre las comillas de la línea `"cert_file"`, especifique la ruta completa al archivo de certificado o el archivo PFX.

   Por ejemplo:

Sistema operativo	Si usa un certificado y una clave	Si usa un archivo .pfx
Windows (tenga en cuenta las barras diagonales)	`"cert_file": "C:/certificate/local-domain.ams.pem"`	`"cert_file": "C:/certificate/local-domain.ams.pfx"`
Linux	`"cert_file": "/home/user/local-`	`"cert_file": "/home/user/local-`

Sistema operativo	Si usa un certificado y una clave	Si usa un archivo .pfx
	`domain.ams.pem"`	`domain.ams.pfx"`

6. Entre las comillas de la línea `"key_file"`, especifique la ruta completa al archivo de la clave privada o el archivo PFX que contiene la clave del certificado.
   Por lo general, un archivo PFX incluye tanto el certificado como su clave. En este caso, en la línea `"key_file"`, especifique la misma ruta que en el paso anterior.
   Por ejemplo:

Sistema operativo	Si usa un certificado y una clave	Si usa un archivo .pfx
Windows (tenga en cuenta las barras diagonales)	`"key_file": "C:/certificate/private.key"`	`"cert_file": "C:/certificate/local-domain.ams.pfx"`
Linux	`"key_file": "/home/user/private.key"`	`"cert_file": "/home/user/local-domain.ams.pfx"`

7. [Opcional] Si la clave privada está cifrada o el archivo PFX está protegido con contraseña, especifique la contraseña entre las comillas de la línea `"passphrase"`.
   Por ejemplo: `"passphrase": "my password"`

Nota
Si falta la línea `"passphrase": ""`, en el archivo de configuración `api_gateway.json`, añádala de forma manual.
Por ejemplo:

```
"tls": {
    "cert_file": "cert.pem",
    "key_file": "key.pem",
    "passphrase": "my password",
}
```

8. Guarde el archivo `api_gateway.json`.

Importante
Tenga cuidado de no eliminar accidentalmente comas, paréntesis o comillas en el archivo de configuración.

9. Reinicie Acronis Service Manager Service como se indica continuación.

Pasos para reiniciar el servicio del administrador de servicios de Acronis

En Windows

1. En el menú **Inicio**, haga clic en **Ejecutar** y luego escriba **cmd**.
2. Haga clic en **Aceptar**.
3. Ejecute los siguientes comandos:

```
net stop asm
net start asm
```

En Linux

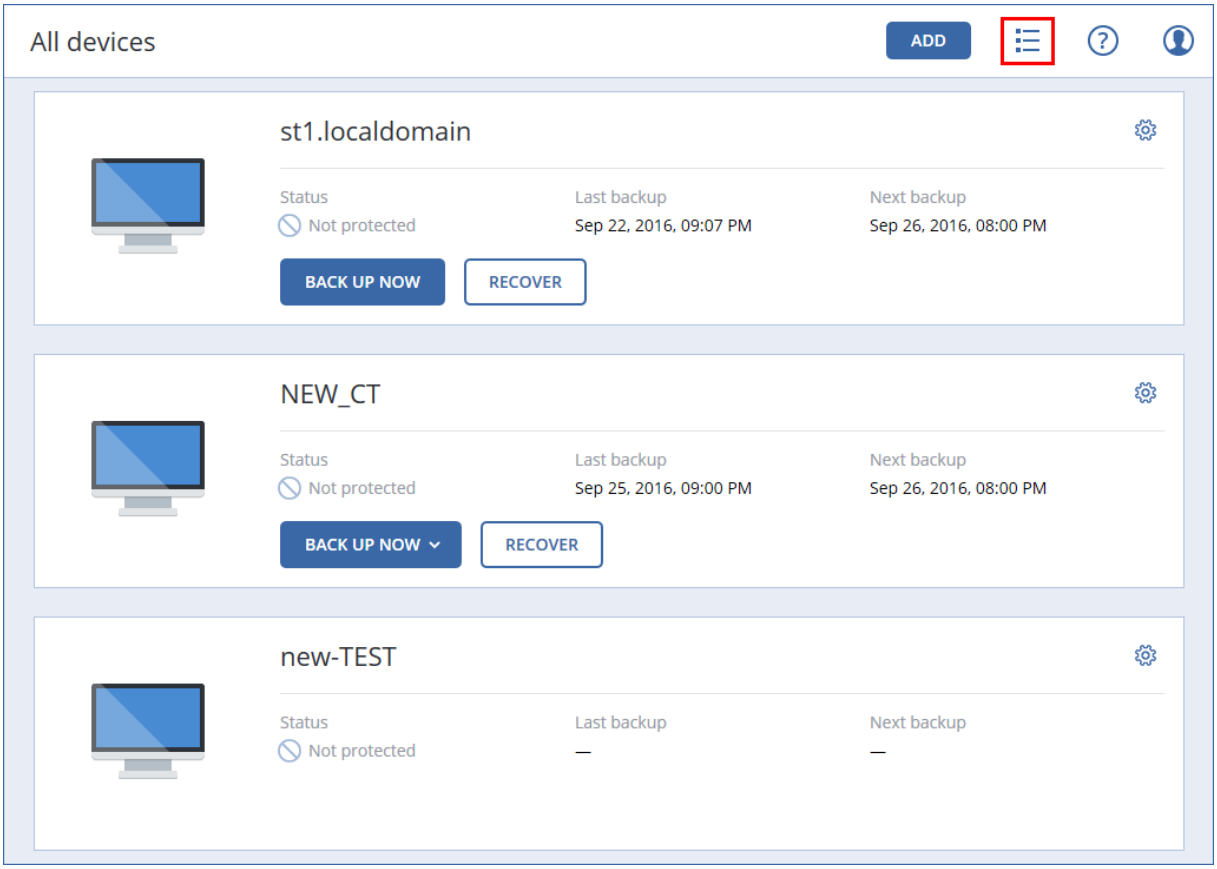
1. Abra el **Terminal**.
2. Ejecute el comando siguiente en cualquier directorio:

```
sudo service acronis_asm restart
```

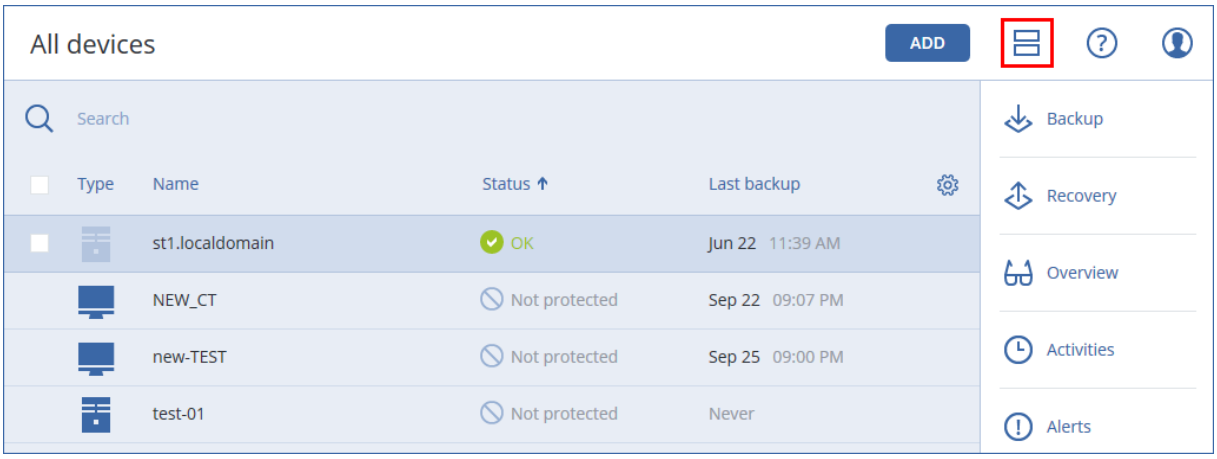
Vista de consola web de Cyber Protect

La consola web de Cyber Protect tiene dos vistas: una simple y una de tabla. Para cambiar el tipo de vista, haga clic en el icono correspondiente en la esquina superior derecha.

La vista simple admite un número reducido de equipos.



La vista de tabla se habilita automáticamente si el número de equipos aumenta considerablemente.



Las dos vistas proporcionan acceso a las mismas operaciones y características. Este documento detalla el acceso a operaciones desde la vista de tabla.

Cuando un equipo se conecta o desconecta de la red, su estado tarda un tiempo en cambiar en la consola web de Cyber Protect.

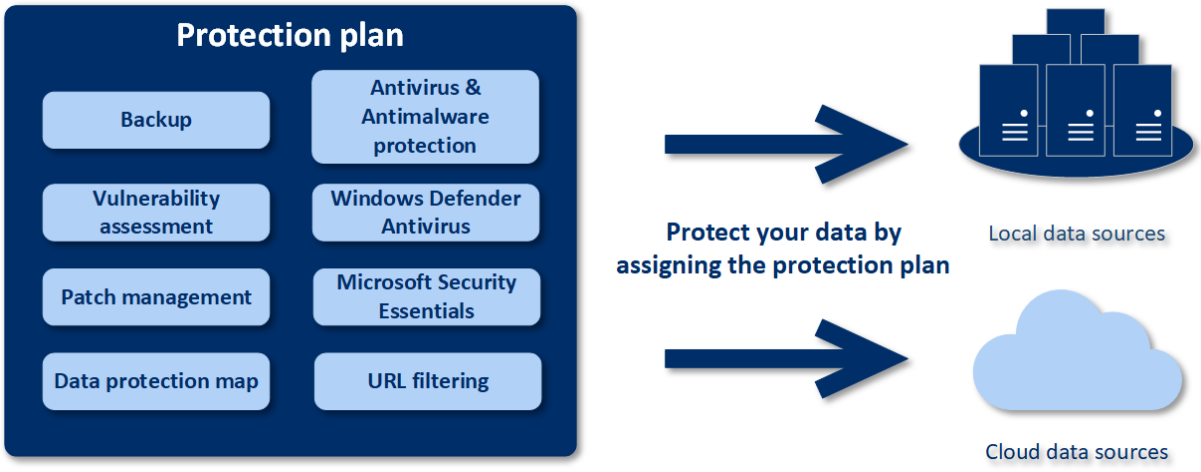
Se verifica el estado del equipo cada minuto. Si el agente instalado en este equipo no transfiere datos y no hay respuesta tras cinco comprobaciones consecutivas, el equipo se mostrará como offline. Se mostrará que el equipo vuelve a estar en línea cuando responda a una comprobación de estado o cuando comience a transferir datos.

Planes de protección y módulos

Un plan de protección es aquel que combina varios módulos de protección de datos, como los siguientes:

- Copia de seguridad: le permite realizar copias de seguridad de sus orígenes de datos o almacenamiento en la nube.
- Protección antimalware y antivirus: le permite comprobar sus equipos con la solución antimalware integrada.
- Filtrado de URL: le permite proteger sus equipos de amenazas procedentes de Internet porque bloquea el acceso para que no se descarguen direcciones URL ni contenido maliciosos.
- Windows Defender Antivirus: puede gestionar la configuración de este antivirus para proteger su entorno.
- Microsoft Security Essentials: puede gestionar la configuración de este antivirus para proteger su entorno.
- Evaluación de vulnerabilidades: realiza comprobaciones automáticas en los productos Microsoft y de terceros instalados en sus equipos por si hay vulnerabilidades y le manda notificaciones sobre ellas.
- Gestión de parches: le permite instalar parches y actualizaciones para productos de Microsoft y terceros en sus equipos con el fin de acabar con las vulnerabilidades detectadas.
- Mapa de protección de datos: le servirá para conocer la información que necesita para supervisar el estado de la protección de archivos importantes.

Con el plan de protección podrá proteger por completo los orígenes de sus datos de amenazas externas e internas. Si habilita y deshabilita distintos módulos y configura los ajustes del módulo, puede crear planes flexibles que satisfagan ciertas necesidades de su empresa.



Creación de un plan de protección

Cuando cree un plan de protección, puede aplicarlo a múltiples equipos en ese momento o más adelante. Cuando crea un plan, el sistema comprueba el sistema operativo y el tipo de dispositivo

(por ejemplo, workstation, equipo virtual, etc.), y muestra únicamente los módulos de plan aplicables a sus dispositivos.

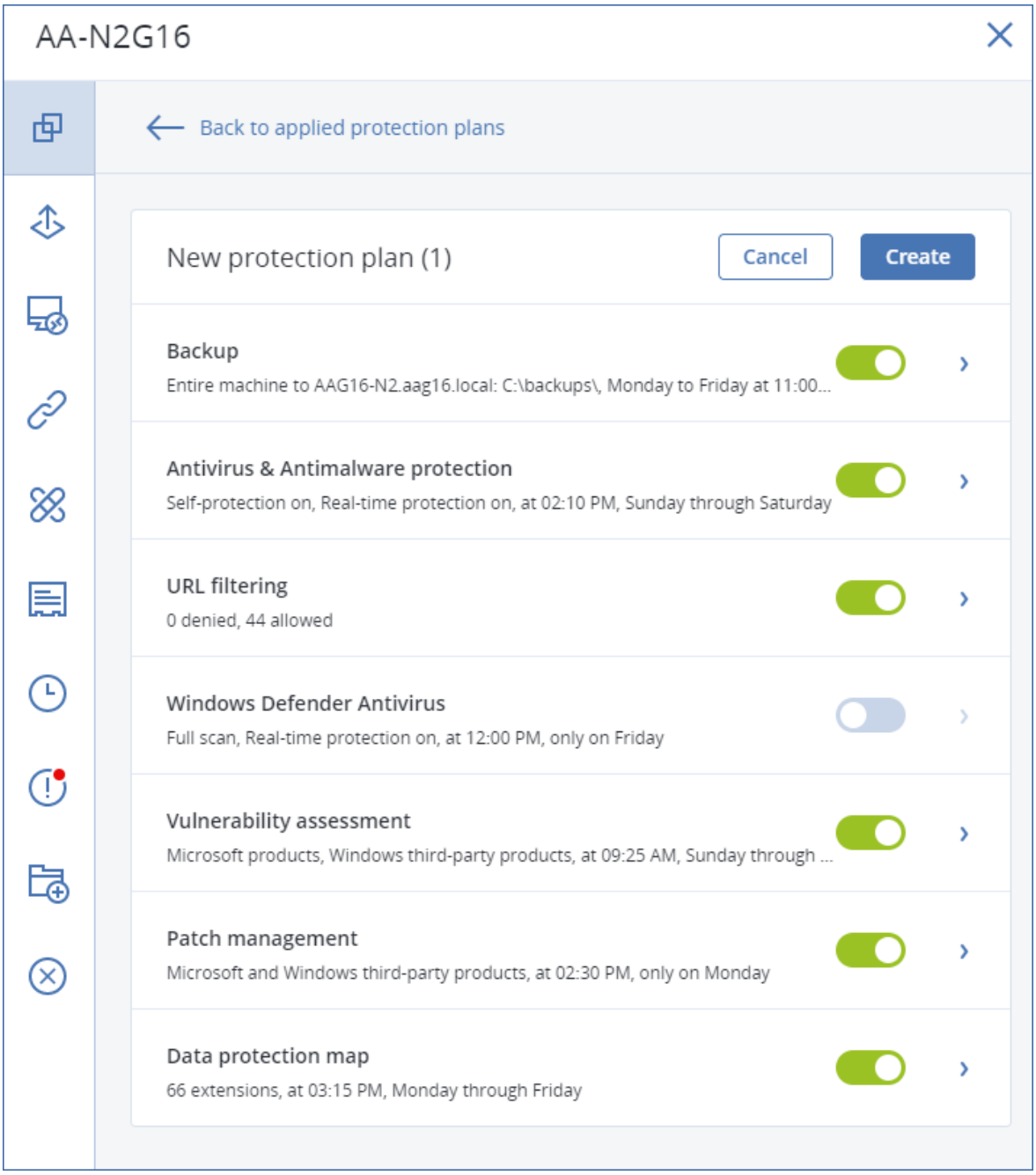
Los planes de protección se pueden crear de dos formas:

- En la sección **Dispositivos**: si selecciona el dispositivo o los dispositivos que se van a proteger y crea un plan para ellos.
- En la sección **Planes**: si crea un plan y selecciona los equipos a los que se va a aplicar.

Centrémonos en la primera manera.

Pasos para crear el primer plan de protección

1. En la consola web de Cyber Protect, vaya a **Dispositivos** > **Todos los dispositivos**.
2. Seleccione los equipos que quiera proteger.
3. Haga clic en **Proteger** y, a continuación, seleccione **Crear plan**. Verá el plan de protección con la configuración predeterminada.



4. [Opcional] Para modificar el nombre del plan de protección, haga clic en el icono de lápiz que se encuentra junto al nombre.
5. [Opcional] Para habilitar o deshabilitar un módulo de plan de protección, haga clic en el interruptor que se encuentra junto al nombre del módulo.
6. [Opcional] Para configurar los parámetros del módulo, haga clic en la sección correspondiente del plan de protección.
7. Cuando tenga todo listo, haga clic en **Crear**.

Los módulos Copia de seguridad, Protección antivirus y antimalware, Evaluación de vulnerabilidades, Gestión de parches y Mapa de protección de datos se pueden llevar a cabo bajo demanda al hacer clic en **Ejecutar ahora**.

Resolución de conflictos entre planes

Los planes de protección pueden tener los siguientes estados:

- **Activo**: plan que está asignado a dispositivos y se ejecuta en ellos.
- **Inactivo**: plan que está asignado a dispositivos, pero está deshabilitado y no se ejecuta en ellos.

Aplicación de varios planes a un dispositivo

Puede aplicar varios planes de protección a un único dispositivo. Como resultado, obtendrá una combinación de distintos planes de protección asignados a un único dispositivo. Por ejemplo, puede aplicar un plan que solo tenga habilitado el módulo de protección antivirus y antimalware y otro que solo tenga habilitado el módulo de copia de seguridad. Los planes de protección se pueden combinar únicamente si no tienen módulos que se crucen. Si los mismos módulos están habilitados en más de un plan de protección, deberá resolver los conflictos entre ellos.

Resolución de conflictos entre planes

Conflictos entre planes que ya están aplicados

Al crear un plan nuevo en uno o varios dispositivos que ya tengan planes aplicados y estos entren en conflicto con el nuevo, puede resolver estos conflictos de una de las siguientes maneras:

- Cree un plan nuevo, aplíquelo y deshabilite todos los planes que entren en conflicto que ya estén aplicados.
- Cree un plan nuevo y deshabilítelo.

Al editar un plan en uno o varios dispositivos que ya tengan planes aplicados y estos entren en conflicto con los cambios realizados, puede resolver estos conflictos de una de las siguientes maneras:

- Guarde los cambios realizados al plan y deshabilite todos los planes aplicados que entren en conflicto.
- Guarde los cambios en el plan y deshabilítelo.

El plan de un dispositivo entra en conflicto con el de un grupo

Si un dispositivo está incluido en un grupo con un plan de grupo asignado y se intenta asignar un plan nuevo a un dispositivo, el sistema le pedirá que resuelva el conflicto mediante una de las siguientes acciones:

- Eliminar el dispositivo del grupo y aplicarle al dispositivo un plan nuevo.
- Aplicar un plan nuevo a todo el grupo o editar su plan actual.

Problemas con las licencias

La cuota asignada en un dispositivo debe ser la adecuada para que el plan de protección se lleve a cabo, se actualice o se aplique. Para resolver un problema relacionado con las licencias, realice uno de los siguientes procedimientos:

- Deshabilite los módulos que no son compatibles con la cuota asignada y siga usando el plan de protección.
- Cambie la cuota asignada manualmente: vaya a **Dispositivos** > **<Particular device>** > **Detalles** > **Cuota de servicio**. A continuación, revoque la cuota existente y asigne una nueva.

Operaciones con planes de protección

Para obtener información sobre cómo crear un plan de protección, consulte "Creación de un plan de protección".

Acciones disponibles relacionadas con un plan de protección

Con un plan de protección puede llevar a cabo las siguientes acciones:

- Cambiar el nombre a un plan
- Habilitar o deshabilitar módulos y editar la configuración de cada uno
- Habilitar o deshabilitar un plan

  Un plan deshabilitado no se llevará a cabo en el dispositivo al que se aplica.

  Esta acción es adecuada para aquellos administradores que pretenden proteger el mismo dispositivo con el mismo plan más adelante. El plan no se revoca del dispositivo y el administrador solo tiene que volver a habilitarlo para restaurar la protección.
- Aplicar un plan a dispositivos o a un grupo de dispositivos
- Revocar un plan de un dispositivo

  Un plan revocado deja de aplicarse a un dispositivo.

  Esta acción es adecuada para aquellos administradores que no necesitan proteger el mismo dispositivo rápidamente con el mismo plan de nuevo. Para restaurar la protección de un plan revocado, el administrador debe saber el nombre del plan, seleccionarlo de la lista de planes disponibles y luego volver a aplicarlo al dispositivo que desee.
- Importar o exportar un plan

  Nota

  Puede importar planes de protección creados únicamente en Acronis Cyber Protect 15. Los planes de protección creados en versiones anteriores no son compatibles con Acronis Cyber Protect 15.
- Eliminar un plan

Pasos para aplicar un plan de protección existente

1. Seleccione los equipos que quiera proteger.
2. Haga clic en **Proteger**. Si ya se aplica un plan de protección común a los equipos seleccionados, haga clic en **Añadir plan de protección**.
3. El software muestra planes de protección creados previamente.
4. Seleccione la protección que desee y haga clic en **Aplicar**.

Pasos para editar un plan de protección

1. Si quiere editar el plan de protección para todos los equipos a los que se aplica, seleccione uno de los equipos. De lo contrario, seleccione los equipos para los cuales quiere editar el plan de protección.
2. Haga clic en **Proteger**.
3. Seleccione el plan de protección que desee editar.
4. Haga clic en el icono de puntos suspensivos que se encuentra junto al nombre del plan de protección y después, haga clic en **Editar**.
5. Para modificar los parámetros del plan, haga clic en la sección correspondiente del panel del plan de protección.
6. Haga clic en **Guardar cambios**.
7. Para cambiar el plan de protección para todos los equipos a los que se aplica, haga clic en **Aplicar los cambios a este plan de protección**. De lo contrario, haga clic en **Crear un nuevo plan de protección solamente para los recursos seleccionados**.

Pasos para revocar un plan de protección de los equipos

1. Seleccione los equipos que desee revocar del plan de protección.
2. Haga clic en **Proteger**.
3. Si se aplican varios planes de protección a los equipos, seleccione el plan de protección que desea revocar.
4. Haga clic en el icono de puntos suspensivos que se encuentra junto al nombre del plan y después, haga clic en **Revocar**.

Pasos para borrar un plan de protección

1. Seleccione cualquiera de los equipos a los que se les aplica el plan de protección que desea borrar.
2. Haga clic en **Proteger**.
3. Si se aplican varios planes de protección a los equipos, seleccione el plan de protección que desea eliminar.
4. Haga clic en el icono de puntos suspensivos que se encuentra junto al nombre del plan y después, haga clic en **Eliminar**.

   Como consecuencia, se revoca el plan de protección en todos los equipos y se elimina completamente de la interfaz web.

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.

Nota
En las implementaciones locales, no se puede aplicar un plan de protección a varios equipos físicos si el servidor de gestión solo tiene licencias estándar. Cada equipo físico debe tener su propio plan de protección.

Pasos para crear el primer plan de protección con el módulo de copia de seguridad habilitado

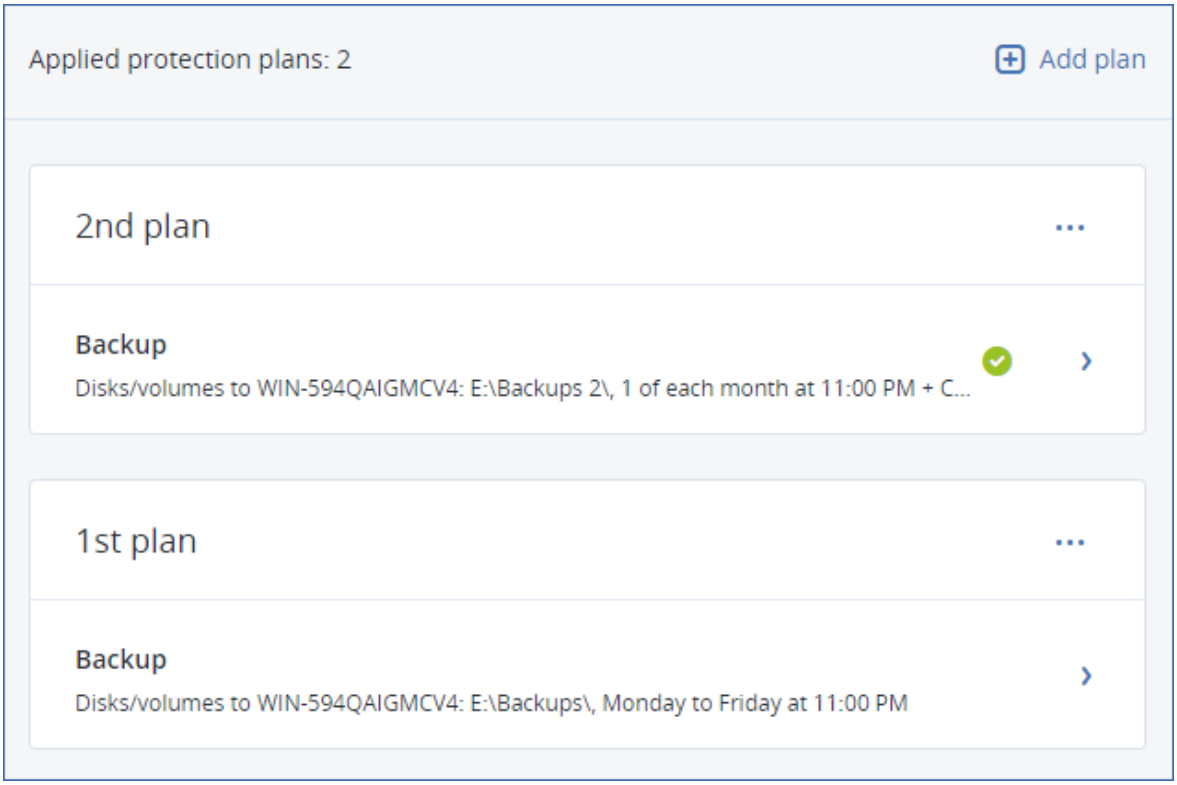
1. Seleccione los equipos que desea incluir en la copia de seguridad.
2. Haga clic en **Proteger**.
   El software muestra los planes de protección que están aplicados al equipo. Si no hay ningún plan de protección asignado al equipo todavía, verá el plan de protección predeterminado que se puede aplicar.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



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

Apuntes del módulo de copias de seguridad

Importante
Algunas de las funciones descritas en esta sección solo están disponibles en implementaciones locales.

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

DE QUÉ REALIZAR COPIAS DE SEGURIDAD	ELEMENTOS PARA INCLUIR EN LA COPIA DE SEGURIDAD	DÓNDE REALIZAR COPIAS DE SEGURIDAD	PLANIFICAR Esquemas de copia de seguridad	CUÁNTO TIEMPO GUARDARLAS

	Métodos de selección		**(no para la cloud)**	
Discos/volúmenes (equipos físicos)	Selección directa Normas de directiva Filtros de archivo	Nube Carpeta local Carpeta de red Servidor SFTP* NFS* Secure Zone* Ubicación gestionada* Dispositivo de cintas*	Siempre incremental (archivo único)* Siempre completas Completa semanal, incremental diaria Completa mensual, diferencial semanal, incremental diaria (GFS) Personalizadas (F-D-I)	Por antigüedad de las copias de seguridad (norma única/por conjunto de copias de seguridad) Por número de copias de seguridad Por tamaño total de las copias de seguridad* Guardar indefinidamente
Discos/volúmenes (equipos virtuales)	Normas de directiva Filtros de archivo	Nube Carpeta local Carpeta de red Servidor SFTP* NFS* Ubicación gestionada* Dispositivo de cintas*		
Archivos (solo equipos físicos)	Selección directa Normas de directiva Filtros de archivo	Nube Carpeta local Carpeta de red Servidor SFTP* NFS* Secure Zone* Ubicación gestionada* Dispositivo de cintas	Siempre completas Completa semanal, incremental diaria Completa mensual, diferencial semanal, incremental diaria (GFS) Siempre incremental (archivo único)* Personalizadas	

			(F-D-I)	

Configuración de ESXi	Selección directa	Carpeta local Carpeta de red Servidor SFTP NFS*		
Bases de datos SQL	Selección directa	Nube Carpeta local Carpeta de red Ubicación gestionada* Dispositivo de cintas	Siempre completas Completas semanalmente, incrementales diariamente Personalizadas (F-I)	
Bases de datos de Exchange	Selección directa			
Buzones de correo de Exchange	Selección directa	Nube Carpeta local Carpeta de red Ubicación gestionada*	Siempre incremental (archivo único)	por antigüedad de
Buzones de correo de Microsoft 365	Selección directa			

				Las copias de seguridad (normalmente incrementales) con

* Consulte las limitaciones a continuación.

Limitaciones

Servidor SFTP y dispositivo de cintas

- Estas ubicaciones no pueden ser un destino para las copias de seguridad de los equipos que ejecutan macOS.
- Estas ubicaciones no pueden ser un destino para las copias de seguridad compatibles con aplicaciones.
- El esquema de copia de seguridad **Siempre incremental (archivo único)** no está disponible al hacer copias de seguridad en estas ubicaciones.
- La regla de retención **Por tamaño total de las copias de seguridad** no está disponible para estas ubicaciones.

NFS

- En Windows no se pueden hacer copias de seguridad en NFS compartidos.
- El esquema de copia de seguridad **Siempre incremental (archivo único)** para archivos (equipos físicos) no está disponible al hacer copias de seguridad en NFS compartidos.

Secure Zone

- Secure Zone no se puede crear en un Mac.

Ubicación gestionada

- Una ubicación gestionada con la deduplicación o el cifrado habilitados no se puede seleccionar como destino:
  - Si el esquema de copias de seguridad está configurado como **Siempre incremental (archivo único)**
  - Si el formato de copia de seguridad está establecido en la **versión 12**
  - Para copias de seguridad a nivel de disco de equipos que ejecutan macOS
  - Para las copias de seguridad de los buzones de correo de Exchange y de los buzones de correo de Microsoft 365.
- La regla de retención **Por tamaño total de las copias de seguridad** no está disponible para las ubicaciones gestionadas con la deduplicación habilitada.

Siempre incremental (archivo único)

- El esquema de copia de seguridad **Siempre incremental (archivo único)** no está disponible al hacer copias de seguridad en un servidor SFTP o un dispositivo de cintas.

- El esquema de copia de seguridad **Siempre incremental (archivo único)** para archivos (equipos físicos) solo está disponible cuando la ubicación de la copia de seguridad principal es Acronis Cloud.

Por tamaño total de las copias de seguridad

- La regla de retención **Por tamaño total de las copias de seguridad** no está disponible:
  - Si el esquema de copias de seguridad está configurado como **Siempre incremental (archivo único)**
  - Cuando la copia de seguridad se realiza en un servidor SFTP un dispositivo de cintas o una ubicación gestionada con la deduplicación habilitada.

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 configurar la copia de seguridad, en **De qué realizar copias de seguridad**, seleccione **Todo el equipo**.

Importante
Las unidades externas, como las unidades flash USB o los discos duros USB, no se incluyen en la copia de seguridad de **Todo el equipo**. Para hacer una copia de estas unidades, configure una copia de seguridad de **Discos/volúmenes**. Para obtener más información sobre la copia de seguridad del disco, consulte "Seleccionar discos/volúmenes" (p. 261).

Seleccionar discos/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 o archivos individuales de una copia de seguridad a nivel de discos. La copia de seguridad de un equipo entero es una copia de seguridad de todos sus discos no extraíbles.

Nota
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 archivo.

Hay dos maneras de seleccionar discos/volúmenes: directamente en cada equipo o usando las normas de política. Puede excluir archivos de una copia de seguridad del disco al configurar los filtros de archivo.

Selección directa

La selección directa está disponible únicamente para los equipos físicos. Para habilitar la selección directa de discos y volúmenes en un equipo virtual, debe instalar el agente de protección en su sistema operativo invitado.

1. En **De qué realizar copias de seguridad**, seleccione **Discos/volúmenes**.
2. Haga clic en **Elementos para incluir en la copia de seguridad**.
3. En **Seleccionar elementos para incluir en la copia de seguridad**, seleccione **Directamente**.
4. Para cada uno de los equipos 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 **Realizado**.

Usar las normas de directiva

1. En **De qué realizar copias de seguridad**, seleccione **Discos/volúmenes**.
2. Haga clic en **Elementos para incluir 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.

   Las normas de directiva se aplicarán a todos los equipos incluidos en el plan de protección. Si ninguno de los datos del equipo cumple como mínimo una de las normas, la copia de seguridad fallará cuando se inicie en ese equipo.
5. Haga clic en **Realizado**.

Normas para Windows, Linux y macOS

- `[All Volumes]` selecciona todos los volúmenes en los equipos que ejecutan Windows y todos los volúmenes montados en los equipos que ejecutan Linux o macOS.

Normas para Windows

- La letra de la unidad (por ejemplo, **C:**) indica el volumen con la letra de la unidad especificada.
- `[Fixed Volumes (physical machines)]` selecciona todos los volúmenes de los equipos físicos, 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 combinación es el conjunto mínimo de datos que garantiza la recuperación del sistema operativo desde la copia de seguridad.
- `[BOOT+SYSTEM DISK (physical machines)]` selecciona todos los volúmenes del disco en el que se encuentran los volúmenes de arranque y del sistema. Si los volúmenes de arranque y del sistema no están en el mismo disco, no se seleccionará nada. Esta regla solo se aplica a los equipos físicos.
- `[Disk 1]` selecciona el primer disco del equipo, incluidos todos los volúmenes de ese disco. Para seleccionar otro disco, escriba el número correspondiente.

Normas para Linux

- `/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, introduzca lo siguiente:

```
/dev/mapper/vg_1-lv1
/dev/mapper/vg-l-lv2
```

Normas para macOS

- `[Disk 1]` selecciona el primer disco del equipo, incluidos todos los volúmenes de ese disco. Para seleccionar otro disco, escriba el número correspondiente.

¿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 arranque 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, a partir de Windows 7, no se hacen copias de seguridad de los 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.

Seleccionar archivos/carpetas

La copia de seguridad a nivel de archivo está disponible para equipos físicos y virtuales con copia de seguridad realizada por un agente instalado en el sistema invitado.

Una copia de seguridad a nivel de archivos no es suficiente para recuperar el sistema operativo. Elija la copia de seguridad de archivos si su intención es proteger únicamente ciertos datos (el proyecto actual, por ejemplo). Esto reducirá la medida de la copia de seguridad y, por lo tanto, ahorrará espacio de almacenamiento.

Nota
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 archivo.

Hay dos métodos para seleccionar archivos: directamente en cada equipo o usando las normas de directiva. Cualquiera de los métodos le permite perfeccionar una futura selección activando los filtros de archivo.

Selección directa

1. En **De qué realizar copias de seguridad**, seleccione **Archivos/carpetas**.
2. Haga clic en **Elementos para incluir en la copia de seguridad**.
3. En **Seleccionar elementos para incluir en la copia de seguridad**, seleccione **Directamente**.
4. Para cada uno de los equipos incluidos en el plan de protección:
   a. Haga clic en **Seleccionar archivos y carpetas**.
   b. Haga clic en **Carpeta local** o **Carpeta de red**.
      El recurso debe ser accesible desde el equipo seleccionado.
   c. Busque los archivos/carpetas requeridos o introduzca la ruta y haga clic en la flecha. Si se le pide, especifique el nombre de usuario y la contraseña de la carpeta compartida.
      No se admite la copia de seguridad de una carpeta con acceso anónimo.
   d. Seleccione los archivos/carpetas requeridos.
   e. Haga clic en **Realizado**.

Usar las normas de directiva

1. En **De qué realizar copias de seguridad**, seleccione **Archivos/carpetas**.
2. Haga clic en **Elementos para incluir 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.

   Las normas de directiva se aplicarán a todos los equipos incluidos en el plan de protección. Si ninguno de los datos del equipo cumple como mínimo una de las normas, la copia de seguridad fallará cuando se inicie en ese equipo.
5. Haga clic en **Realizado**.

Reglas de selección para Windows

- Ruta completa a un archivo o carpeta, por ejemplo **D:\Work\Text.doc** o **C:\Windows**.
- Plantillas:
  - `[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 (normalmente, **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 (normalmente, **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 donde se encuentra 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, escriba **%PROGRAMFILES%\Java**.

Reglas de selección para Linux

- Ruta completa a un archivo o directorio. Por ejemplo, para realizar una copia de seguridad de **file.txt** en el volumen **/dev/hda3** incorporado en **/home/usr/docs**, especifique **/dev/hda3/file.txt** o **/home/usr/docs/file.txt**.
  - `/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.
- Plantillas:

- `[All Profiles Folder]` selecciona **/home**. En esta carpeta se ubican todos los perfiles de usuario de manera predeterminada.

Reglas de selección para macOS

- Ruta completa a un archivo o directorio.
- Plantillas:
  - `[All Profiles Folder]` selecciona **/Users**. En esta carpeta se ubican todos los perfiles de usuario de manera predeterminada.

Ejemplos:

- Para realizar una copia de seguridad de **file.txt** en su escritorio, especifique **/Users/<username>/Desktop/file.txt**. En este caso, <username> es su nombre de usuario.
- Para realizar copias de seguridad de todos los directorios de inicio de los usuarios, especifique **/Users**.
- Para realizar copias de seguridad del directorio donde están instaladas las aplicaciones, especifique **/Applications**.

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.
- Para hacer una copia de seguridad de la configuración ESXi, el Agente para VMware utiliza una conexión SSH para el host ESXi en el puerto TCP 22. Asegúrese de que su firewall no bloquea esta conexión.
- 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 VMware vSphere 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 **Copia de seguridad**.
3. En **De qué realizar copias de seguridad**, seleccione **Configuración de ESXi**.
4. En **Contraseña "raíz" de ESXi**, indique una contraseña para la cuenta "raíz" de cada uno de los servidores seleccionados o aplique la misma contraseña a todos los servidores.

Protección continua de datos (CDP)

Las copias de seguridad se suelen llevar a cabo con intervalos regulares pero bastante largos debido a razones de rendimiento. Si el sistema se daña de repente, se perderán los cambios que se hayan producido en los datos entre la última copia de seguridad y el fallo del sistema.

La funcionalidad **Protección continua de datos** le permite realizar copias de seguridad de los cambios que tengan lugar en los datos seleccionados entre una copia de seguridad planificada y la siguiente de forma continua:

- Realizando un seguimiento de los cambios que tengan lugar en los archivos o las carpetas especificados
- Realizando un seguimiento de los cambios que tengan lugar en los archivos modificados por las aplicaciones especificadas

Puede seleccionar archivos concretos para que se aplique en ellos la protección continua de datos a partir de los datos seleccionados de una copia de seguridad. El sistema realizará una copia de seguridad de todos los cambios que se produzcan en estos archivos. Puede recuperar estos archivos tal y como se encontraban en el momento en que se hizo el último cambio.

Actualmente, la función **Protección continua de datos** es compatible con los siguientes sistemas operativos:

- Windows 7 y posterior
- Windows Server 2008 R2 y posterior

Sistema de archivos compatible: Solo NTFS, solo carpetas locales (las carpetas compartidas no son compatibles)

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

Nota

Las funciones varían según la edición. Puede que algunas de las funciones descritas en esta documentación no estén disponibles con su licencia. Para obtener más información sobre las funciones que incluye cada edición, consulte Comparación de ediciones de Acronis Cyber Protect 15 que incluyen implementaciones en la nube.

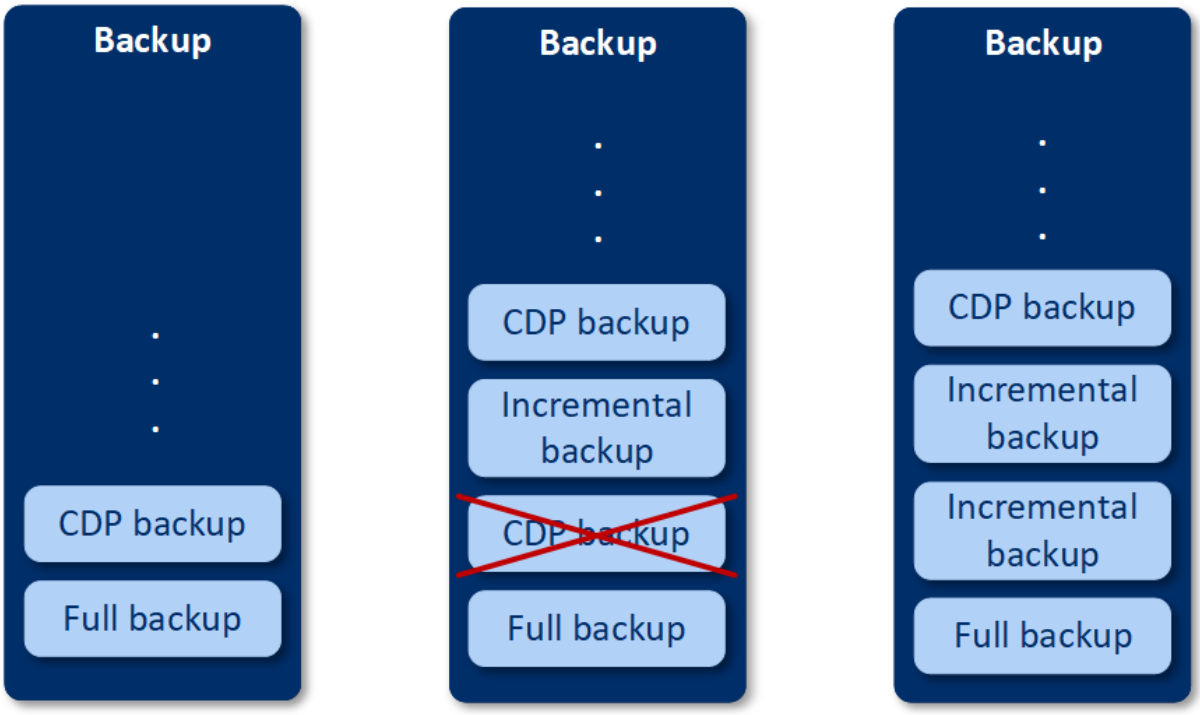
Cómo funciona

A la copia de seguridad que se crea de forma continua la llamaremos "copia de seguridad de la CDP". Para que se cree la copia de seguridad de la CDP, se tiene que crear primero una copia de seguridad completa o una incremental.

La primera vez que ejecute el plan de protección con el módulo de copia de seguridad y la opción **Protección continua de datos** habilitados, se creará primero una copia de seguridad completa. Justo después, se creará una copia de seguridad de la CDP de las carpetas o los archivos seleccionados o en los que se hayan producido cambios. La copia de seguridad de la CDP siempre incluye los datos que usted haya seleccionado en el último estado. Cuando realice cambios en las carpetas o los archivos seleccionados, no se creará ninguna copia de seguridad de la CDP, sino que todos los cambios se registrarán en la misma copia de seguridad de la CDP.

Cuando llegue el momento de realizar una copia de seguridad incremental planificada, se archivará la copia de seguridad de la CDP y se creará una copia de seguridad de la CDP nueva cuando se haya realizado la incremental.

Por tanto, la copia de seguridad de la CDP siempre se conserva como la última copia de seguridad de la cadena que tiene el estado más actual de los archivos o las carpetas protegidos.



Si ya tiene un plan de protección con el módulo de copia de seguridad habilitado y decide habilitar la opción **Protección continua de datos**, la copia de seguridad de la CDP se creará justo después de habilitar esta opción porque la cadena de copia de seguridad ya tendrá copias de seguridad completas.

Orígenes de datos y destinos compatibles con la protección continua de datos

Para que la protección continua de datos funcione correctamente, tiene que especificar los siguientes elementos para los siguientes orígenes de datos:

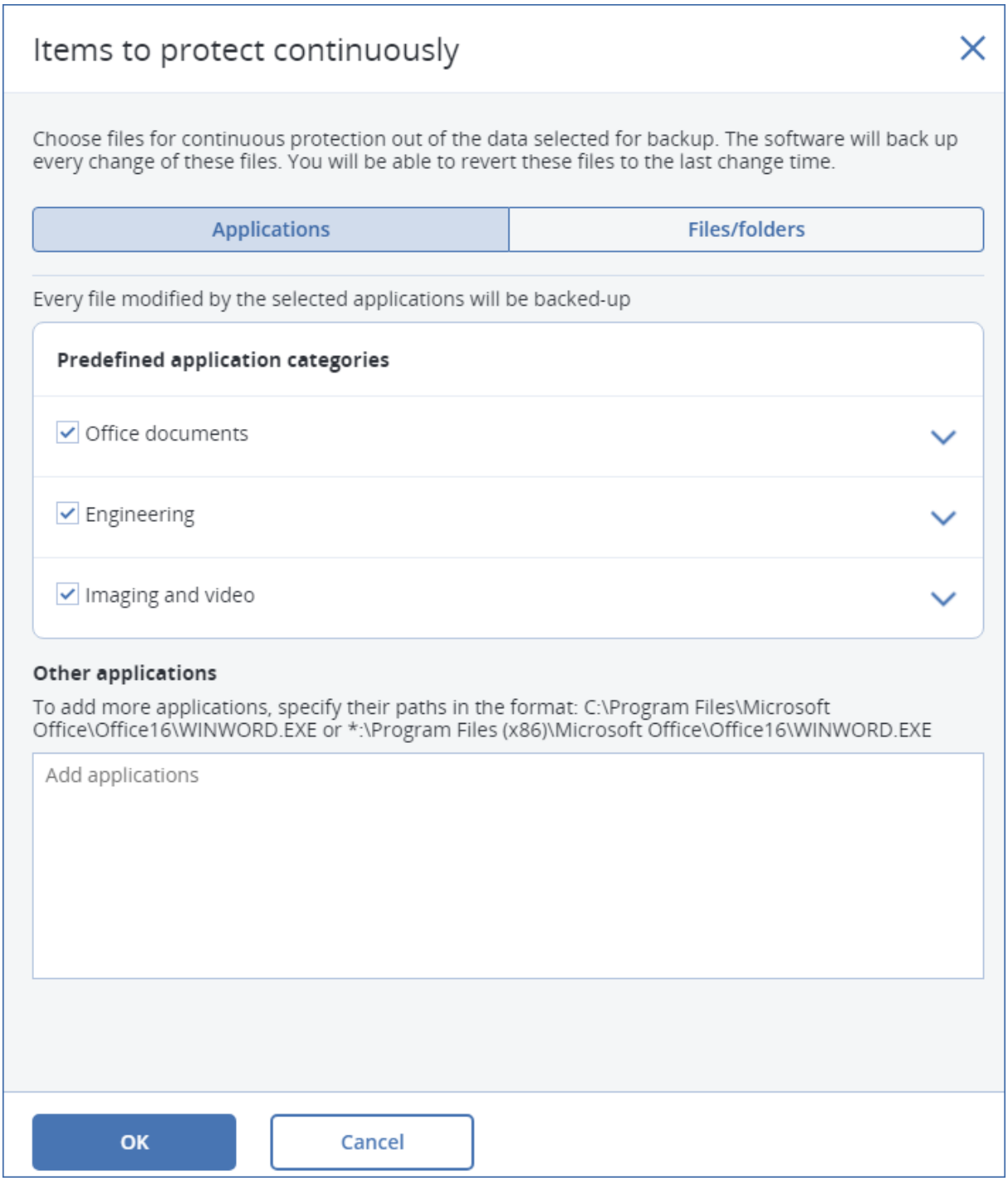
Qué incluir en la copia de seguridad	Elementos de los cuales realizará la copia de seguridad
Todo el equipo	Se deben especificar los archivos/las carpetas o aplicaciones.
Discos/volúmenes	Se deben especificar los discos/volúmenes, y los archivos/las carpetas o las aplicaciones.
Archivos/carpetas	Se deben especificar los archivos o las carpetas. Se pueden especificar las aplicaciones, pero no es obligatorio.

Los siguientes destinos de copia de seguridad son compatibles con la protección continua de datos:

- Carpeta local
- Carpeta de red
- Ubicación definida por secuencia de comandos
- Almacenamiento en la cloud
- Acronis Cyber Infrastructure

Pasos para proteger los dispositivos con la protección continua de datos

1. En la consola web de Cyber Protect, cree un plan de protección con el módulo **Copia de seguridad** habilitado.
2. Habilite la opción **Protección continua de datos (CDP)**.
3. Especifique los **elementos que desea proteger de forma continua**:
   - **Aplicaciones** (se realizará una copia de seguridad de todos los archivos modificados por las aplicaciones seleccionadas). Le recomendamos que use esta opción para proteger los documentos de Office con la copia de seguridad CDP.



- Puede seleccionar las aplicaciones de las categorías predefinidas o especificar otras. Para hacerlo, indique la ruta que lleva al archivo ejecutable de la aplicación. Utilice uno de los siguientes formatos:

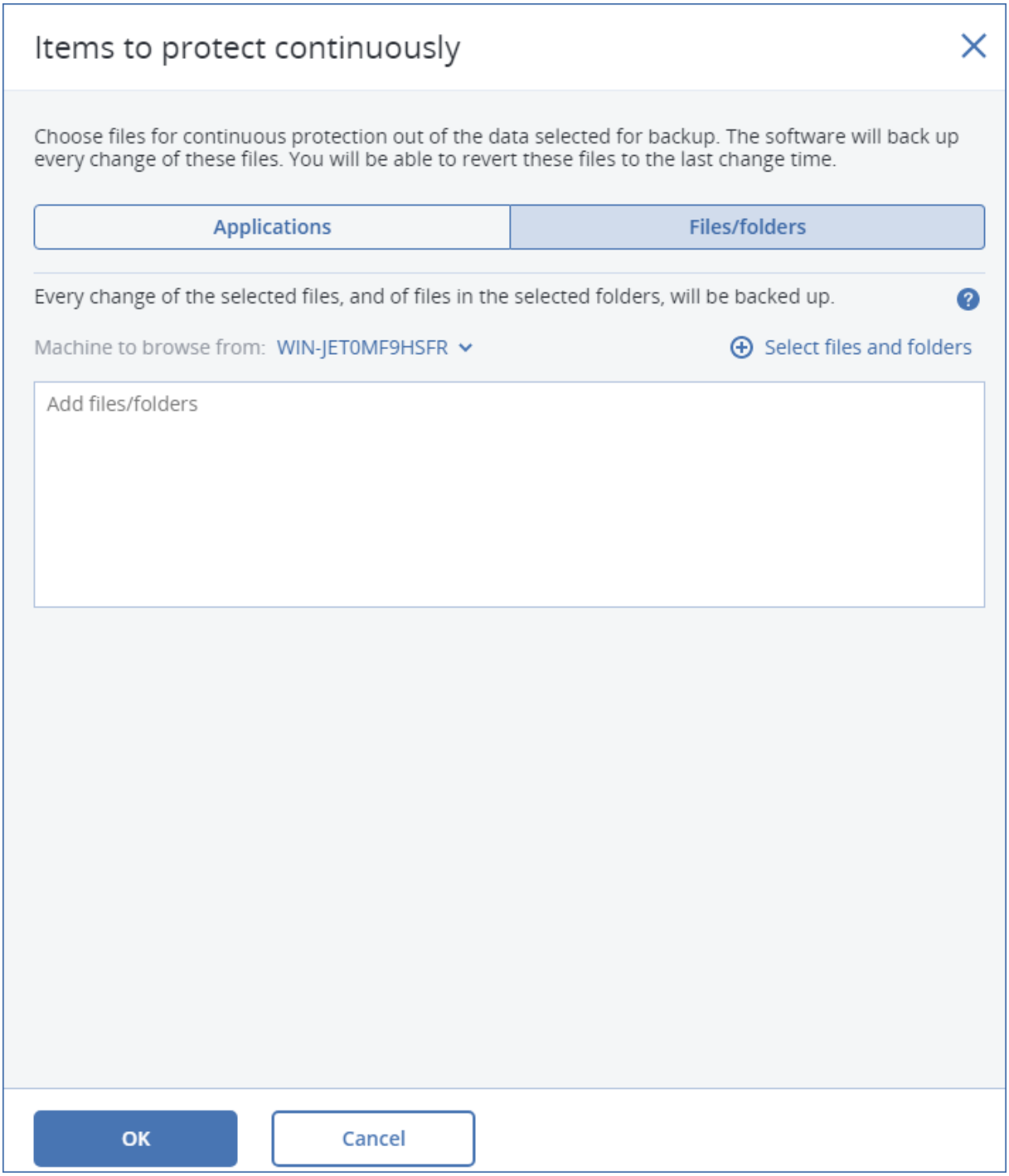
  `C:\Program Files\Microsoft Office\Office16\WINWORD.EXE`

  O

  `*:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE`

  - **Archivos/carpetas** (se realizará una copia de seguridad de todos los archivos modificados en

la ubicación especificada). Le recomendamos que use esta opción para proteger aquellos archivos o esas carpetas que cambian continuamente.



1. **Equipo desde el cual examinar**: especifique el equipo cuyos archivos y carpetas quiera seleccionar para aplicar en ellos la protección continua de datos.

   Haga clic en **Seleccionar archivos y carpetas** para seleccionar los archivos o las carpetas en el equipo especificado.

Importante
Si especifica manualmente una carpeta entera de cuyos archivos se realizará una copia de seguridad de forma continua, use la máscara, por ejemplo:
Ruta correcta: D:\Data*
Ruta incorrecta: D:\Data\

En el campo de texto, puede especificar también reglas para los archivos o las carpetas de los que se vaya a realizar la copia de seguridad. Pero tenemos información sobre cómo definir reglas, consulte "Seleccionar archivos/carpetas". Haga clic en **Listo** cuando tenga todo a punto.

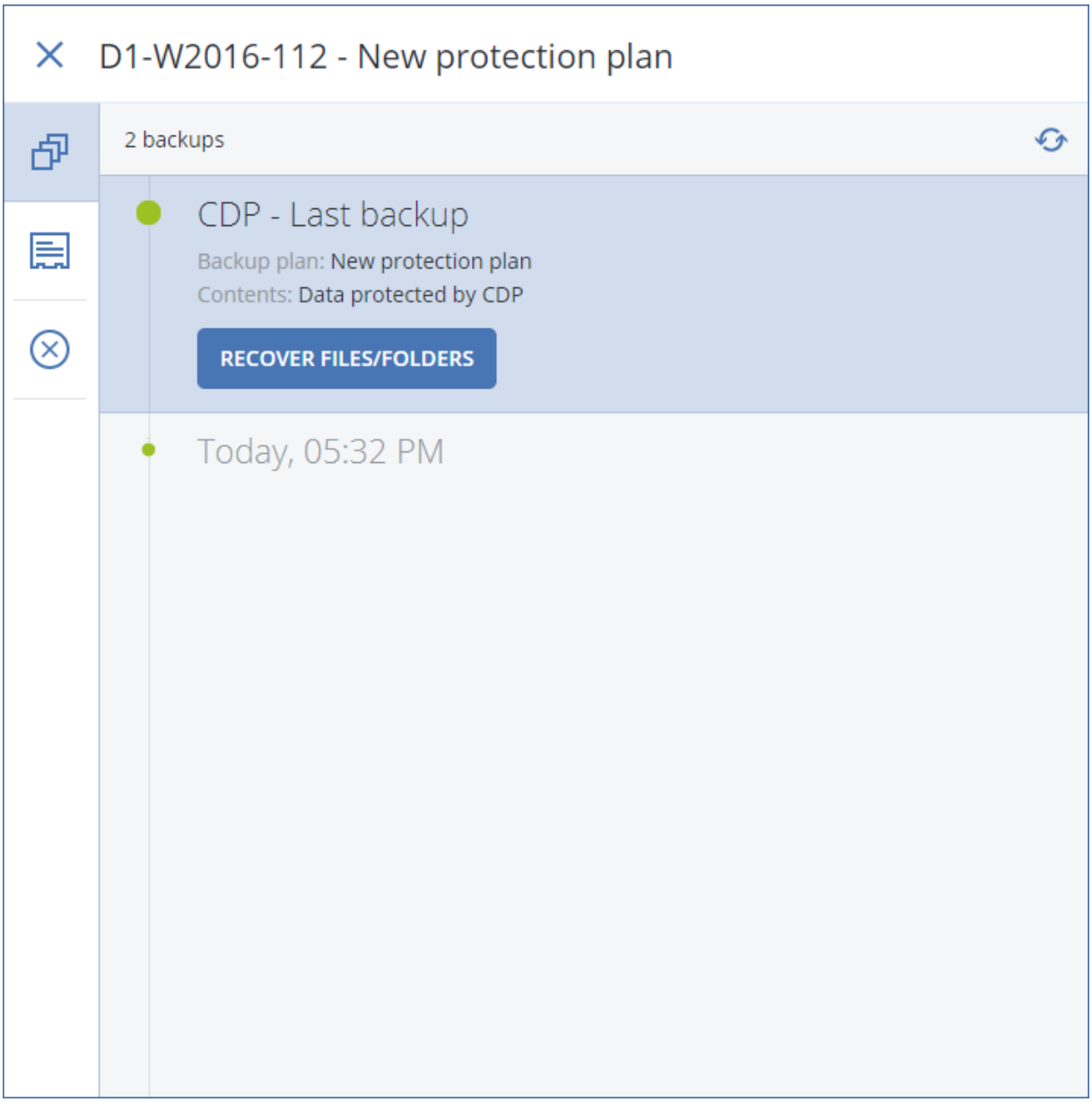
2. Haga clic en **Crear**.

Como resultado, el plan de protección con la protección continua de datos habilitada se asignará al equipo seleccionado. Después de que se lleve a cabo la primera copia de seguridad regular, se crearán de forma continua las copias de seguridad con la última copia de los datos protegidos por la CDP. Se realizará una copia de seguridad tanto de los datos definidos mediante las aplicaciones como aquellos de los archivos o las carpetas.

Los datos de los que se realizan copias de seguridad continuas se retienen de acuerdo con la directiva de retención definida por el módulo de copia de seguridad.

Cómo distinguir las copias de seguridad que están protegidas de forma continua

Las copias de seguridad que se realizan de forma continua tienen el prefijo CDP.



Cómo recuperar todo su equipo al último estado

Si quiere recuperar un equipo completo a su último estado, puede utilizar la opción **Protección continua de datos (CDP)** del módulo de copia de seguridad de un plan de protección.

Puede recuperar un equipo entero o los archivos o las carpetas de una copia de seguridad de la CDP. En el primer caso obtendrá el equipo completo en su último estado; en el segundo, los archivos o las carpetas en su último estado.

Seleccionar un destino

Importante
Algunas de las funciones descritas en esta sección solo están disponibles en implementaciones locales.

Para seleccionar una ubicación de copia de seguridad

1. Haga clic en **Dónde realizar copias de seguridad**.
2. Realice uno de los siguientes procedimientos:
   - Seleccionar una ubicación de copia de seguridad predefinida o usada previamente
   - Haga clic en **Agregar ubicación** y después especificar una nueva ubicación de la copia de seguridad.

Ubicaciones compatibles

- **Almacenamiento en la cloud**
  Las copias de seguridad se almacenarán en el centro de datos de la cloud.
- **Carpeta local**
  Si se selecciona un único equipo, busque una carpeta en el equipo seleccionado o escriba la ruta de la carpeta.
  Si se seleccionan varios equipos, escriba la ruta de la carpeta. Las copias de seguridad se almacenarán en esta carpeta en cada uno de los equipos seleccionados o en el equipo en el que está instalado el Agente para equipos virtuales. Si la carpeta no existe, se creará.
- **Carpeta de red**
  Esta carpeta se comparte a través de SMB/CIFS/DFS.
  Busque la carpeta compartida requerida o escriba la ruta con el siguiente formato:
  - Para recursos compartidos de SMB o CIFS: `\\<host name>\<path>\` o `smb://<host name>/<path>/`.
  - Para recursos compartidos de DFS: `\\<full DNS domain name>\<DFS root>\<path>`.
    Por ejemplo, `\\ejemplo.empresa.com\archivos\compartidos`.

  Luego haga clic en el botón de la flecha. Si se le pide, especifique el nombre de usuario y la contraseña de la carpeta compartida. Puede modificar estas credenciales en cualquier momento al hacer clic en el icono de llave que se encuentra junto al nombre de la carpeta.
  No se admite la copia de seguridad a una carpeta con acceso anónimo.
- **Acronis Cyber Infrastructure**
  Acronis Cyber Infrastructure se puede usar como almacenamiento definido por software muy fiable con redundancia de datos y autorrecuperación automática. Este almacenamiento puede configurarse como una puerta de enlace para almacenar copias de seguridad en Microsoft Azure o en las diversas soluciones de almacenamiento compatibles con S3 o Swift. El almacenamiento

también puede utilizar el back-end de NFS. Para obtener más información, consulte «Acerca de Acronis Cyber Infrastructure».

Importante
Las copias de seguridad en Acronis Cyber Infrastructure no están disponibles para equipos macOS.

- **Carpeta NFS** (disponible para equipos que ejecutan Linux o macOS)
  Compruebe que el paquete nfs-utils esté instalado en el equipo Linux en el que está instalado el agente para Linux.
  Busque la carpeta NFS requerida o introduzca la ruta con el siguiente formato:
  `nfs://<host name>/<exported folder>:/<subfolder>`
  Luego haga clic en el botón de la flecha.
  No se puede realizar una copia de seguridad en una carpeta NFS protegida con contraseña.
- **Secure Zone** (disponible si está en todos los equipos seleccionados)
  Secure Zone es una partición segura que está en un disco del equipo incluido en la copia de seguridad. Esta partición debe crearse manualmente antes de configurar una copia de seguridad. Para obtener información sobre cómo crear Secure Zone y sus ventajas y limitaciones, consulte "Acerca de Secure Zone".
- **SFTP**
  Escriba el nombre o dirección IP del servidor SFTP. Las siguientes notaciones son compatibles:
  `sftp://<server>`
  `sftp://<server>/<folder>`
  Después de introducir el nombre de usuario y la contraseña, puede examinar las carpetas del servidor.
  En cualquier notación, también puede especificar el puerto, el nombre de usuario y la contraseña.
  `sftp://<server>:<port>/<folder>`
  `sftp://<user name>@<server>:<port>/<folder>`
  `sftp://<user name>:<password>@<server>:<port>/<folder>`
  Si no se especifica el número de puerto, se utilizará el puerto 22.
  Los usuarios que tengan configurado un acceso SFTP sin contraseña no podrán realizar copias de seguridad a SFTP.
  La copia de seguridad en servidores FTP no es compatible.

Opciones de almacenamiento avanzadas

- **Definido por una secuencia de comandos** (disponible en equipos Windows)
  Puede almacenar las copias de seguridad de cada equipo en una carpeta definida por un script. El software es compatible con comandos escritos en JScript, VBScript o Python 3.5. Al implementar el plan de protección, el software ejecuta el comando en todos los equipos. El resultado del script para cada equipo debería ser una ruta de carpeta local o de red. Si una

carpeta no existe, se creará (limitación: los comandos escritos en Python no pueden crear carpetas en redes compartidas). En la pestaña **Almacenamiento de copias de seguridad**, cada carpeta aparece como una ubicación de copia de seguridad independiente.

En **Tipo de secuencia de comandos**, seleccione el tipo de script (**JScript**, **VBScript** o **Python**), e importe el script, o cópielo y péguelo. Con carpetas de red, especifique las credenciales de acceso con permiso de lectura y escritura.

Ejemplos:

- El siguiente comando **JScript** devuelve la ubicación de la copia de seguridad para un equipo con el formato `\\bkpsrv\<machine name>`:

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

- El siguiente comando **JScript** da salida a la ubicación de la copia de seguridad en una carpeta del equipo en el que se ejecuta dicho comando:

  ```
  WScript.Echo("C:\\Backup");
  ```

  Nota
  La ruta de la ubicación de estos comandos distingue entre mayúsculas y minúsculas. Por lo tanto, `C:\Backup` y `C:\backup` se muestran como distintas ubicaciones en la consola web de Cyber Protect. Use mayúsculas para la letra de unidad.

- El siguiente comando **VBScript** devuelve la ubicación de la copia de seguridad para un equipo con el formato `\\bkpsrv\<machine name>`:

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

De ese modo, las copias de seguridad de cada equipo se guardarán en una carpeta con el mismo nombre en el servidor **bkpsrv**.

- **Nodo de almacenamiento**

  Un nodo de almacenamiento es un servidor diseñado para optimizar el uso de diversos recursos (como, por ejemplo, la capacidad de almacenamiento corporativo, el ancho de banda de red o la carga de la CPU de los servidores de producción) necesarios para proteger los datos de la empresa. Este objetivo se consigue gracias a la organización y la gestión de ubicaciones que funcionan como almacenamientos dedicados de las copias de seguridad de la empresa (ubicaciones gestionadas).

  Puede seleccionar una ubicación creada con anterioridad o crear una nueva haciendo clic en **Agregar ubicación** > **Nodo de almacenamiento**. Para obtener más información acerca de los ajustes, consulte "Incorporación de la ubicación gestionada".

  Puede que se le solicite que especifique el nombre de usuario y la contraseña del nodo de almacenamiento. Los miembros de los siguientes grupos de Windows del equipo en donde el nodo de almacenamiento esté instalado tienen acceso a todas las ubicaciones gestionadas en dicho nodo.

- **Administradores**
- **Usuarios remotos de Acronis ASN**

  El grupo se crea automáticamente al instalar el nodo de almacenamiento. De manera predeterminada, el grupo está vacío. Puede agregar usuarios a este grupo manualmente.

- **Cinta**

  Si se conecta un dispositivo de cintas al equipo donde se realiza la copia de seguridad o a un nodo de almacenamiento, la lista de ubicaciones muestra el pool de cintas predeterminado. Este pool se crea automáticamente.

  Puede seleccionar el pool predeterminado o crear uno nuevo haciendo clic en **Agregar ubicación** > **Cinta**. Para obtener más información acerca de los ajustes del pool, consulte "Creación de un pool".

Acerca de Secure Zone

Secure Zone es una partición segura que está en un disco del equipo incluido en la copia de seguridad. La partición puede almacenar copias de seguridad de discos o archivos de este equipo.

Si el disco presenta un error físico, las copias de seguridad almacenadas en Secure Zone podrían perderse. Esa es la razón por la que Secure Zone no debe ser la única ubicación donde se almacene una copia de seguridad. En entornos empresariales, se puede pensar en Secure Zone como una ubicación intermedia utilizada para realizar copias de seguridad cuando una ubicación normal no está disponible temporalmente o se conecta a partir de un canal lento u ocupado.

¿Por qué se debe usar Secure Zone?

Secure Zone:

- Permite la recuperación de un disco en el mismo disco en donde reside la copia de seguridad del disco.
- Constituye un método rentable y práctico para la protección de datos ante un funcionamiento defectuoso del software, ataques de virus o errores humanos.
- Elimina la necesidad de medios o conexiones de red diferentes para realizar copias de seguridad o recuperar los datos. Esto es muy útil para los usuarios itinerantes.
- Puede funcionar como destino primario cuando se usa la replicación de copias de seguridad.

Limitaciones

- Secure Zone no se puede organizar en un Mac.
- Secure Zone es una partición en un disco básico. No puede organizarse en un disco dinámico ni crearse como volumen lógico (administrado por LVM).
- Secure Zone tiene el formato de sistema de archivos FAT32. Como FAT32 tiene un límite de tamaño de archivos de 4 GB, las copias de seguridad de mayor tamaño se dividen al guardarse en Secure Zone. Esto no afecta al procedimiento de recuperación ni a la velocidad.

Cómo la creación de Secure Zone transforma el disco

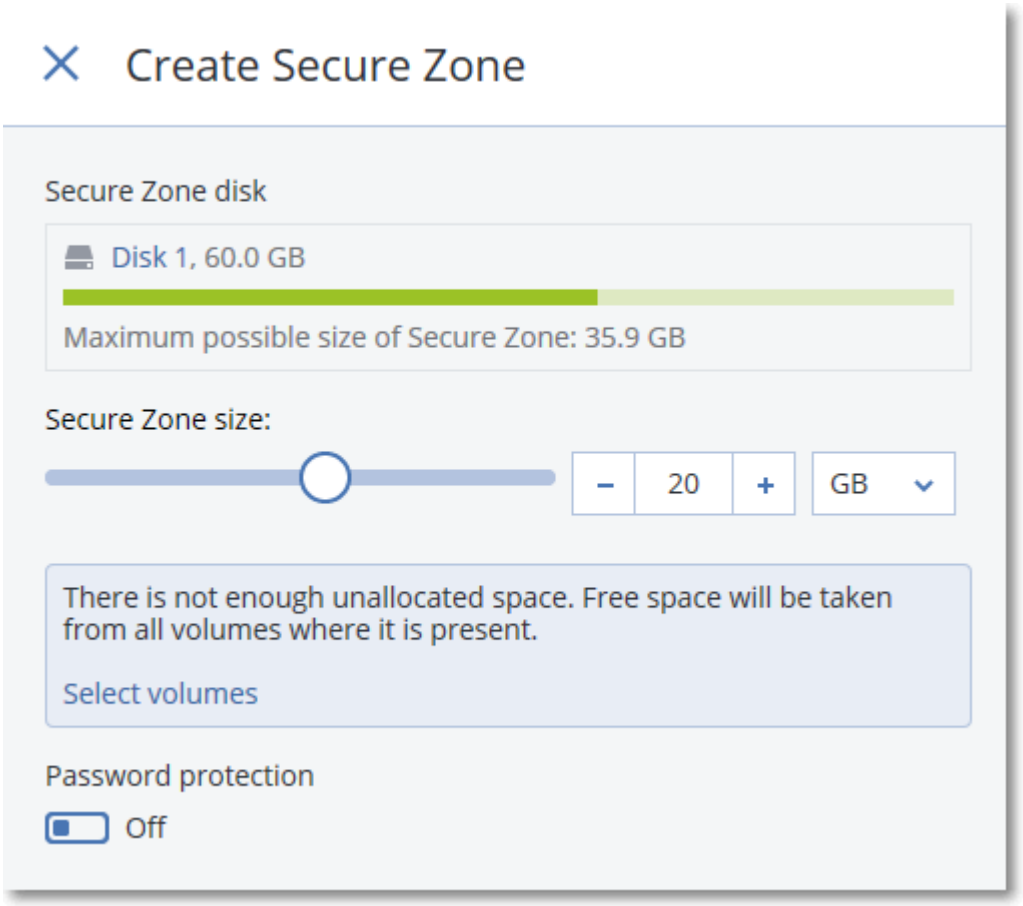
- Secure Zone siempre se crea al final del disco rígido.
- Si no hay espacio sin asignar suficiente o no hay al final del disco, pero sí hay espacio sin asignar entre volúmenes, estos últimos se moverán para agregar más espacio sin asignar al final del disco.
- Cuando se recopile todo el espacio sin asignar y el mismo siga siendo insuficiente, el software sacará espacio libre de los volúmenes que seleccione, de forma proporcional, reduciendo el tamaño de los volúmenes.
- Sin embargo, debería haber espacio libre en un volumen para que el sistema operativo y las aplicaciones puedan funcionar; por ejemplo, para crear archivos temporales. El software no reducirá un volumen en el que el espacio libre ocupe el 25 % o menos del tamaño total del volumen. El software continuará reduciendo los volúmenes de forma proporcional únicamente cuando todos los volúmenes del disco tengan el 25 % o menos espacio libre.

Como se deduce de esto, no es recomendable especificar el tamaño máximo posible para Secure Zone. Acabará sin espacio libre en ningún volumen, lo que puede hacer que el sistema operativo o las aplicaciones funcionen de forma inestable e incluso que no puedan iniciarse.

Importante
Para mover o cambiar el tamaño del volumen desde el que se arranca el sistema actualmente, es necesario reiniciar.

Cómo crear Secure Zone

1. Seleccione el equipo en el que desea crear Secure Zone.
2. Haga clic en **Detalles** > **Crear Secure Zone**.
3. En el **disco Secure Zone**, haga clic en **Seleccionar** y, a continuación, elija el disco rígido (si hay más de uno) en el que desea crear la zona.
   El software calcula el tamaño máximo posible de Secure Zone.
4. Introduzca el tamaño de Secure Zone o arrastre el deslizador para seleccionar cualquier tamaño entre los mínimos y los máximos.
   El tamaño mínimo es de aproximadamente 50 MB, de acuerdo con la geometría del disco duro.
   El tamaño máximo es igual al espacio sin asignar del disco más el espacio libre total de todos los volúmenes del disco.
5. Si el espacio sin asignar no es suficiente para el tamaño que ha indicado, el software obtendrá el espacio libre de los volúmenes existentes. De manera predeterminada, se seleccionan todos los volúmenes. Si desea excluir algunos volúmenes, haga clic en **Seleccionar volúmenes**. De lo contrario, omita este paso.



6. [Opcional] Habilite el conmutador **Protección mediante contraseña** y especifique una contraseña.
   La contraseña es obligatoria para acceder a las copias de seguridad ubicadas en Secure Zone. No se necesita contraseña para realizar una copia de seguridad en Secure Zone, salvo que dicha copia de seguridad se haga en un soporte de arranque.
7. Haga clic en **Crear**.
   El software muestra la distribución esperada de la partición. Haga clic en **Aceptar**.
8. Espere mientras el software crea Secure Zone.

Ahora puede escoger Secure Zone en **Dónde realizar copias de seguridad** al crear un plan de protección.

Cómo eliminar Secure Zone

1. Seleccione un equipo con Secure Zone.
2. Haga clic en **Detalles**.
3. Haga clic en el icono de engranaje situado junto a **Secure Zone** y, a continuación, haga clic en **Eliminar**.
4. [Opcional] Seleccione los volúmenes a los que desea agregar el espacio liberado de la zona. De manera predeterminada, se seleccionan todos los volúmenes.

El espacio se distribuirá a partes iguales entre los volúmenes seleccionados. Si no selecciona ningún volumen, el espacio liberado se convertirá en espacio sin asignar.

Para cambiar el tamaño del volumen desde el que se arranca el sistema, es necesario reiniciar.

5. Haga clic en **Eliminar**.

Como resultado, se eliminan Secure Zone y todas las copias de seguridad almacenadas en ella.

Acerca de Acronis Cyber Infrastructure

Acronis Cyber Protect 15 admite la integración con Acronis Cyber Infrastructure 3.5 a partir de la actualización 5 o posterior.

Las copias de seguridad en Acronis Cyber Infrastructure no están disponibles para equipos macOS.

Implementación

Para usar Acronis Cyber Infrastructure, impleméntelo en una instalación desde cero en un sistema local. Se recomienda tener al menos cinco servidores físicos para sacar el máximo partido al producto. Si solo necesita la funcionalidad de puerta de enlace, puede usar un servidor físico o virtual, o configurar un clúster de puerto de enlace con todos los servidores que desee.

Asegúrese de que la configuración de hora esté sincronizada entre el servidor de gestión y Acronis Cyber Infrastructure. La configuración de hora de Acronis Cyber Infrastructure puede establecerse durante la implementación. La sincronización de hora mediante Network Time Protocol (NTP) está habilitada de forma predeterminada.

Puede implementar varias instancias de Acronis Cyber Infrastructure y registrarlas en el mismo servidor de gestión.

Registro

El registro se lleva a cabo en la interfaz web de Acronis Cyber Infrastructure. Solo los administradores de la organización pueden registrar Acronis Cyber Infrastructure, y únicamente puede llevarse a cabo en la organización. Una vez registrado, el almacenamiento estará disponible para todas las unidades de la organización. Puede añadirse como una ubicación de copia de seguridad a cualquier unidad o a la organización.

La operación inversa (anulación de registro) se lleva a cabo en la interfaz de Acronis Cyber Protect. Haga clic en **Configuración** > **Nodos de almacenamiento** y, a continuación, en infraestructura definida por Acronis Cyber Infrastructure y en **Eliminar**.

Incorporación de una ubicación de la copia de seguridad

Solo puede añadirse una ubicación de copia de seguridad en cada instancia de Acronis Cyber Infrastructure a una unidad u organización. Una ubicación añadida en el nivel de unidad estará disponible para esta unidad y para los administradores de la organización. Una ubicación añadida en el nivel de organización estará disponible únicamente para los administradores de la organización.

Al añadir una ubicación, creará e introducirá el nombre de esta. Si necesita añadir una ubicación existente a un servidor de gestión nuevo o diferente, active la casilla de verificación **Usar una ubicación existente...**, haga clic en **Examinar** y seleccione la ubicación en la lista.

Si hay registradas varias instancias de Acronis Cyber Infrastructure en el servidor de gestión, puede seleccionarse una instancia de Cyber Infrastructure al añadir una ubicación.

Esquemas, operaciones y limitaciones de copias de seguridad

El acceso directo a Acronis Cyber Infrastructure desde el dispositivo de arranque no está disponible. Para trabajar con Acronis Cyber Infrastructure, registre el dispositivo en el servidor de gestión y gestiónelo mediante la consola web de Cyber Protect.

El acceso a Acronis Cyber Infrastructure mediante la interfaz de la línea de comandos no está disponible.

En términos de esquemas de copias de seguridad disponibles y operaciones con copias de seguridad, Acronis Cyber Infrastructure es similar al almacenamiento en la nube. La única diferencia es que las copias de seguridad pueden replicarse *desde* Acronis Cyber Infrastructure durante la ejecución de un plan de protección.

Documentación

Toda la documentación de Acronis Cyber Infrastructure está disponible en el sitio web de Acronis.

Planificación

Importante
Algunas de las funciones descritas en esta sección solo están disponibles en implementaciones locales.

La planificación usa la configuración de hora (incluida la zona horaria) del sistema operativo en el que el agente está instalado. La zona horaria de Agente para VMware (dispositivo virtual) se puede configurar en la interfaz del agente.

Por ejemplo, si un plan de protección está planificado para ejecutarse a las 21:00 y aplicarse a varios equipos ubicados en zonas horarias diferentes, la copia de seguridad se iniciará en cada equipo a las 21:00 (hora local).

Los parámetros de planificación dependen del destino de la copia de seguridad.

Cuando realice copias de seguridad en el almacenamiento en la cloud

De forma predeterminada, las copias de seguridad se realizan a diario de lunes a viernes. Puede seleccionar la hora a la que la copia de seguridad se ejecutará.

Si quiere cambiar la frecuencia con que se realizan las copias de seguridad, mueva el control deslizante y especifique la planificación de las copias de seguridad.

Puede programar la copia de seguridad para que se ejecute en función de los eventos, en lugar de la hora. Para hacerlo, seleccione el tipo de evento en el selector de planificación. Para obtener más información, consulte "Planificación por eventos" (p. 286).

Importante
La primera copia de seguridad es completa, por lo que precisa más tiempo. Las copias posteriores son incrementales y requieren mucho menos tiempo.

Cuando realice copias de seguridad en otras ubicaciones

Puede elegir uno de los esquemas de copias de seguridad predefinidos o crear un esquema personalizado. Un esquema de copias de seguridad es parte del plan de protección que incluye la planificación de copia de seguridad y los métodos de copias de seguridad.

En el **esquema de copias de seguridad**, seleccione una de las siguientes opciones:

- **Siempre incremental (archivo único)**
  De forma predeterminada, las copias de seguridad se realizan a diario de lunes a viernes. Puede seleccionar la hora a la que la copia de seguridad se ejecutará.
  Si quiere cambiar la frecuencia con que se realizan las copias de seguridad, mueva el control deslizante y especifique la planificación de las copias de seguridad.
  Las copias de seguridad usan el nuevo formato de copia de seguridad de archivo único[1].
  Este esquema no está disponible al hacer una copia de seguridad en un dispositivo de cintas o un servidor SFTP.
- **Siempre completas**
  De forma predeterminada, las copias de seguridad se realizan a diario de lunes a viernes. Puede seleccionar la hora a la que la copia de seguridad se ejecutará.
  Si quiere cambiar la frecuencia con que se realizan las copias de seguridad, mueva el control deslizante y especifique la planificación de las copias de seguridad.
  Todas las copias de seguridad son completas.
- **Completas semanalmente, incrementales diariamente**
  De forma predeterminada, las copias de seguridad se realizan a diario de lunes a viernes. Puede modificar los días de la semana y la hora a la que desea que se realicen las copias de seguridad.

[1] Es un nuevo formato de copia de seguridad en el que las copias de seguridad iniciales completas e incrementales subsiguientes se guardan en un único archivo .tib en lugar de una cadena de archivos. 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, por ejemplo: servidores SFTP.

Se crea una copia de seguridad completa una vez a la semana. El resto de copias de seguridad son incrementales. El día de creación de la copia de seguridad completa depende de la opción **Copias de seguridad semanales** (haga clic en el icono de engranaje y después, en **Opciones de copia de seguridad** > **Copias de seguridad semanales**).

- **Completa mensual, diferencial semanal, incremental diaria (GFS)**

  De manera predeterminada, las copias de seguridad incrementales se realizan diariamente, 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. Puede modificar esta planificación y la hora a la que la copia de seguridad se ejecutará.

  Este esquema de copias de seguridad se muestra como esquema **Personalizado** en el panel del plan de protección.

- **Personalizado**

  Especifique la planificación para las copias de seguridad completas, diferenciales e incrementales.

  La copia de seguridad diferencial no está disponible cuando se está realizando una copia de seguridad de datos SQL, de datos de Exchange o del estado del sistema.

Con cualquier esquema de copias de seguridad, puede programar la copia de seguridad para que se ejecute en función de los eventos, en lugar de la hora. Para hacerlo, seleccione el tipo de evento en el selector de planificación. Para obtener más información, consulte "Planificación por eventos" (p. 286).

Opciones de planificación adicionales

Con cualquier destino, puede realizar lo siguiente:

- Especifique las condiciones de inicio de la copia de seguridad, de forma que las copias de seguridad programadas se realicen solo si se cumplen las condiciones. Para obtener más información, consulte "Condiciones de inicio" (p. 289).
- Fije el rango de fechas en el que la planificación tendrá efecto. Seleccione la casilla de verificación **Ejecutar el plan en un rango de fechas** y especifique el rango de fechas.
- Deshabilite la planificación. Mientras la planificación está deshabilitada, no se aplican las normas de retención a menos que se inicie una copia de seguridad de forma manual.
- Especifique una demora a partir de la hora planificada. El valor de demora de cada equipo se selecciona de forma aleatoria y oscila entre cero y el valor máximo que especifique. Puede resultarle útil para evitar una carga excesiva de la red al realizar copias de seguridad de varios equipos simultáneamente en una misma ubicación de red. Para obtener más información, consulte "Planificación" (p. 350).

  Haga clic en el icono de engranaje y, a continuación, en **Opciones de copia de seguridad** > **Planificación**. Seleccione **Distribuir las horas de inicio de las copias de seguridad en un intervalo de tiempo** y, a continuación, especifique el valor máximo de demora. El valor de demora de cada equipo se determina cuando se aplica el plan de protección en el equipo y

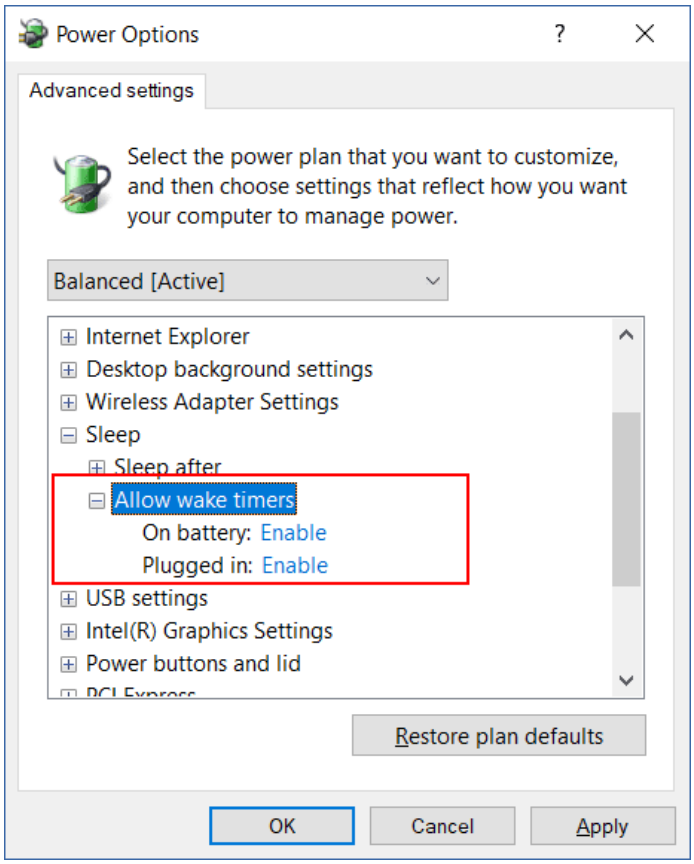
permanece igual hasta que se edita el plan de protección y se modifica el valor máximo de demora.

Nota
Esta opción está habilitada de forma predeterminada en las implementaciones en la nube, con un valor máximo de demora establecido en 30 minutos. En el caso de implementaciones locales, de manera predeterminada todas las copias de seguridad se inician según la planificación.

- [Solo disponible con la opción Planificación por tiempo] Haga clic en **Mostrar más** para acceder a las opciones siguientes:
  - **Si el equipo está apagado, ejecutar las tareas perdidas al iniciar el equipo** (deshabilitado de forma predeterminada)
  - **Evitar el modo de suspensión o hibernación durante una copia de seguridad** (habilitado de forma predeterminada)

    Esta opción solo se aplica en equipos que ejecuten Windows.
  - **Reactivar desde el modo de suspensión o hibernación para iniciar una copia de seguridad planificada** (deshabilitado de forma predeterminada)

    Esta opción solo se aplica a los equipos que ejecutan Windows y tienen la configuración **Permitir temporizadores de reactivación** habilitada en los planes de energía.



Esta opción no utiliza la funcionalidad Wake-On-LAN y no se aplica a los equipos apagados.

Planificación por eventos

Cuando se configura una programación para un plan de protección, puede seleccionar el tipo de evento en el selector de programación. La copia de seguridad se iniciará tan pronto se produzcan los eventos.

Puede escoger una de los siguientes eventos:

- **En el momento en que se realizó la última copia de seguridad**
  Este es el tiempo transcurrido desde la finalización de la última copia de seguridad correcta en el mismo plan de protección. Puede especificar la duración.

  Nota
  Dado que la programación se basa en una copia de seguridad que se ha realizado correctamente, si una copia de seguridad no llega a efectuarse con éxito, el programador no ejecutará de nuevo la tarea hasta que un operador ejecute el plan de forma manual y dicha ejecución se complete correctamente.

- **Cuando un usuario inicia sesión en el sistema**
  De forma predeterminada, el inicio de sesión de cualquier usuario dará comienzo a una copia de seguridad. Puede cambiar cualquier usuario a una cuenta de usuario específica.
- **Cuando un usuario cierra sesión en el sistema**
  De forma predeterminada, el cierre de sesión de cualquier usuario dará comienzo a una copia de seguridad. Puede cambiar cualquier usuario a una cuenta de usuario específica.

  Nota
  La copia de seguridad no se ejecutará durante un apagado del sistema porque el apagado no es lo mismo que el cierre de sesión.

- **Al iniciarse el sistema**
- **Al apagarse el sistema**
- **Al ocurrir un evento en el registro de eventos de Windows**
  Debe especificar las propiedades del evento.

En la siguiente tabla se muestran los eventos disponibles para diversos datos en Windows, Linux y macOS.

DE QUÉ REALIZAR COPIAS DE SEGURIDAD	Desde el momento en que se realizó la última copia de seguridad	Cuando un usuario inicia sesión en el sistema	Cuando un usuario cierra sesión en el sistema	Al iniciarse el sistema	Al apagarse el sistema	Al ocurrir un evento en el registro de eventos

						de Windows
Discos/volúmenes o archivos (equipos físicos)	Windows, Linux y macOS	Windows	Windows	Windows, Linux y macOS	Windows	Windows
Discos/volúmenes (equipos virtuales)	Windows, Linux	–	–	–	–	–
Configuración de ESXi	Windows, Linux	–	–	–	–	–
Buzones de correo de Microsoft 365	Windows	–	–	–	–	Windows
Buzones de correo y bases de datos de Exchange	Windows	–	–	–	–	Windows
Bases de datos SQL	Windows	–	–	–	–	Windows

Al ocurrir un evento en el registro de eventos de Windows

Puede planificar una copia de seguridad para que se inicie al registrarse un evento en particular en uno de los registros de eventos de Windows, tales como los registros de la **Aplicación**, **Seguridad** o del **Sistema**.

Por ejemplo, podría crear un plan de protección que realice automáticamente una copia de seguridad completa de emergencia con sus datos en cuanto Windows detecte que se está por producir un error en su unidad de disco rígido.

Para examinar los eventos y ver las propiedades, utilice el complemento **Visor de eventos**, disponible en la consola **Administración del equipo**. Para abrir el registro de **Seguridad**, debe ser formar parte del grupo de **Administradores**.

Propiedades de evento

Nombre del registro

Especifica el nombre del registro. Seleccione en la lista el nombre de un registro estándar (**Aplicación, Seguridad** o **Sistema**) o escríbalo. Por ejemplo: **Sesiones de Microsoft Office**

Origen del evento

Especifica el origen del evento que, por lo general, indica qué programa o componente del sistema generó el evento. Por ejemplo: **disco**

Todos los orígenes de eventos que incluyan la cadena especificada activarán la copia de seguridad planificada. Esta opción no distingue entre mayúsculas y minúsculas. Por lo tanto, si especifica la cadena **servicio**, los orígenes de evento **Administrador de control del servicio** y **Tiempo-servicio** activarán una copia de seguridad.

Tipo de evento

Especifica el tipo de suceso: **Error**, **Advertencia**, **Información**, **Auditoría correcta** o **Error en auditoría**.

ID del evento

Especifica el número del suceso, que suele identificar los tipos de sucesos en particular entre sucesos del mismo origen.

Por ejemplo, un evento **Error** con Origen del evento **disco** e ID del evento **7** ocurre cuando Windows descubre 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 todavía no está preparado.

Ejemplo: Copia de seguridad de emergencia "Bloque dañado"

La aparición repentina de uno o más bloques dañados en un disco duro generalmente indica que pronto se producirá un error en la unidad de disco duro. Supongamos que desea crear un plan de protección para copiar datos del disco rígido en cuanto se presente tal situación.

Cuando Windows detecta un bloque dañado en un disco duro, registra un suceso en el **disco** de origen del suceso y el número de suceso **7** en el registro del **Sistema**; el tipo de suceso es **Error**.

Al crear un plan, escriba o seleccione las siguientes opciones en la sección **Programar**:

- **Nombre del registro**: **Sistema**
- **Disco Origen del evento**:
- **Tipo de evento**: **Error**
- **Id. suceso**: **7**

Importante
Para garantizar que dicha copia de seguridad se realice a pesar de la presencia de bloques dañados, debe hacer que la copia de seguridad omita los bloques dañados. Para eso, en **Opciones de copia de seguridad**, vaya a **Manejo de errores** y luego marque la casilla de verificación **Ignorar los sectores defectuosos**.

Condiciones de inicio

Esta configuración otorga más flexibilidad al programador y le permite llevar a cabo una tarea de copia de seguridad con respecto a ciertas condiciones. En el caso de varias condiciones, deben cumplirse todas simultáneamente para que se ejecute una copia de seguridad. Las condiciones de inicio no se aplican si se inicia un plan de copias de seguridad manualmente.

Para acceder a esta configuración, haga clic en **Mostrar más** cuando configure una planificación para un plan de protección.

En caso de que no se cumpla la condición (o alguna de ellas, si son varias), el comportamiento del programador estará definido por la opción de copia de seguridad Condiciones de inicio de la copia de seguridad. Para manejar la situación cuando no se cumplen con las condiciones por mucho tiempo y si el retraso de la copia de seguridad se vuelve peligroso, puede definir el intervalo en que la copia de seguridad se ejecutará independientemente de la condición.

En la siguiente tabla se muestran las condiciones de inicio disponibles para diversos datos en Windows, Linux y macOS.

DE QUÉ REALIZAR COPIAS DE SEGURIDAD	Discos/volúmenes o archivos (equipos físicos)	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	–	–	–	–	–
El servidor de la ubicación de copia de seguridad está disponible	Windows, Linux y macOS	Windows, Linux	Windows, Linux	Windows	Windows	Windows
Los usuarios cerraron la sesión	Windows	–	–	–	–	–

Se adapta al intervalo de tiempo	Windows, Linux y macOS	Windows, Linux	–	–	–	–
Ahorrar batería	Windows	–	–	–	–	–
No iniciar con conexiones de uso medido	Windows	–	–	–	–	–
No iniciar con conexiones a las siguientes redes Wi-Fi	Windows	–	–	–	–	–
Comprobar dirección IP del dispositivo	Windows	–	–	–	–	–

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 la copia de seguridad en el equipo todos los días a las 21:00, preferentemente 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 copia de seguridad de todos modos después de 2** hora(s).

Como resultado:

(1) Si el usuario queda inactivo antes de las 21:00, la copia de seguridad se inicia a las 21:00.

(2) Si el usuario queda inactivo entre las 21:00 y las 23:00, la copia de seguridad se inicia inmediatamente después de que este hecho ocurra.

(3) 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 el destino para almacenar las copias de seguridad está disponible a través de la red.

Esta condición es eficaz para carpetas de red, el almacenamiento en la nube y 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

Se realiza una copia de seguridad de los datos 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 trabajos de 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:

(1) Si son las 21:00 y el servidor está disponible, la copia de seguridad se iniciará inmediatamente.

(2) Si son las 21:00 pero el servidor no está disponible, la copia de seguridad se iniciará el siguiente día hábil si el servidor está disponible.

(3) Si es imposible que el servidor esté disponible en días hábiles a las 21:00, la copia de seguridad nunca se iniciará.

Los usuarios cerraron la sesión

Permite poner en espera una copia de seguridad hasta que todos los usuarios cierren la sesión en Windows.

Ejemplo

Ejecutar 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,

la copia de seguridad se ejecuta de todos modos.

- Programación: Semanalmente, 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** hora(s).

Como resultado:

(1) Si, para las 20:00, todos los usuarios cerraron la sesión, la copia de seguridad se iniciará a las 20:00.

(2) Si el último usuario cierra la sesión entre las 20:00 y las 23:00, la copia de seguridad se inicia inmediatamente después de que este hecho ocurra.

(3) Si algún usuario mantiene abierta la sesión a las 23:00, la copia de seguridad se inicia a las 23:00.

Se adapta al intervalo de tiempo

Restrinja la hora de inicio de la copia de seguridad a un intervalo concreto.

Ejemplo

Una empresa utiliza distintas ubicaciones en el mismo dispositivo de almacenamiento conectado a la red para realizar copias de seguridad de los servidores y los datos de los 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. Por lo tanto, es preferible que las copias de seguridad de los datos de los usuarios se realicen antes de esta hora, para liberar ancho de banda de la red. Se supone que 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, no se realizan copias de seguridad de los datos de los usuarios, es decir, se omitirá la ejecución de la copia de seguridad.

- 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:

(1) si el usuario cierra la sesión entre las 16:30 y las 22:00, la copia de seguridad comenzará de inmediato al cerrar la sesión.

(2) si el usuario cierra la sesión en cualquier otro momento, la copia de seguridad se omitirá.

Ahorrar batería

Evita una copia de seguridad es el dispositivo (un portátil o tableta) no está conectado a una fuente de alimentación. En función del valor de la opción de copia de seguridad Condiciones de inicio de la copia de seguridad, la copia de seguridad omitida se iniciará o no después de que el dispositivo se conecte a una fuente de alimentación. Las siguientes opciones están disponibles:

- **No iniciar con alimentación por batería**
  La copia de seguridad se iniciará únicamente si el dispositivo está conectado a una fuente de alimentación.
- **Iniciar con alimentación por batería si su nivel es superior a**
  La copia de seguridad se iniciará si el dispositivo está conectado a una fuente de alimentación o si el nivel de la batería es superior al valor especificado.

Ejemplo

La copia de seguridad de los datos se realiza cada día laborable a las 21:00. Si el dispositivo no está conectado a una fuente de alimentación (por ejemplo, el usuario está en una reunión que se alarga por la tarde), querrá omitir la copia de seguridad para ahorrar batería y esperar a que el usuario conecte el dispositivo 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:

(1) Si son las 21:00 y el dispositivo está conectado a una fuente de alimentación, la copia de seguridad se iniciará inmediatamente.

(2) Si son las 21:00 y el dispositivo está funcionando con batería, la copia de seguridad se iniciará en cuanto el dispositivo se conecte una fuente de alimentación.

No iniciar con conexiones de uso medido

Evita una copia de seguridad (incluida la copia de seguridad a un disco local) si el dispositivo 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.

Como medida adicional para evitar copias de seguridad en puntos de conexión móviles, cuando se habilita la condición **No iniciar con conexiones de uso medido**, la condición **No iniciar con conexiones a las siguientes redes Wi-Fi** se habilita automáticamente. Los siguientes nombres de red están especificados de forma predeterminada: "android", "phone", "mobile" y "modem". Puede eliminar estos nombres de la lista haciendo clic en el signo X.

Ejemplo

La copia de seguridad de los datos se realiza cada día laborable a las 21:00. Si el dispositivo está conectado a Internet mediante una conexión de uso medido (por ejemplo, el usuario está en un viaje de trabajo), querrá omitir la copia de seguridad para ahorrar el tráfico de red y esperar al inicio planificado en el siguiente día laborable.

- 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:

(1) Si son las 21:00 y el dispositivo no está conectado a Internet mediante una conexión de uso medido, la copia de seguridad se iniciará inmediatamente.

(2) 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 laborable.

(3) Si el dispositivo siempre está conectado a Internet mediante una conexión de uso medido a las 21:00 en días laborables, la copia de seguridad nunca se iniciará.

No iniciar con conexiones a las siguientes redes Wi-Fi

Evita 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. Puede especificar los nombres de red Wi-Fi, también conocidos como identificadores de conjunto de servicios (SSID).

La restricción se aplica todas las redes de contengan el nombre especificado como una subcadena en su nombre, sin distinción de mayúsculas y minúsculas. Por ejemplo, si especifica "teléfono" como nombre de red, la copia de seguridad no se iniciará cuando el dispositivo esté conectado a alguna de las siguientes redes: "Teléfono de Juan", "teléfono_wifi" o "mi_teléfono_wifi".

Esta condición es útil para evitar copias de seguridad cuando el dispositivo está conectado a Internet mediante un punto de conexión móvil.

Como medida adicional para evitar copias de seguridad en puntos de conexión móviles, la condición **No iniciar con conexiones a las siguientes redes Wi-Fi** se habilita automáticamente cuando se 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". Puede eliminar estos nombres de la lista haciendo clic en el signo X.

Ejemplo

La copia de seguridad de los datos se realiza cada día laborable a las 21:00. Si el dispositivo está conectado a Internet mediante un punto de conexión móvil (por ejemplo, un portátil conectado en modo de anclaje a red), querrá omitir la copia de seguridad y esperar al inicio planificado en el siguiente día laborable.

- Programación: Cada día, Ejecutar de lunes a viernes. Iniciar a las: 21:00.
- Condición: **No iniciar con conexiones a las siguientes redes Wi-Fi**, **Nombre de la red**: `<SSID of the hotspot network>`.
- Condiciones de inicio de la copia de seguridad: **Omita la copia de seguridad planificada**.

Como resultado:

(1) Si son las 21:00 y el equipo no está conectado a la red especificada, la copia de seguridad se iniciará inmediatamente.

(2) Si son las 21:00 y el equipo está conectado a la red especificada, la copia de seguridad se iniciará el siguiente día laborable.

(3) Si el equipo siempre está conectado a la red especificada a las 21:00 en días laborables, la copia de seguridad nunca se iniciará.

Comprobar dirección IP del dispositivo

Evita una copia de seguridad (incluida la copia de seguridad a un disco local) si cualquiera de las direcciones IP de los dispositivos quedan dentro o fuera del intervalo de direcciones IP especificado. 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.

Esta condición es útil en el caso de un usuario internacional para evitar cargos importantes por el consumo de datos. Asimismo, ayuda a evitar copias de seguridad con una conexión VPN.

Ejemplo

La copia de seguridad de los datos se realiza cada día laborable a las 21:00. Si el dispositivo está conectado a la red corporativa mediante un túnel de VPN (por ejemplo, si el usuario trabaja desde casa), querrá omitir la copia de seguridad y esperar hasta que el usuario lleve el dispositivo a la oficina.

- Programación: Cada día, Ejecutar de lunes a viernes. Iniciar a las: 21:00.
- Condición: **Comprobar dirección IP del dispositivo**, **Iniciar si queda fuera del intervalo IP**, **De**: `<beginning of the VPN IP address range>`, **A**: `<end of the VPN IP address range>`.
- Condiciones de inicio de la copia de seguridad: **Esperar hasta que se cumplan las condiciones**.

Como resultado:

(1) Si son las 21:00 y la dirección IP del equipo no está en el intervalo especificado, la copia de seguridad se iniciará inmediatamente.

(2) Si son las 21:00 y la dirección IP del equipo está en el intervalo especificado, la copia de seguridad se iniciará en cuanto el dispositivo obtenga una dirección IP no proveniente de VPN.

(3) Si la dirección IP del equipo siempre está dentro del intervalo especificado en días laborables a las 21:00, la copia de seguridad nunca se iniciará.

Reglas de retención

Importante
Algunas de las funciones descritas en esta sección solo están disponibles en implementaciones locales.

1. Haga clic en **Cuánto tiempo guardarlas**.
2. En **Limpieza**, elija una de las siguientes opciones:
   - **Por antigüedad de la copia de seguridad** (opción predeterminada)
     Especifique cuánto tiempo desea guardar las copias de seguridad que ha creado el plan de protección. De manera predeterminada, las reglas de retención se especifican para cada conjunto de copias de seguridad[1] por separado. Si desea usar una única regla para todas las copias de seguridad, haga clic en **Cambiar a una única regla para todos los conjuntos de copias de seguridad**.
   - **Por número de copias de seguridad**
     Especifique el número máximo de copias de seguridad que desea guardar.
   - **Por tamaño total de las copias de seguridad**
     Especifique el tamaño total máximo de copias de seguridad que desea guardar.
     Este ajuste no está disponible con el esquema de copia de seguridad **Siempre incremental (archivo único)** o al hacer copias de seguridad en un servidor SFTP o un dispositivo de cintas.
   - **Guardar las copias de seguridad indefinidamente**
3. Seleccione cuándo desea iniciar la limpieza:
   - **Después de la copia de seguridad** (opción predeterminada)
     Las reglas de retención se aplicarán después de haber creado una copia de seguridad nueva.
   - **Antes de la copia de seguridad**

[1] Es un grupo de copias de seguridad al que se le puede aplicar una regla de retención individual. Para el esquema personalizado de copia de seguridad, los conjuntos de copias de seguridad se corresponden con los métodos de copia de seguridad (completa, diferencial e incremental). En los demás casos, los conjuntos de copias de seguridad son mensual, diaria, semanal o cada hora. Una copia de seguridad mensual es la primera copia de seguridad creada una vez comenzado un mes. Una copia de seguridad semanal es la primera copia de seguridad que se crea el día de la semana seleccionado en la opción Copia de seguridad semanal (haga clic en el icono de engranaje y, a continuación, en Opciones de copia de seguridad > Copia de seguridad semanal). Si una copia de seguridad semanal es también la primera copia de seguridad que se crea en un nuevo mes, se considerará mensual. En ese caso, se creará una copia de seguridad semanal el día de la semana siguiente seleccionado. Una copia de seguridad diaria es la primera copia de seguridad que se crea en un día, excepto si puede considerarse mensual o semanal. Una copia de seguridad de cada hora es la primera copia de seguridad que se crea en una hora, excepto si puede considerarse mensual, semanal o diaria.

Las reglas de retención se aplicarán antes de haber creado una copia de seguridad nueva.

Este ajuste no está disponible cuando se hacen copias de seguridad de los clústeres de Microsoft SQL Server o Microsoft Exchange Server.

Qué más debe saber

- La última copia de seguridad creada por el plan de protección se mantiene en todos los casos, a no ser que configure una regla de retención para limpiar copias de seguridad antes de iniciar una nueva operación de copia de seguridad y establezca que el número de copias de seguridad que se deben mantener sea cero.

  Advertencia.
  Si elimina la única copia de seguridad que tiene aplicando las reglas de retención de esta forma, en el caso de que se produzca un error en la copia de seguridad, no dispondrá de ninguna con la que restaurar los datos, ya que no habrá ninguna copia de seguridad disponible para su uso.

- Las copias de seguridad almacenadas en cintas no se eliminan hasta que la cinta se sobreescriba.
- Si, de acuerdo con el esquema de copias de seguridad y el formato de copia de seguridad, cada copia de seguridad se almacena como un archivo independiente, este archivo no se podrá eliminar hasta que expire la vida útil de todas las copias de seguridad dependientes (incrementales y diferenciales). El almacenamiento de copias de seguridad cuya eliminación ha sido pospuesta, requiere espacio adicional. Además, la antigüedad, la cantidad o el tamaño de las copias de seguridad pueden superar los valores que especifique.

  Este comportamiento se puede cambiar utilizando la opción de copia de seguridad "Consolidación de copias de seguridad".
- Las reglas de retención forman parte del plan de protección. Dejan de funcionar en las copias de seguridad del equipo cuando se revoca o elimina el plan de protección de dicho equipo o se elimina el equipo del servidor de gestión. Si ya no necesita las copias de seguridad creadas por el plan, elimínelas tal y como se describe en "Eliminación de copias de seguridad".

Cifrado

Se recomienda que cifre todas las copias de seguridad que estén almacenadas en el almacenamiento en la cloud, sobre todo si su empresa está sujeta al cumplimiento de reglamentaciones.

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

Cifrado en un plan de protección

Para habilitar el cifrado, especifique los valores de cifrado al crear un plan de protección. Después de aplicar un plan de protección, los valores de cifrado ya no se pueden modificar. Para usar valores de cifrado diferentes, cree un nuevo plan de protección.

Pasos para especificar los valores de cifrado en un plan de protección

1. En el panel del plan de protección, habilite el conmutador **Cifrado**.
2. Especifique y confirme la contraseña de cifrado.
3. Seleccione uno de los siguientes algoritmos de cifrado:
   - **EEA 128**: las copias de seguridad se cifrarán por medio del algoritmo Estándar de encriptación avanzada (EEA) con una clave de 128 bits.
   - **EEA 192**: las copias de seguridad se cifrarán por medio del algoritmo EEA con una clave de 192 bits.
   - **EEA 256**: las copias de seguridad se cifrarán por medio del algoritmo EEA con una clave de 256 bits.
4. Haga clic en **Aceptar**.

Cifrado como propiedad del equipo

Esta opción está dirigida a administradores que manejan las copias de seguridad de varios equipos. Si necesita disponer de una contraseña de cifrado diferente para cada equipo o si tiene que aplicar el cifrado de copias de seguridad independientemente de la configuración de cifrado del plan de protección, guarde la configuración de cifrado en cada equipo de forma individual. Las copias de seguridad se cifrarán por medio del algoritmo EEA con una clave de 256 bits.

Guardar la configuración de cifrado en un equipo afecta los planes de protección de la siguiente manera:

- **Planes de protección que ya se han aplicado al equipo.** Si la configuración de cifrado de un plan de protección es diferente, las copias de seguridad fallarán.
- **Planes de protección que se aplicarán al equipo más adelante.** La configuración de cifrado guardados en un equipo reemplazarán los valores de cifrado en un plan de protección. Todas las copias de seguridad se cifrarán, incluso si el cifrado está deshabilitado en la configuración del plan de protección.

Esta opción puede usarse en un equipo que ejecute el Agente para VMware. Sin embargo, tenga cuidado si tiene más de un Agente para VMware conectado al mismo vCenter Server. Es obligatorio usar la misma configuración de cifrado para todos los agentes, porque así hay cierto equilibrio de carga entre ellos.

Una vez guardada la configuración de cifrado, se puede cambiar o restablecer tal como se describe a continuación.

Importante
Si un plan de protección que se ejecuta en este equipo ya ha creado copias de seguridad, al cambiar la configuración de cifrado, el plan no se ejecutará. Para seguir con la copia de seguridad, cree un nuevo plan.

Para guardar la configuración de cifrado en un equipo

1. Inicie sesión como administrador (en Windows) o como usuario raíz (en Linux).
2. Ejecute el siguiente script:
   - En Windows: `<installation_path>`**\PyShell\bin\acropsh.exe -m manage_creds --set-password** `<encryption_password>`

     En este caso, `<installation_path>` es la ruta de instalación del agente de protección. De manera predeterminada, la ruta es **%ProgramFiles%\BackupClient** para las implementaciones en la nube y **%ProgramFiles%\Acronis** para las implementaciones locales.
   - En Linux: **/usr/sbin/acropsh -m manage_creds --set-password** `<encryption_password>`

Para restablecer la configuración de cifrado en un equipo

1. Inicie sesión como administrador (en Windows) o como usuario raíz (en Linux).
2. Ejecute el siguiente script:
   - En Windows: `<installation_path>`**\PyShell\bin\acropsh.exe -m manage_creds --reset**

     En este caso, `<installation_path>` es la ruta de instalación del agente de protección. De manera predeterminada, la ruta es **%ProgramFiles%\BackupClient** para las implementaciones en la nube y **%ProgramFiles%\Acronis** para las implementaciones locales.
   - En Linux: **/usr/sbin/acropsh -m manage_creds --reset**

Para cambiar la configuración de cifrado mediante Cyber Protect Monitor

1. Inicie sesión como administrador en Windows o macOS.
2. Haga clic en el icono de **Cyber Protect Monitor** en el área de notificaciones (en Windows) o en la barra del menú (en macOS).
3. Haga clic en el icono de engranaje.
4. Haga clic en **Cifrado**.
5. Realice uno de los siguientes procedimientos:
   - Seleccione **Establecer una contraseña específica para este equipo**. Especifique y confirme la contraseña de cifrado.
   - Seleccione **Usar la configuración de cifrado especificada en el plan de protección**.
6. Haga clic en **Aceptar**.

Cómo funciona el cifrado

El algoritmo de cifrado EEA funciona en el modo Cipher-block chaining (CBC) y utiliza una clave generada de manera aleatoria con un tamaño definido por el usuario de 128, 192 o 256 bits. Cuanto mayor sea el tamaño de la clave, más tiempo tardará el programa en cifrar las copias de seguridad y más protegidos estarán los datos.

A continuación, la clave de cifrado se cifra con EEA-256, que usa un hash SHA-256 de la contraseña como clave. La contraseña no se guarda en ninguna parte del disco o de las copias de seguridad; el

hash de la contraseña se usa con fines de comprobación. Con esta seguridad en dos niveles, los datos de la copia de seguridad están protegidos contra accesos no autorizados, pero no es posible recuperar una contraseña perdida.

Notarización

La notarización permite demostrar que un archivo es auténtico y que no ha cambiado desde su copia de seguridad. Se recomienda habilitar la notarización cuando realice la copia de seguridad de documentos legales u otros archivos cuya autenticidad se desee demostrar.

La Notarización está disponible solo para copias de seguridad a nivel de archivo. Se omiten los archivos con firma digital, ya que no se requiere su notarización.

La notarización *no* está disponible:

- Si el formato de copia de seguridad está establecido en la **versión 11**
- Si el destino de la copia de seguridad es Secure Zone
- Si el destino de la copia de seguridad es una ubicación gestionada donde se ha habilitado la deduplicación o cifrado

Cómo utilizar la notarización

Para habilitar la certificación de todos los archivos seleccionados para su copia de seguridad (excepto los archivos con firma digital), active la opción **Notarización** cuando cree un plan de protección.

Al configurar la recuperación, los archivos notarizados se marcarán con un icono especial y podrá verificar la autenticidad del archivo.

Cómo funciona

Durante una copia de seguridad, el agente calcula los códigos de cifrado de los archivos de los que se ha realizado la copia de seguridad, crea un árbol de cifrado (en función de la estructura de carpetas), guarda el árbol en la copia de seguridad y envía la raíz del árbol de cifrado al servicio de notarización. El servicio de notarización guarda la raíz del árbol de cifrado en la base de datos de cadenas de bloques de Ethereum para garantizar que este valor no cambie.

Al verificar la autenticidad del archivo, el agente calcula su cifrado y lo compara con el almacenado en el árbol de cifrado de la copia de seguridad. Si los cifrados no coinciden, se considerará que el archivo no es auténtico. De lo contrario, la autenticidad del archivo queda garantizada por el árbol de cifrado.

Para verificar que el propio árbol de cifrado no se haya visto alterado, el agente envía la raíz del árbol de cifrado al servicio de notarización. El servicio de notarización lo compara con el almacenado en la base de datos de cadenas de bloques. Si los cifrados coinciden, se garantiza que el archivo seleccionado es auténtico. De lo contrario, el software muestra un mensaje para indicar que el archivo no es auténtico.

Conversión a equipo virtual

Importante
Algunas de las funciones descritas en esta sección solo están disponibles en implementaciones locales.

La conversión a un equipo virtual está disponible solo para copias de seguridad de nivel del disco. Si una copia de seguridad incluye el volumen del sistema y contiene toda la información necesaria para el inicio del sistema operativo, el equipo virtual resultante podrá iniciarse por su cuenta. De lo contrario, puede añadir sus discos virtuales a otro equipo virtual.

Métodos de conversión

- **Conversión periódica**
  Hay dos maneras de configurar una conversión periódica:
  - **Incluir la conversión en un plan de protección**
    La conversión se realizará después de cada copia de seguridad (si está configurada para la ubicación primaria) o después de cada replicación (si se configura para ubicaciones secundarias o ulteriores).
  - **Crear un plan de conversión independiente**
    Este método permite especificar una planificación de la conversión independiente.
- **Recuperación a una nueva máquina virtual**
  Este método permite elegir discos para la recuperación y configurar cada disco virtual. Utilice este método para realizar la conversión una vez u ocasionalmente (por ejemplo, para realizar una migración de físico a virtual).

Lo que necesita saber sobre conversión

Tipos de equipos virtuales admitidos

La conversión de una copia de seguridad a un equipo virtual la puede realizar el mismo agente que creó la copia de seguridad u otro.

Para realizar una conversión a VMware ESXi, Hyper-V o Scale Computing HC3, necesitará un servidor ESXi, Hyper-V o Scale Computing HC3 respectivamente y un agente de protección (Agente para VMware, Agente para Hyper-V o Agente para Scale Computing HC3) que gestione el servidor.

Al realizar una conversión a archivos VHDX, se asume que los archivos se conectarán como unidades de disco virtuales a un equipo virtual Hyper-V.

En la siguiente tabla aparecen los tipos de equipos virtuales que pueden crear los agentes:

Tipo de VM	Agente	Agente	Agente	Agente	Agente	Agent para

	para VMware	para Hyper-V	para Windows	para Linux	para Mac	Scale Computing HC3
VMware ESXi	+	–	–	–	–	–
Microsoft Hyper-V	–	+	–	–	–	–
VMware Workstation	+	+	+	+	–	–
Archivos VHDX	+	+	+	+	–	–
Scale Computing HC3	–	–	–	–	–	+

Limitaciones

- Ni el Agente para Windows, Agente para VMware (Windows) ni el Agente para Hyper-V pueden convertir copias de seguridad almacenadas en NFS.
- Las copias de seguridad almacenadas en un NFS o un servidor SFTP no se pueden convertir en un plan de conversión independiente.
- Las copias de seguridad almacenadas en Secure Zone únicamente pueden convertirse mediante el agente que se ejecute en el mismo equipo.
- Las copias de seguridad solo se pueden convertir a una máquina virtual de Scale Computing HC3 en un plan de conversión independiente.
- Las copias de seguridad que contienen volúmenes lógicos (LVM) de Linux se pueden convertir únicamente si las ha creado Agente para VMware, Agente para Hyper-V o Agente para Scale Computing HC3 y se dirigen al mismo hipervisor. No se admite la conversión entre hipervisores.
- Cuando las copias de seguridad de un equipo Windows se convierten en archivos VHDX o VMware Workstation, el equipo virtual resultante hereda el tipo de CPU del equipo que realiza la conversión. Como resultado, los controladores de la CPU correspondiente se instalan en el sistema operativo invitado. Si se inicia en un servidor cuyo tipo de CPU es diferente, aparece un error relacionado con el controlador en el sistema invitado. Actualice este controlador de forma manual.

Conversión periódica a ESXi y Hyper-V frente a ejecución de un equipo virtual desde una copia de seguridad

Ambas operaciones proporcionan un equipo virtual que puede iniciarse en cuestión de segundos si falla el equipo original.

La conversión periódica consume recursos de la CPU y memoria. Los archivos del equipo virtual ocupan espacio constantemente en el almacén de datos (almacenamiento). Esto podría no ser práctico si se utiliza un servidor de producción para la conversión. Sin embargo, el rendimiento del equipo virtual está limitado únicamente por los recursos del servidor.

En el segundo caso, solo se consumen recursos mientras el equipo virtual está en ejecución. El espacio del almacén de datos (almacenamiento) es necesario únicamente para mantener los cambios en las unidades de disco virtuales. Sin embargo, el equipo virtual podría ejecutarse con mayor lentitud debido a que el servidor no accede a los discos virtuales directamente, sino que se comunica con el agente que lee datos de la copia de seguridad. Además, el equipo virtual es temporal.

Conversión a un equipo virtual en un plan de protección

Puede configurar la conversión a un equipo virtual desde cualquier ubicación de copia de seguridad o replicación presente en un plan de protección. La conversión se llevará a cabo después de cada copia de seguridad o replicación.

Para obtener más información sobre los requisitos previos y las limitaciones, consulte "Lo que necesita saber sobre conversión".

Pasos para configurar una conversión a un equipo virtual en un plan de protección

1. Decida desde qué ubicación de copia de seguridad desea realizar la conversión.
2. En el panel del plan de protección, haga clic en **Conversión a VM** en esta ubicación.
3. Habilite el conmutador de **Conversión**.
4. En **Convertir a**, seleccione el tipo de equipo virtual de destino. Puede seleccionar una de las siguientes opciones:
   - **VMware ESXi**
   - **Microsoft Hyper-V**
   - **VMware Workstation**
   - **Archivos VHDX**
5. Realice uno de los siguientes procedimientos:
   - Para VMware ESXi y Hyper-V: haga clic en **Servidor**, seleccione el servidor de destino y, a continuación, especifique la nueva plantilla del nombre del equipo.
   - Para otros tipos de equipos virtuales: en **Ruta**, especifique el lugar en que guardar los archivos del equipo virtual y la plantilla de los nombres de los archivos.

   El nombre predeterminado es **[Machine Name]_converted**.
6. [Opcional] Haga clic en **Agente que realizará la conversión** y seleccione un agente.
   Este puede ser el agente que realiza la copia de seguridad (de forma predeterminada) o un agente instalado en otro equipo. Si opta por la segunda opción, las copias de seguridad deben almacenarse en una ubicación compartida, como una carpeta de red, para que el otro equipo tenga acceso a ellas.

7. [Opcional] Para VMware ESXi y Hyper-V, también puede hacer lo siguiente:
   - 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.
   - Cambie el modo de aprovisionamiento de disco. La configuración predeterminada es **Fina** para VMware ESXi y **Expansión dinámica** para Hyper-V.
   - 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.
8. Haga clic en **Realizado**.

Cómo funciona la conversión regular a equipos virtuales

La forma en la que funcionan las conversiones periódicas depende de dónde decide crear el equipo virtual.

- **Si escoge guardar el equipo virtual como un conjunto de archivos:** cada conversión recrea el equipo virtual desde cero.
- **Si escoge crear el equipo virtual en un servidor de virtualización:** al convertir una copia de seguridad incremental o diferencial, el software actualiza el equipo virtual en vez de recrearlo. Dicha conversión generalmente es más rápida. Ahorra tráfico de la red y recursos de la CPU del servidor que lleva a cabo la conversión. Si no es posible actualizar un equipo virtual, el software lo recreará desde cero.

A continuación encontrará una descripción detallada de ambos casos.

Si escoge guardar el equipo virtual como un conjunto de archivos

Como resultado de esta primero conversión, se creará una nueva equipo virtual. Todos las conversiones posteriores recrearán este equipo de cero. Primero, el equipo antiguo cambia de nombre temporalmente. A continuación, se crea un equipo virtual nuevo que tiene el nombre anterior del equipo antiguo. Si esta operación se realiza correctamente, se eliminará el equipo anterior. Si esta operación no se completa, el equipo nuevo se elimina y el equipo antiguo recupera su nombre anterior. De esta manera, la conversión siempre termina con un único equipo. Sin embargo, se necesita espacio de almacenamiento adicional durante la conversión para almacenar el equipo antiguo.

Si escoge crear el equipo virtual en un servidor de virtualización

La primero conversión crea un nuevo equipo virtual. Cualquier conversión subsiguiente funciona de la siguiente manera:

- Si existe una *copia de seguridad completa* desde la última conversión, el equipo virtual se recreará desde cero, como se describe en la sección anterior.
- De lo contrario, el equipo virtual existente se actualiza para reflejar los cambios desde la último conversión. Si no es posible realizar la actualización (por ejemplo, si eliminó las instantáneas intermedias, consulte a continuación), el equipo virtual se recreará desde cero.

Instantáneas intermedias

Para poder actualizar el equipo virtual, el software almacena algunas instantáneas intermedias del mismo. Se llaman **Copia de seguridad...** y **Réplica...** y deben mantenerse. Las instantáneas que no se necesiten se eliminarán automáticamente.

La última instantánea **Réplica...** corresponde a los resultados de la última conversión. Puede ir a esta instantánea si desea volver el equipo a ese estado; por ejemplo, si trabajó con el equipo y ahora desea eliminar los cambios que le realizó.

Otras instantáneas son para el uso interno del software.

Replicación

Importante
Algunas de las funciones descritas en esta sección solo están disponibles en implementaciones locales.

En esta sección se describe la réplica de copia de seguridad como una parte del plan de protección. Para obtener más información acerca de la creación de un plan de replicación independiente, consulte "Procesamiento de datos fuera del host".

Si habilita la réplica de copia de seguridad, cada una de las copias de seguridad se copiará en otra ubicación inmediatamente tras su creación. Si las copias de seguridad anteriores no se replicaron (por ejemplo, se perdió la conexión a la red), el software también replica todas las copias de seguridad que aparecieron desde la última replicación realizada correctamente.

Las copias de seguridad replicadas no dependen de las copias de seguridad que permanecen en la ubicación original y viceversa. Puede recuperar los datos desde cualquier copia de seguridad, sin acceso a otras ubicaciones.

Ejemplos de uso

- **Recuperación ante desastres fiable**
  Almacene sus copias de seguridad tanto en el lugar (para la recuperación inmediata) como fuera del lugar (para asegurar las copias de seguridad de un fallo de almacenamiento o un desastre natural).
- **Uso del almacenamiento en la cloud para proteger los datos de un desastre natural**
  Replique las copias de seguridad en el almacenamiento en la cloud transfiriendo solo los cambios realizados en los datos.
- **Mantenimiento de solo los últimos puntos de recuperación**
  Elimine las copias de seguridad anteriores para un almacenamiento rápido según las reglas de retención para no utilizar demasiado el espacio de almacenamiento caro.

Ubicaciones compatibles

Puede replicar una copia de seguridad *desde* cualquiera de las siguientes ubicaciones:

- Una carpeta local
- Una carpeta de red
- Secure Zone
- Un servidor SFTP
- Ubicaciones gestionadas por un nodo de almacenamiento

Puede replicar una copia de seguridad *en* cualquiera de las siguientes ubicaciones:

- Una carpeta local
- Una carpeta de red
- El almacenamiento en la cloud
- Un servidor SFTP
- Ubicaciones gestionadas por un nodo de almacenamiento
- Un dispositivo de cinta

Para permitir la replicación de copias de seguridad

1. En el panel del plan de protección, haga clic en **Añadir ubicación**.
   El control **Añadir ubicación** está disponible si la replicación es compatible *con* la última ubicación de copia de seguridad o de replicación seleccionada.
2. Especifique la ubicación en que se replicarán las copias de seguridad.
3. [Opcional] En **Cuánto tiempo guardarlas**, cambie las reglas de retención para la ubicación elegida, tal como se describe en "Reglas de retención".
4. [Opcional] En **Convertir a VM**, especifique los ajustes de conversión a un equipo virtual, tal como se describe en "Conversión a un equipo virtual".
5. [Opcional] Haga clic en el icono de engranaje > **Ventana de copia de seguridad y rendimiento** y establezca la ventana de copia de seguridad para la ubicación seleccionada, como se indica en "Ventana de copia de seguridad y rendimiento". Esta configuración definirá el rendimiento de la replicación.
6. [Opcional] Repita los pasos del 1 al 5 para todas las ubicaciones en que desee replicar las copias de seguridad. Se admiten hasta cinco ubicaciones consecutivas (incluyendo la principal).

Importante
Si habilita la copia de seguridad y la replicación en el mismo plan de protección, asegúrese de que la replicación se completa antes de la siguiente copia de seguridad programada. Si todavía se está realizando la replicación, no se iniciará la copia de seguridad programada. Por ejemplo, una copia de seguridad programada que se ejecuta cada 24 horas no se iniciará si la replicación tarda 26 horas en completarse.

Para evitar esta dependencia, use un plan independiente para la replicación de copia de seguridad. Para obtener más información sobre este plan específico, consulte "Replicación de copias de seguridad" (p. 405).

Consideraciones para usuarios con licencias de Advanced

Consejo

Puede configurar las copias de seguridad de replicación *desde* el almacenamiento en la nube creando un plan de replicación independiente. Para obtener más información, consulte "Procesamiento de datos fuera del host".

Restricciones

- No es posible replicar copias de seguridad *desde* una ubicación gestionada por medio de un nodo de almacenamiento en una carpeta local. Una carpeta local significa una carpeta en el equipo donde está el agente que creó la copia de seguridad.
- No es posible replicar copias de seguridad *en* una ubicación gestionada con la deduplicación activada para copias de seguridad que tengan el formato de copia de seguridad de la **versión 12**.

¿Qué equipo realiza la operación?

El agente que creó la copia de seguridad inicia la replica de una copia de seguridad *desde* cualquier ubicación; y lo hacen los siguientes elementos:

- El propio agente, si la ubicación *no* está gestionada por un nodo de almacenamiento.
- El nodo de almacenamiento correspondiente, si la ubicación está gestionada. No obstante, la réplica de una copia de seguridad desde la ubicación gestionada en el almacenamiento en la nube la realiza el agente que ha creado la copia de seguridad.

Como se deriva de la descripción anterior, la operación se realizará solo si el equipo con el agente está encendido.

Réplica de copias de seguridad entre ubicaciones gestionadas

El nodo de almacenamiento se encarga de replicar una copia de seguridad desde una ubicación gestionada a otra ubicación gestionada.

Si se ha habilitado la deduplicación para la ubicación de destino (probablemente en un nodo de almacenamiento diferente), el nodo de almacenamiento de origen envía solo los bloques de datos que no están presentes en la ubicación de destino. Es decir, igual que un agente, el nodo de almacenamiento realiza la deduplicación en el origen. Esto ahorra tráfico de red cuando replica los datos entre nodos de almacenamiento separados geográficamente.

Iniciar una copia de seguridad manualmente

1. Seleccione un equipo que tenga como mínimo un plan de protección aplicado.
2. Haga clic en **Copia de seguridad**.
3. Si se le aplica más de un plan de protección, seleccione el plan de protección.

4. Realice uno de los siguientes procedimientos:
   - Haga clic en **Ejecutar ahora**. Se creará una copia de seguridad incremental.
   - Si el esquema de copias de seguridad incluye varios métodos de copias de seguridad, puede escoger cuál usar. Haga clic en la flecha del botón **Ejecutar ahora** y, a continuación, seleccione **Completa, Incremental** o **Diferencial**.

La primera copia de seguridad creada por un plan de protección siempre es completa.

El progreso de la copia de seguridad se muestra en la columna **Estado** del equipo.

Opciones de copia de seguridad

Importante
Algunas de las funciones descritas en esta sección solo están disponibles en implementaciones locales.

Para modificar las opciones de copia de seguridad, haga clic en el icono del engranaje que se encuentra al lado del nombre del plan de protección y, a continuación, haga clic en **Opciones de copia de seguridad**.

Disponibilidad de las opciones de copia de seguridad

El conjunto de opciones de copia de seguridad disponible depende de:

- El entorno en el que opera el agente (Windows, Linux o macOS).
- El tipo de datos que se está incluyendo en la copia de seguridad (discos, archivos, equipos virtuales, datos de aplicación).
- El destino de la copia de seguridad (el almacenamiento en la cloud o la carpeta local o de red).

La siguiente tabla resume la disponibilidad de las opciones de copia de seguridad.

	Copia de seguridad a nivel de discos			**Copia de seguridad a nivel de archivos**			**Equipos virtuales**			**SQL y Exchange**
	Windows	**Linux**	**macOS**	**Windows**	**Linux**	**macOS**	**ESXi**	**Hyper-V**	**Scale Computing**	**Windows**
Alertas	+	+	+	+	+	+	+	+	+	+
Consolidación de la copia de seguridad	+	+	+	+	+	+	+	+	+	-
Nombre del	+	+	+	+	+	+	+	+	+	+

archivo de la copia de seguridad										
Formato de la copia de seguridad	+	+	+	+	+	+	+	+	+	+
Validación de la copia de seguridad	+	+	+	+	+	+	+	+	+	+
Seguimiento de bloques modificados (CBT)	+	-	-	-	-	-	+	+	+	+
Modo de copia de seguridad de clústeres	-	-	-	-	-	-	-	-	-	+
Tasa de compresión	+	+	+	+	+	+	+	+	+	+
Notificaciones por correo electrónico	+	+	+	+	+	+	+	+	+	+
Manejo de errores										
Reintentar si se produce un error	+	+	+	+	+	+	+	+	+	+
No mostrar mensajes ni diálogos durante el procesamiento (modo silencioso)	+	+	+	+	+	+	+	+	+	+
Ignorar los sectores defectuosos	+	-	+	+	-	+	+	+	+	-
Reintentar si se produce un	-	-	-	-	-	-	+	+	+	-

error durante la creación de instantáneas de VM										
Copias de seguridad incrementales/ diferenciales rápidas	+	+	+	-	-	-	-	-	-	-
Filtros de archivo	+	+	+	+	+	+	+	+	+	-
Instantánea de la copia de seguridad a nivel de archivo	-	-	-	+	+	+	-	-	-	-
Truncamiento de registros	-	-	-	-	-	-	+	+	-	Solo SQL
Toma de instantáneas de LVM	-	+	-	-	-	-	-	-	-	-
Puntos de montaje	-	-	-	+	-	-	-	-	-	-
Instantánea multivolumen	+	+	-	+	+	-	-	-	-	-
Ventana de copia de seguridad y rendimiento	+	+	+	+	+	+	+	+	+	+
Envío de datos físicos	+	+	+	+	+	+	+	+	+	-
Comandos previos/posteriores	+	+	+	+	+	+	+	+	+	+
Comandos previos o posteriores a la captura de	+	+	+	+	+	+	+	-	-	+

datos										
Instantáneas de hardware SAN	-	-	-	-	-	-	+	-	-	-
Planificación										
Distribuir las horas de inicio en una ventana de tiempo	+	+	+	+	+	+	+	+	+	+
Limitar el número de copias de seguridad ejecutadas a la vez	-	-	-	-	-	-	+	+	+	-
Copia de seguridad sector por sector	+	+	-	-	-	-	+	+	+	-
División	+	+	+	+	+	+	+	+	+	+
Gestión de cintas	+	+	+	+	+	+	+	+	+	+
Manejo de fallos de la tarea	+	+	+	+	+	+	+	+	+	+
Condiciones de inicio de la tarea	+	+	-	+	+	-	+	+	+	+
Servicio de instantáneas de volumen (VSS)	+	-	-	+	-	-	-	+	-	+
Volume Shadow Copy Service (VSS) para equipos virtuales	-	-	-	-	-	-	+	+	+	-

Copia de seguridad semanal	+	+	+	+	+	+	+	+	+	+
Registro de eventos de Windows	+	-	-	+	-	-	+	+	+	+

Alertas

No se realizan copias de seguridad correctamente durante un número especificado de días

El valor predeterminado es el siguiente: **Deshabilitado**.

Esta opción determina si se debe crear una alerta cuando el plan de protección no ha realizado una copia de seguridad correcta en un periodo de tiempo determinado. Además de las copias de seguridad fallidas, el software también hace un recuento de las copias de seguridad que no se han realizado según la planificación (copias de seguridad perdidas).

Las alertas se generan por equipo y se muestran en la pestaña **Alertas**.

Puede especificar el número de días consecutivos sin realizar copias de seguridad tras los que se generará la alerta.

Consolidación de la copia de seguridad

Esta opción define si se consolidarán las copias de seguridad durante la limpieza o si se eliminarán cadenas de copia de seguridad completas.

El valor predeterminado es el siguiente: **Deshabilitado**.

La consolidación es el proceso de combinar dos o más copias de seguridad subsiguientes en una sola.

Si esta opción está habilitada, una copia de seguridad que debería eliminarse durante la limpieza se consolida con la siguiente copia de seguridad dependiente (incremental o diferencial).

Si no, la copia de seguridad se retiene hasta que se puedan eliminar todas las dependientes. Esto ayuda a evitar una consolidación que requeriría mucho tiempo, pero necesita espacio extra para almacenar copias de seguridad cuya eliminación se ha postergado. El número de copias de seguridad o su antigüedad puede superar los valores indicados en las reglas de retención.

Importante
Tenga en cuenta que la consolidación es solo un método para eliminar y no una alternativa a la eliminación. La copia de seguridad resultante no tendrá los datos que estaban en la copia de seguridad eliminada y que no estaban en la copia de seguridad incremental o diferencial retenida.

Esta opción *no* es eficaz si sucede algo de lo que se indica a continuación:

- El destino de la copia de seguridad es un dispositivo de cintas o el almacenamiento en la nube.
- El esquema de copias de seguridad está configurado como **Siempre incremental (archivo único)**.
- El formato de copia de seguridad se configura en la **versión 12**.

Las copias de seguridad almacenadas en cintas no pueden consolidarse. Las copias de seguridad almacenadas en el almacenamiento en la cloud, con el formato tanto de la versión 11 como de la 12, y las copias de seguridad de archivo único, siempre se consolidan ya que la estructura interna permite realizar una consolidación rápida y sencilla.

Sin embargo, si se usa el formato de la versión 12 y hay varias cadenas de copias de seguridad (cada cadena almacenada en un archivo .tibx independiente), la consolidación solo funciona en la última cadena. El resto de cadenas se eliminan como un todo, excepto la primera, que se reduce al mínimo tamaño para conservar la metainformación (~12 KB). Esta metainformación es necesaria para garantizar la consistencia de los datos cuando se lleven a cabo operaciones de lectura y escritura simultáneas. Las copias de seguridad incluidas en estas cadenas desaparecen de la GUI en cuanto se aplica la regla de retención, aunque existan físicamente hasta que se elimine toda la cadena.

En el resto de los casos, las copias de seguridad cuya eliminación se posponga se marcan con el icono de la papelera () en el GUI. Si hace clic en el signo de X para eliminar una copia de seguridad, se llevará a cabo la consolidación. Las copias de seguridad almacenadas en una cinta desaparecen de la GUI únicamente cuando la cinta se sobrescriba o se borre.

Nombre del archivo de copia de seguridad.

Esta opción define los nombres de los archivos de copia de seguridad creados por el plan de protección.

Estos nombres se pueden ver en un administrador de archivos al buscar la ubicación de la copia de seguridad.

¿Qué es un archivo de copia de seguridad?

Cada plan de protección crea uno o varios archivos en la ubicación de la copia de seguridad, en función del esquema de copias de seguridad y del formato de copia de seguridad utilizados. La tabla que aparece a continuación incluye los archivos que se pueden crear por equipo o buzón de correo.

	Siempre incremental (archivo único)	**Otros esquemas de copia de seguridad**
Formato de copia de seguridad **versión 11**	Un archivo TIB y otro archivo de metadatos XML	Varios archivos TIB y un archivo de metadatos XML (formato tradicional)

Formato de copia de seguridad **versión 12**	Un archivo TIBX por cadena de copia de seguridad (una copia de seguridad completa o diferencial y todas las copias de seguridad incrementales que dependan de ella)

Todos los archivos tienen el mismo nombre, con o sin marca horaria o número de secuencia. Puede definir este nombre (denominado nombre de archivo de copia de seguridad) al crear o modificar un plan de protección.

Nota
La marca de fecha y hora se añade al nombre del archivo de copia de seguridad solo en el formato de copia de seguridad de la versión 11.

Después de cambiar el nombre de un archivo de copia de seguridad, la siguiente copia de seguridad será completa, a menos que especifique el nombre de archivo de una copia de seguridad que ya existe en el mismo equipo. Si es este el caso, se creará una copia de seguridad completa, incremental o diferencial de conformidad con la planificación del plan de protección.

Tenga en cuenta que es posible configurar nombres de archivos de copia de seguridad para ubicaciones que un administrador de archivos no puede buscar (por ejemplo, el almacenamiento en la nube o un dispositivo de cintas). Esto es así si desea ver los nombres personalizados en la pestaña **Almacenamiento de copias de seguridad**.

¿Dónde se ven los nombres del archivo de copia de seguridad?

Seleccione la pestaña **Almacenamiento de copias de seguridad** y, a continuación, el grupo de copias de seguridad.

- El nombre del archivo de copia de seguridad predeterminado aparece en el panel **Detalles**.
- Si configura un nombre de archivo de copia de seguridad no predeterminado, aparecerá directamente en la pestaña **Almacenamiento de copias de seguridad**, en la columna **Nombre**.

Limitaciones de los nombres de archivos de copia de seguridad

- Los nombres de archivo de copia de seguridad no pueden acabar en un dígito.
  Con el fin de impedir que el nombre termine con un dígito, se añade la letra "A" al nombre de copia de seguridad predeterminado. Al crear un nombre personalizado, asegúrese siempre de que no termine en un dígito. Al usar variables, el nombre no puede acabar con una variable, ya que la variable podría finalizar a su vez en un dígito.
- Un nombre de archivo de copia de seguridad no puede contener los símbolos siguientes: **()&?*$<>":\|/#**, finalizaciones de línea (**\n**) ni pestañas (**\t**).

Nombre de archivo de copia de seguridad predeterminado

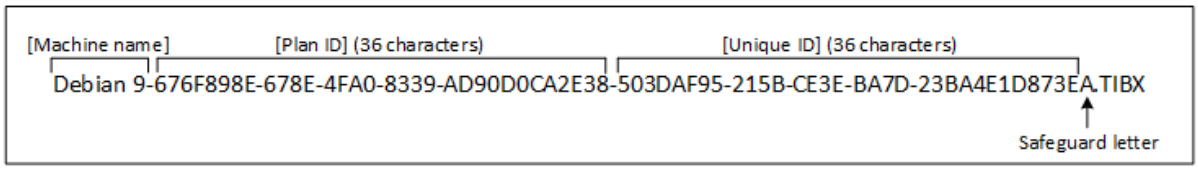
El nombre del archivo de copia de seguridad predeterminado es `[Machine Name]-[Plan ID]-[Unique ID]A`.

El nombre de archivo de copia de seguridad predeterminado de la copia de seguridad del buzón de correo es `[Mailbox ID]_mailbox_[Plan ID]A`.

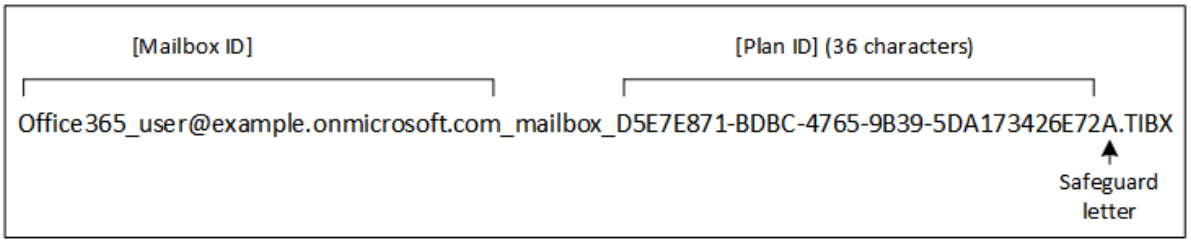
El nombre consta de las variables siguientes:

- `[Machine Name]` Esta variable se sustituye por el nombre del equipo (el mismo nombre que aparece en la consola web de Cyber Protect) para todos los tipos de datos incluidos en la copia de seguridad, salvo los buzones de correo de Microsoft 365. En el caso de los buzones de correo de Microsoft 365, se sustituye por el nombre principal del usuario del buzón de correo (UPN, por sus siglas en inglés).
- `[Plan ID]` Esta variable se sustituye por el identificador único de un plan de protección. Este valor no cambia en caso de que se modifique el nombre del plan.
- `[Unique ID]` Esta variable se sustituye por un identificador único del equipo o el buzón de correo electrónico seleccionado. Este valor no cambia si se modifica el nombre del equipo o si el UPN del buzón de correo varía.
- `[Mailbox ID]` Esta variable se sustituye por el UPN del buzón de correo.
- `"A"` es una letra de protección que se añade con el fin de impedir que el nombre acabe en un dígito.

El diagrama que aparece a continuación muestra el nombre del archivo de copia de seguridad predeterminado.



El diagrama que aparece a continuación muestra el nombre del archivo de copia de seguridad predeterminado para los buzones de correo electrónico.



Nombres sin variables

Si cambia el nombre del archivo de copia de seguridad a `MyBackup`, los archivos de copia de seguridad tendrán el aspecto que aparece a continuación. En ambos ejemplos se supone que hay copias de seguridad incrementales diarias programadas a las 14:40, desde el 13 de septiembre de 2016.

Para el formato de la versión 12 con el esquema de copias de seguridad **Siempre incremental (archivo único)**:

```
MyBackup.tibx
```

Para el formato de la versión 12 con otros esquemas de copias de seguridad:

```
MyBackup.tibx
MyBackup-0001.tibx
MyBackup-0002.tibx
...
```

Para el formato de la versión 11 con el esquema de copias de seguridad **Siempre incremental (archivo único)**:

```
MyBackup.xml
MyBackup.tib
```

Para el formato de la versión 11 con otros esquemas de copias de seguridad:

```
MyBackup.xml
MyBackup_2016_9_13_14_49_20_403F.tib
MyBackup_2016_9_14_14_43_00_221F.tib
MyBackup_2016_9_15_14_45_56_300F.tib
...
```

Uso de variables

Además de las variables que se utilizan de forma predeterminada, puede usar la variable `[Plan name]`, que se sustituye por el nombre del plan de protección.

Si se seleccionan varios equipos o buzones de correo electrónico para la copia de seguridad, el nombre del archivo de copia de seguridad tiene que contener las variables `[Machine Name]`, `[Mailbox ID]` o `[Unique ID]`.

Nombre del archivo de la copia de seguridad frente a nomenclatura de archivo simplificada

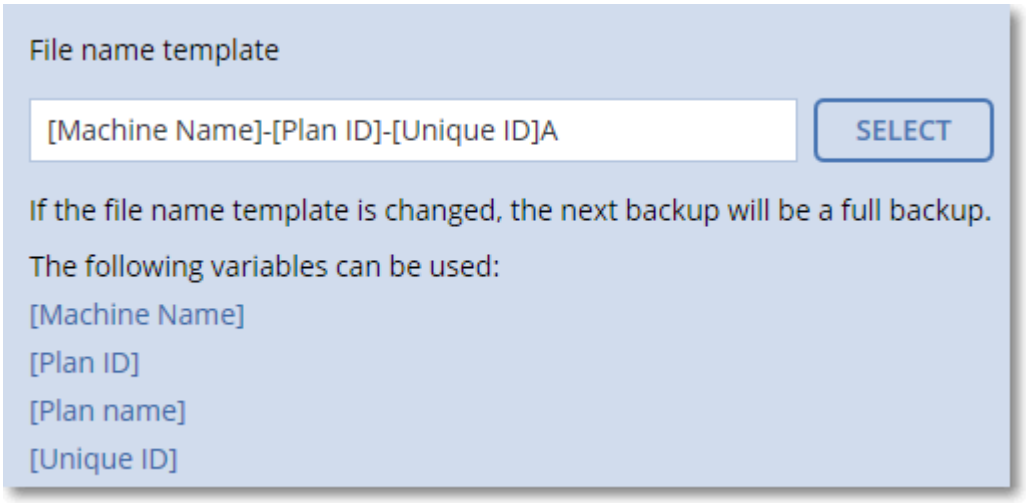
Si utiliza texto o variables, puede construir los mismos nombres de archivo de las versiones anteriores de Acronis Cyber Protect. No obstante, los nombres de archivo simplificados no se pueden reconstruir; en la versión 12, un nombre de archivo tendrá una marca de fecha y hora a menos que se utilice el formato de archivo único.

Ejemplos de uso

- **Ver nombres de archivo sencillos**
  Desea distinguir fácilmente copias de seguridad al buscar su ubicación con un administrador de archivos.
- **Continuar una secuencia existente de copias de seguridad**

Supongamos que se aplica un plan de protección a un solo equipo y tiene que eliminar este equipo de la consola web de Cyber Protect o desinstalar el agente junto con sus ajustes de configuración. Cuando se vuelva a añadir el equipo o cuando el agente se vuelva a instalar, podrá forzar el plan de protección para que continúe realizando la misma copia de seguridad o la secuencia de copias de seguridad. Para hacerlo, en las opciones de copia de seguridad del plan de protección, haga clic en **Nombre del archivo de la copia de seguridad** y, a continuación, en **Seleccionar** para elegir la copia de seguridad.

El botón **Examinar** muestra las copias de seguridad de la ubicación seleccionada en la sección **Dónde realizar copias de seguridad** del panel del plan de protección. No es posible buscar nada fuera de esta ubicación.



- **Actualizar desde las versiones de productos anteriores**

  Si un plan de protección no se migra de forma automática durante la actualización, vuelva a crear el plan y especifique el archivo de copia de seguridad antiguo. Si solo se ha seleccionado un equipo para la copia de seguridad, haga clic en **Examinar** y, a continuación, seleccione la copia de seguridad pertinente. Si se han seleccionado varios equipos para la copia de seguridad, vuelva a crear el nombre del archivo de copia de seguridad antiguo utilizando las variables.

Nota
El botón **Seleccionar** solo está disponible para aquellos planes de protección que se hayan creado para un único dispositivo y se hayan aplicado tan solo en ese.

Formato de la copia de seguridad

Esta opción define el formato de las copias de seguridad creadas por el plan de protección. Solo está disponible en los planes de protección que utilizan el formato de copia de seguridad heredado versión 11. En este caso, puede cambiarlo al nuevo formato versión 12. Después de cambiarlo, la opción deja de ser accesible.

Esta opción *no* es eficaz para las copias de seguridad de buzones de correo. Las copias de seguridad de buzones de correo siempre utilizan el formato nuevo.

El valor predeterminado es el siguiente: **Selección automática**.

Puede seleccionar una de las siguientes opciones:

- **Selección automática**

  Se usará la versión 12, salvo que el plan de protección anexe copias de seguridad a las que se crearon con versiones del producto anteriores.
- **Versión 12**

  Un nuevo formato recomendado en la mayoría de los casos para realizar copias de seguridad y recuperaciones de forma más rápida. Cada cadena de copias de seguridad (una copia de seguridad completa o diferencial y todas las copias de seguridad incrementales que dependen de ella) se guardan en un solo archivo TIBX.

  Con este formato, la regla de retención **Por tamaño total de las copias de seguridad** no tiene efecto.
- **Versión 11**

  Un formato heredado que se conserva para permitir la compatibilidad con versiones anteriores. Permite anexar copias de seguridad a las que se crearon con versiones del producto anteriores.

  Utilice este formato también (con cualquier esquema de copias de seguridad salvo para **Siempre incremental [archivo único]**) si desea disponer de copias de seguridad completas, incrementales y diferenciales como archivos independientes.

  Este formato se selecciona automáticamente si el destino de copias de seguridad (o destino de replicación) es una ubicación gestionada con la deduplicación habilitada o una ubicación gestionada con el cifrado habilitado. Si cambia el formato a la **versión 12**, no será posible realizar las copias de seguridad.

Nota

No es posible realizar la copia de seguridad de Grupos de disponibilidad de bases de datos (DAG) con la versión 11 del formato de la copia de seguridad. La copia de seguridad de DAG solo es posible en el formato de la versión 12.

Formato y archivos de copia de seguridad

En el caso de las ubicaciones de copia de seguridad que se puedan buscar con un administrador de archivos (como carpetas locales o de red), el formato de copia de seguridad determinará el número de archivos y su extensión. Puede definir los nombres de archivos utilizando la opción copia de seguridad del nombre de archivo. La tabla que aparece a continuación incluye los archivos que se pueden crear por equipo o buzón de correo.

	Siempre incremental (archivo único)	**Otros esquemas de copia de seguridad**
Formato de copia de seguridad **versión 11**	Un archivo TIB y otro archivo de metadatos XML	Varios archivos TIB y un archivo de metadatos XML (formato tradicional)
Formato de copia de seguridad	Un archivo TIBX por cadena de copia de seguridad (una copia de seguridad completa o diferencial y todas las copias de seguridad incrementales que	

versión 12	dependan de ella)

Cambiar el formato de copia de seguridad a la versión 12 (TIBX)

Si cambia el formato de copia de seguridad de la versión 11 (formato TIB) a la 12 (formato TIBX):

- La siguiente copia de seguridad será completa.
- En el caso de las ubicaciones de copia de seguridad que se puedan buscar con un administrador de archivos (como carpetas locales o de red), se creará un nuevo archivo TIBX. El nuevo archivo llevará el nombre del archivo original con el sufijo **_v12A**.
- Solo se aplicarán reglas de retención y replicación a las copias de seguridad nuevas.
- Las copias de seguridad antiguas no se eliminarán y seguirán estando disponibles en la pestaña **Almacenamiento de copias de seguridad**. Se pueden eliminar manualmente.
- Las copias de seguridad en el cloud antiguas no consumirán la cuota de **almacenamiento en el cloud**.
- Las copias de seguridad locales antiguas consumirán la cuota de **copia de seguridad local** hasta que las elimine manualmente.
- Si el destino de su copia de seguridad (o destino de replicación) es una ubicación gestionada con la deduplicación habilitada, no será posible realizar las copias de seguridad.

Deduplicación en archivos comprimidos

El formato de la versión 12 es compatible con la deduplicación en archivos comprimidos.

La deduplicación en archivos comprimidos utiliza la deduplicación por parte del cliente y ofrece estas ventajas:

- Tamaño de copia de seguridad reducido de forma importante, con deduplicación integrada a nivel de bloque para cualquier tipo de dato
- La gestión eficiente de enlaces fijos garantiza que no haya almacenamientos duplicados.
- Fragmentación basada en hashes

Nota
La deduplicación en archivos comprimidos está habilitada de forma predeterminada para todas las copias de seguridad en formato TIBX. No es necesario habilitarla en las opciones de copia de seguridad y no se puede deshabilitar.

Validación de la copia de seguridad

La validación es una operación que verifica la posibilidad de recuperación de datos en una copia de seguridad. Cuando esta opción está habilitada, cada copia de seguridad que crea el plan de protección se valida justo después de su creación. Esta operación la realiza el agente de protección.

El valor predeterminado es el siguiente: **Deshabilitado**.

La validación calcula una suma de comprobación por cada bloque de datos que se puede recuperar desde la copia de seguridad. La única excepción es la validación de las copias de seguridad a nivel de archivo que se encuentran en el almacenamiento en la nube. Estas copias de seguridad se validan comprobando la coherencia de los metadatos guardados en la copia de seguridad.

La validación lleva bastante tiempo, incluso cuando se trata de copias de seguridad incrementales o diferenciales, que son de pequeño tamaño. Esto se debe a que la operación valida no solo los datos contenidos físicamente en la copia de seguridad, sino también todos los datos recuperables al seleccionar la copia de seguridad. Esto exige acceso a las copias de seguridad creadas anteriormente.

Si bien la validación correcta significa una gran probabilidad de tener una recuperación exitosa, no verifica todos los factores que tienen influencia sobre el proceso de recuperación. Si realiza una copia de seguridad del sistema operativo, le recomendamos que realice una recuperación de prueba con el dispositivo de arranque en un disco duro libre o que ejecute un equipo virtual desde la copia de seguridad en el entorno de ESXi o Hyper-V.

Seguimiento de bloques modificados (CBT)

Esta opción sirve para las copias de seguridad a nivel de disco de equipos virtuales y de equipos físicos que ejecutan Windows. También sirve para realizar copias de seguridad de bases de datos de Microsoft SQL Server y Microsoft Exchange Server.

El valor predeterminado es el siguiente: **Habilitado**.

Esta opción determina si se usa el Seguimiento de bloques modificados (CBT) cuando se realiza una copia de seguridad incremental o diferencial.

La tecnología CBT acelera el proceso de copia de seguridad. Los cambios realizados en el disco o contenido de la base de datos se rastrean continuamente en el nivel del bloque. Cuando se inicia una copia de seguridad, los cambios se pueden guardar inmediatamente en esta.

Modo de copia de seguridad de clústeres

Estas opciones son eficaces para las copias de seguridad de nivel de la base de datos de Microsoft SQL Server y Microsoft Exchange Server.

Estas opciones son eficaces solo si se selecciona el propio clúster (Grupos de disponibilidad de Always On de Microsoft SQL Server [AAG] o el grupo de disponibilidad de base de datos de Microsoft Exchange Server [DAG]) para la copia de seguridad, en lugar de los nodos concretos o las bases de datos que tiene. Si selecciona elementos concretos del clúster, la copia de seguridad no será compatible con el clúster y solo se incluirán en la copia de seguridad las copias seleccionadas de los elementos.

Microsoft SQL Server

Esta opción determina el modo de copia de seguridad para los grupos de disponibilidad de Always On (AAG) de SQL Server. Para que se realice la operación, Agent for SQL debe estar instalado en

todos los nodos de los AAG. Para obtener más información acerca de cómo realizar la copia de seguridad de los grupo de disponibilidad de AlwaysOn, consulte "Protección de los grupos de disponibilidad AlwaysOn (AAG)".

El valor predeterminado es el siguiente: **Si es posible, realice una réplica secundaria**.

Puede escoger una de las siguientes acciones:

- **Si es posible, realice una réplica secundaria**
  Si todas las réplicas secundarias están fuera de línea, se realizará una copia de seguridad de la principal. Realizar una copia de seguridad de la réplica principal podría ralentizar el funcionamiento de SQL Server, pero los datos se incluirán en la copia de seguridad con su estado más reciente.
- **Réplica secundaria**
  Si todas las réplicas secundarias están fuera de línea, no se podrá realizar la copia de seguridad. Realizar la copia de seguridad de las réplicas secundarias no afecta al rendimiento de SQL server y le permite ampliar la ventana de copia de seguridad. No obstante, las réplicas pasivas podrían contener información que no está actualizada, ya que dichas réplicas frecuentemente se configuran para actualizarse asíncronamente (retrasado).
- **Réplica principal**
  Si la réplica principal está fuera de línea, no será posible realizar la copia de seguridad. Realizar una copia de seguridad de la réplica principal podría ralentizar el funcionamiento de SQL Server, pero los datos se incluirán en la copia de seguridad con su estado más reciente.

Independientemente del valor de esta opción, para garantizar la consistencia de la base de datos, el software omite las bases de datos que *no* tienen los estados **SINCRONIZADA** o **SINCRONIZANDO** cuando se inicia la copia de seguridad. Si se omiten todas las bases de datos, no se podrá realizar la copia de seguridad.

Microsoft Exchange Server

Esta opción determina el modo de copia de seguridad para los grupos de disponibilidad de base de datos de Exchange Server (DAG). Para que se realice la operación, Agent for Exchange debe estar instalado en todos los nodos del DAG. Para obtener más información acerca de cómo realizar la copia de seguridad de grupos de disponibilidad de base de datos, consulte "Protección de grupos de disponibilidad de base de datos (DAG)".

El valor predeterminado es el siguiente: **La copia pasiva, a ser posible.**

Puede escoger una de las siguientes acciones:

- **La copia pasiva, a ser posible.**
  Si todas las copias pasivas están fuera de línea, se realiza una copia de seguridad de la copia activa. Si realiza la copia de seguridad de la copia activa podría ralentizar el funcionamiento de Exchange Server, pero los datos se incluirían en la copia de seguridad en su estado más reciente.
- **Copia pasiva**

Si todas las copias pasivas están fuera de línea, la copia de seguridad no se realizará correctamente. Realizar copias de seguridad de las copias pasivas no afecta el rendimiento de Exchange Server y le permite extender la ventana de copia de seguridad. Sin embargo, las copias pasivas pueden contener información que no este actualizada, porque dichas copias normalmente se configuran para actualizarse de forma asincrónica (retardada).

- **Copia activa**
  Si la copia activa está fuera de línea, la copia de seguridad no se realizará correctamente. Si realiza la copia de seguridad de la copia activa podría ralentizar el funcionamiento de Exchange Server, pero los datos se incluirían en la copia de seguridad en su estado más reciente.

Independientemente del valor de esta opción, para garantizar la consistencia de la base de datos, el software omite las bases de datos que *no* tienen los estados **BUENO** o **ACTIVO** cuando se inicia la copia de seguridad. Si se omiten todas las bases de datos, no se podrá realizar la copia de seguridad.

Tasa de compresión

Esta opción define el tasa de compresión que se aplicará a los datos que se incluyen en la copia de seguridad. Los niveles disponibles son: **Ninguno**, **Normal**, **Alto**, **Máximo**.

El valor predeterminado es el siguiente: **Normal**.

Un tasa de compresión mayor implica que el proceso de copia de seguridad requiere más tiempo, pero la copia de seguridad resultante ocupa menos espacio. Actualmente los niveles Alto y Máximo funcionan de forma similar.

El tasa de compresión de datos óptimo dependerá del tipo de datos que se incluyen en la copia de seguridad. Por ejemplo, ni siquiera la máxima compresión conseguirá reducir significativamente el tamaño de la copia de seguridad si esta contiene archivos esencialmente comprimidos, como .jpg, .pdf o .mp3. Sin embargo, los formatos como .doc o .xls se comprimirán correctamente.

Notificaciones por correo electrónico

Esta opción permite configurar notificaciones por correo electrónico sobre eventos que suceden durante la copia de seguridad.

Esta opción solo está disponible en implementaciones locales. En el caso de las implementaciones en la cloud, los ajustes se configuran en cada cuenta cuando se crea una cuenta.

El valor predeterminado es el siguiente: **Usar la configuración de fuentes predeterminada.**

Puede utilizar la configuración del sistema o anularla mediante los valores personalizados que se especificarán únicamente para este plan. La configuración del sistema se configura como se describe en la sección "Notificaciones por correo electrónico".

Importante
Los cambios en la configuración del sistema afectan a todos los planes de protección que la utilizan.

Antes de habilitar esta opción, asegúrese de que se han configurado los ajustes del **Servidor de correo electrónico**.

Pasos para personalizar las notificaciones por correo electrónico en un plan de protección

1. Seleccione **Personalizar los ajustes de este plan de protección**.
2. En el campo **Direcciones de correo electrónico de los destinatarios**, escriba la dirección de correo electrónico de destino. Puede introducir varias direcciones separadas por punto y coma.
3. [Opcional] En **Asunto**, cambie el asunto de la notificación por correo electrónico.

   Puede utilizar las variables siguientes:

   - `[Alert]` - resumen de alerta.
   - `[Device]` - nombre del dispositivo.
   - `[Plan]` - el nombre del plan que ha generado la alerta.
   - `[ManagementServer]` - el nombre del servidor del equipo en el que está instalado el servidor de gestión.
   - `[Unit]` - el nombre de la unidad al que pertenece el equipo.

   El asunto predeterminado es `[Alert]` **Dispositivo:** `[Device]` **Plan:** `[Plan]`
4. Seleccione las casillas de verificación de los eventos sobre los que desea recibir notificaciones. Puede hacerlo mediante la lista de todas las alertas que suceden durante una copia de seguridad, agrupadas en función de la gravedad.

Manejo de errores

Estas opciones le permiten que establezca como se manejarán los errores que puedan suceder durante la copia de seguridad.

Reintentar si se produce un error

El valor predeterminado es el siguiente: **Habilitado. Número de intentos: 30. Intervalo entre intentos: 30 segundos**.

Cuando se produce un error recuperable, 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.

Por ejemplo, si no se tiene acceso o no está disponible el destino de la copia de seguridad en la red, el programa intentará llegar al destino cada 30 segundos, pero solo 30 veces. Se detendrán los intentos tan pronto como se reanude la operación O se realice el número de intentos especificados, lo que suceda primero.

Almacenamiento en la cloud

Si se selecciona el almacenamiento en la cloud como destino de la copia de seguridad, el valor de la opción se establece automáticamente en **Habilitado**. **Número de intentos: 300**. **Intervalo entre**

intentos: 30 segundos.

En este caso, el número de intentos real es ilimitado, pero el tiempo de espera anterior al fallo de la copia de seguridad se calcula de la siguiente manera: (300 segundos + **intervalo entre intentos**) * (**número de intentos** + 1).

Ejemplos:

- Con los valores predeterminados, la copia de seguridad fallará después de (300 segundos + 30 segundos) * (300 + 1) = 99 330 segundos o ~27,6 horas.
- Si establece el **número de intentos** en 1 y el **intervalo entre intentos** en 1 segundo, la copia de seguridad fallará después de (300 segundos + 1 segundo) * (1 + 1) = 602 segundos o 10 minutos.

Si el tiempo de espera calculado es superior a 30 minutos y la transferencia de datos no ha empezado todavía, el tiempo de espera real se establece en 30 minutos.

No mostrar mensajes ni diálogos durante el procesamiento (modo silencioso)

El valor predeterminado es el siguiente: **Habilitado**.

Cuando se habilite el modo silencioso, el programa manejará automáticamente las situaciones que requieran interacción del usuario (a excepción del manejo de sectores defectuosos que se definen con otra opción). Si una operación no puede continuar sin la acción del usuario, ésta fallará. Los detalles de la operación, incluyendo los errores, si los hubiera, pueden encontrarse en el registro de la operación.

Ignorar los sectores defectuosos

El valor predeterminado es el siguiente: **Deshabilitado**.

Cuando esta opción está deshabilitada, cada vez que el programa encuentre un sector defectuoso, se asignará a la actividad de copia de seguridad el estado **Interacción necesaria**. Para realizar una copia de seguridad de información válida en un disco que se está dañando rápidamente, habilite ignorar sectores defectuosos Se realizará una copia de seguridad del resto de los datos y podrá montar la copia de seguridad del disco resultante y extraer los archivos válidos a otro disco.

Reintentar si se produce un error durante la creación de instantáneas de VM

El valor predeterminado es el siguiente: **Habilitado. Número de intentos: 3. Intervalo entre intentos: 5 minutos.**

Cuando se produce un fallo al tomar una instantánea de un equipo virtual, el programa reintenta la operación fallida. Puede establecer el intervalo temporal y el número de intentos. Se detendrán los intentos tan pronto como la operación se lleve a cabo correctamente o se realice el número de intentos especificados, lo que suceda primero.

Copias de seguridad incrementales/diferenciales rápidas

Esta opción es eficaz para las copias de seguridad incrementales y diferenciales a nivel de disco.

Esta opción no es efectiva (siempre está deshabilitada) para volúmenes formateados con los sistemas de archivos JFS, ReiserFS3, ReiserFS4, ReFS o XFS.

El valor predeterminado es el siguiente: **Habilitado**.

La copia de seguridad incremental o diferencial sólo captura los cambios en los datos. Para acelerar el proceso de copia de seguridad, el programa determina si un archivo ha cambiado por su tamaño y la fecha/hora en la que se guardó por última vez. Si deshabilita esta característica, el programa compara el contenido completo del archivo con el que esté almacenado en la copia de seguridad.

Filtros de archivo

Utilizando filtros de archivo, puede incluir o excluir solo ciertos archivos y carpetas específicos en una copia de seguridad.

Los filtros de archivo están disponibles para copias de seguridad tanto a nivel de discos como a nivel de archivos, a no ser que se indique lo contrario.

Los filtros de archivo no son efectivos cuando se aplican a discos dinámicos (volúmenes LVM o LDM) de una máquina virtual con una copia de seguridad realizada por Agente para VMware, Agente para Hyper-V o Agente para Scale Computing en el modo sin agente.

Para habilitar los filtros de archivo:

1. En un plan de protección, expanda el módulo **Copia de seguridad**.
2. En **Opciones de copia de seguridad**, haga clic en **Cambiar**.
3. Seleccione **Filtros de archivo**.
4. Use cualquiera de las opciones que se especifican a continuación.

Excluya los archivos que cumplan criterios específicos

Hay dos opciones que funcionan de manera inversa.

- **Realice copias de seguridad solo de los archivos que coincidan con los siguientes criterios.**
  Ejemplo: si selecciona realizar una copia de seguridad de todo el equipo y especifica **C:\File.exe** en los criterios de filtro, solamente se hará la copia de seguridad de ese archivo.

  Nota
  Este filtro no funciona con copias de seguridad a nivel de archivo si se selecciona **Versión 11** en **Formato de copia de seguridad** y el destino de la copia de seguridad NO es un almacenamiento en la nube.

- **No realice copias de seguridad de los archivos que coincidan con los siguientes criterios.**

Ejemplo: si selecciona realizar una copia de seguridad de todo el equipo y especifica **C:\File.exe** en los criterios de filtro, solamente se omitirá ese archivo.

Es posible usar las dos opciones simultáneamente. La segunda opción anula la primera. Por ejemplo, si especifica **C:\File.exe** en los dos campos, este archivo se omitirá durante el proceso de copia de seguridad.

Criterios

- **Ruta completa**

  Especifique la ruta completa hasta el archivo o carpeta, empezando por la letra de unidad de disco (al realizar copias de seguridad en Windows) o del directorio raíz (al hacer copias de seguridad en Linux o macOS).

  Puede usar una barra diagonal en la ruta de archivo o carpeta (como en **C:/Temp/File.tmp**) tanto en Windows como en Linux/macOS. En Windows, también puede usar la tradicional barra inversa (como en **C:\Temp\File.tmp**).

  Importante

  Si el sistema operativo del equipo con copia de seguridad no se detecta durante una copia de seguridad a nivel de disco, los filtros de archivo de directorio completo no funcionarán. Para un filtro de exclusión, aparecerá una advertencia. Si hay un filtro de inclusión, la copia de seguridad no se realizará correctamente.

  El filtro de ruta completa incluye la letra de unidad (en Windows) o el directorio raíz (en Linux o macOS). Un ejemplo de ruta completa de un archivo sería **C:\Temp\File.tmp**. Un filtro que incluya la letra de unidad o el directorio raíz, por ejemplo **C:\Temp\File.tmp** o **C:\Temp***, generará una advertencia o un error.

  Un filtro que no emplee la letra de unidad ni el directorio raíz (por ejemplo, **Temp*** o **Temp\File.tmp**) o que empiece con un asterisco (por ejemplo, ***C:**) no generará una advertencia o un error. Sin embargo, si el sistema operativo del equipo con copia de seguridad no se detecta correctamente, estos filtros tampoco funcionarán.

- **Nombre**

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

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

Puede utilizar uno o varios caracteres comodín (*, **, y ?) en el criterio. Estos caracteres se pueden utilizar dentro de la ruta completa y en el nombre del archivo o carpeta.

El asterisco (*) sustituye a cero o más caracteres en el nombre del archivo. Por ejemplo, el criterio **Doc*.txt** coincide con archivos como **Doc.txt** y **Document.txt**.

[Solo para copias de seguridad en el formato de la **versión 12**] El asterisco doble (**) sustituye a cero o más caracteres en el nombre del archivo y la ruta, incluido el carácter de la barra diagonal o inversa. Por ejemplo, el criterio ****/Docs/**.txt**coincide con todos los archivos txt en todas las subcarpetas de todas las carpetas **Docs**.

El signo de pregunta (?) sustituye exactamente un carácter en el nombre del archivo. Por ejemplo, el criterio **Doc?.txt** coincide con archivos como **Doc1.txt** y **Docs.txt**, pero no con los archivos **Doc.txt** o **Doc11.txt**.

Excluir archivos y carpetas ocultos

Seleccione esta casilla de verificación para omitir los archivos y carpetas que tengan el atributo **Oculto** (para los sistemas de archivos compatibles con Windows) o que empiecen con un punto (.) (para los sistemas de archivos en Linux, como Ext2 y Ext3). Si una carpeta está oculta, se excluirán todos sus contenidos (incluso los archivos que no se encuentren ocultos).

Excluir archivos y carpetas del sistema

Esta opción está vigente solo para sistemas de archivos compatibles con Windows. Seleccione esta casilla de verificación para omitir archivos y carpetas con el atributo **Sistema**. Si una carpeta tiene el atributo **Sistema**, se excluirán todos sus contenidos (incluso los archivos que no tengan el atributo **Sistema**).

Nota
Puede ver los atributos del archivo o carpeta en las propiedades del archivo/carpeta utilizando el comando atrib. Para obtener más información, consulte el Centro de Soporte Técnico y Ayuda de Windows.

Instantánea de la copia de seguridad a nivel de archivo

Esta opción solo sirve para la copia de seguridad a nivel de archivo.

Esta opción define si se hace una copia de seguridad archivo por archivo o si se toma una instantánea de los datos.

Nota
A los archivos que no estén almacenados en redes compartidas se le realizará la copia de seguridad uno a uno.

El valor predeterminado es el siguiente:

- Si se han seleccionado únicamente equipos que se ejecutan en Linux para realizar la copia de seguridad: **No se crea una instantánea.**
- De lo contrario: **Se crea una instantánea si es posible.**

Puede seleccionar una de las siguientes opciones:

- **Crear una instantánea si es posible**

  Realizar la copia de seguridad directamente si no es posible tomar una instantánea.
- **Siempre crear una instantánea**

  La instantánea permite la copia de seguridad de todos los archivos, inclusive los archivos abiertos para accesos exclusivos. Los archivos se incluirán en la copia de seguridad al mismo momento determinado. Seleccione esta configuración sólo si los factores son críticos, es decir: la copia de seguridad sin tomar una instantánea no tiene sentido. Si no se puede tomar una instantánea, la copia de seguridad fallará.
- **No crear una instantánea**

  Siempre realizar la copia de seguridad directamente. El intento de copia de seguridad de archivos que están abiertos para acceso exclusivo generará un error de lectura. Los archivos en la copia de seguridad puede que no sean consistentes en el tiempo.

Datos forenses

Las actividades maliciosas de un equipo las pueden llevar a cabo virus, malware y ransomware. La otra situación que puede requerir que se realicen investigaciones se produce cuando diferentes programas roban o cambian datos de un equipo. Es posible que haya que investigar estas actividades, pero esto se puede hacer únicamente si hay pruebas digitales en un equipo en las que basarse. Sin embargo, es posible que las pruebas (archivos, rastros, etc.) se eliminen o que un equipo deje de estar disponible.

Con la opción de copias de seguridad llamada **Datos forenses** se pueden recopilar pruebas digitales para utilizarlas en investigaciones forenses. Los siguientes elementos se pueden usar como prueba digital: una instantánea del espacio del disco sin usar, volcados de memoria y una instantánea de los procesos que se están ejecutando. La funcionalidad **Datos forenses** está disponible únicamente para copias de seguridad de todo el equipo.

Actualmente, la opción **Datos forenses** está disponible únicamente para equipos Windows con las siguientes versiones del sistema operativo:

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

Nota

• Después de aplicar un plan de protección con el módulo de copia de seguridad en un equipo, no se podrá modificar la configuración de los datos forenses. Para usar una configuración diferente de datos forenses, cree un nuevo plan de protección.

• No se admiten las copias de seguridad con recopilación de datos forenses para los equipos conectados a su red mediante una VPN y sin acceso directo a Internet.

Las ubicaciones admitidas para guardar copias de seguridad con datos forenses son las siguientes:

- Almacenamiento en la cloud
- Carpeta local

Nota

1. La carpeta local solo se admite en un disco duro externo conectado mediante USB.
2. Los discos dinámicos locales no se admiten como ubicaciones para copias de seguridad de datos forenses.

- Carpeta de red

Las copias de seguridad con datos forenses se certifican automáticamente. Gracias a las copias de seguridad con datos forenses, los investigadores pueden analizar áreas de disco no incluidas en una copia de seguridad del disco habitual.

Proceso de copia de seguridad forense

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

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

Pasos para configurar la recopilación de datos forenses

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

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

8. Especifique la ubicación.
9. Haga clic en **Ejecutar ahora** para llevar a cabo directamente una copia de seguridad con datos forenses o espere a que la copia de seguridad se cree según la planificación.
10. Vaya a **Panel de control** > **Actividades** y verifique que se haya creado correctamente la copia de seguridad con datos forenses.

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

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

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

     El sistema mostrará una carpeta con los datos forenses. Seleccione un archivo de volcado de memoria o cualquier otro archivo de datos forenses, y haga clic en **Descargar**.
   - Para recuperar una copia de seguridad forense completa, haga clic en **Todo el equipo**. El sistema recuperará la copia de seguridad sin el modo de arranque. Por lo tanto, será posible comprobar que el disco no ha cambiado.

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

Certificación de copias de seguridad con datos forenses

Para asegurarse de que una copia de seguridad con datos forenses es exactamente igual que el contenido que se incluyó y que no se ha alterado nada, el módulo de copia de seguridad ofrece la certificación de las copias de seguridad con datos forenses.

Cómo funciona

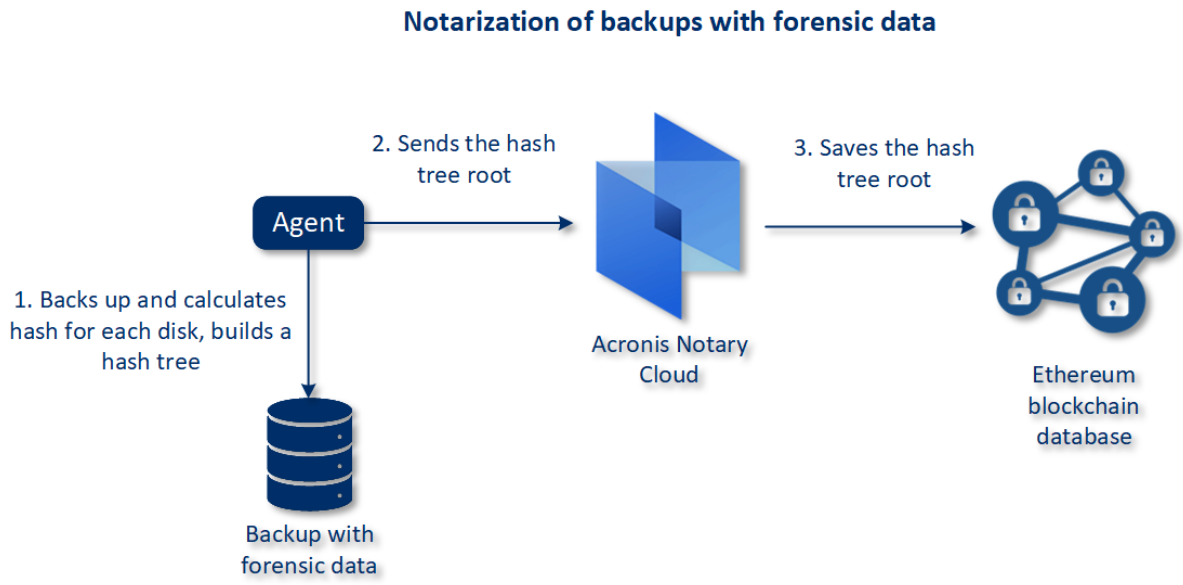
La certificación permite demostrar que un disco con datos forenses es auténtico y que no ha cambiado desde su copia de seguridad.

Durante una copia de seguridad, el agente calcula los códigos de cifrado de los discos de los que se ha realizado la copia de seguridad, crea un árbol de cifrado, guarda el árbol en la copia de seguridad y envía la raíz del árbol de cifrado al servicio de notarización. El servicio de notarización guarda la raíz del árbol de cifrado en la base de datos de cadenas de bloques de Ethereum para garantizar que este valor no cambie.

Al verificar la autenticidad del disco con datos forenses, el agente calcula su cifrado y lo compara con el almacenado en el árbol de cifrado de la copia de seguridad. Si los hashes no coinciden, se considerará que el disco no es auténtico. De lo contrario, la autenticidad del disco queda garantizada por el árbol de cifrado.

Para verificar que el propio árbol de cifrado no se haya visto alterado, el agente envía la raíz del árbol de cifrado al servicio de notarización. El servicio de notarización lo compara con el almacenado en la base de datos de cadenas de bloques. Si los hashes coinciden, se garantiza que el disco seleccionado es auténtico. De lo contrario, el software muestra un mensaje para indicar que el disco no es auténtico.

En el esquema que aparece a continuación se muestra brevemente el proceso de certificación de copias de seguridad con datos forenses.



Para comprobar manualmente la copia de seguridad del disco certificada, puede obtener su certificado y seguir el proceso de verificación que viene con él mediante la herramienta tibxread.

Obtener el certificado de copias de seguridad con datos forenses

Para obtener el certificado de una copia de seguridad con datos forenses de la consola, lleve a cabo los siguientes pasos:

1. Vaya a **Almacenamiento de la copia de seguridad** y seleccione la copia de seguridad con datos forenses.
2. Recupere todo el equipo.
3. El sistema abre la vista **Asignación de discos**.
4. Haga clic en el icono **Obtener certificado** del disco.
5. El sistema generará el certificado y este aparecerá en la nueva ventana de navegador que se abrirá. Debajo de certificado, verá las instrucciones necesarias para comprobar manualmente una copia de seguridad del disco certificada.

Herramienta "tibxread" para obtener datos incluidos en una copia de seguridad

Cyber Protect ofrece la herramienta llamada `tibxread`, que sirve para comprobar manualmente la integridad de los datos incluidos en una copia de seguridad. Con esta herramienta, puede obtener los datos de una copia de seguridad y calcular el hash del disco especificado. Además, se instala automáticamente con los siguientes componentes: Agente para Windows, Agente para Linux y Agente para Mac. Está ubicada en: `C:\Program Files\Acronis\BackupAndRecovery`.

Las ubicaciones admitidas son las siguientes:

- El disco local.
- La carpeta de red (CIFS/SMB) a la que se puede acceder sin credenciales.
  En el caso de que la carpeta de red esté protegida por una contraseña, puede montar la carpeta de red en la carpeta local mediante las herramientas del sistema operativo, y luego la carpeta local como fuente para esta herramienta.
- El almacenamiento en la cloud
  Debe proporcionar la URL, el puerto y el certificado. La URL y el puerto se pueden obtener de la clave del registro de Windows, o de los archivos de configuración en equipos Linux o Mac.
  Para Windows:

  ```
  HKEY_LOCAL_
  MACHINE\SOFTWARE\Acronis\BackupAndRecovery\Settings\OnlineBackup\FesAddressCache\Defa
  ult\<tenant_login>\FesUri
  ```

  Para Linux:

  ```
  /etc/Acronis/BackupAndRecovery.config
  ```

  Para macOS:

  ```
  /Library/Application Support/Acronis/Registry/BackupAndRecovery.config
  ```

  El certificado se puede encontrar en las siguientes ubicaciones:
  Para Windows:

  ```
  %allusersprofile%\Acronis\BackupAndRecovery\OnlineBackup\Default
  ```

  Para Linux:

  ```
  /var/lib/Acronis/BackupAndRecovery/OnlineBackup/Default
  ```

  Para macOS:

  ```
  /Library/Application Support/Acronis/BackupAndRecovery/OnlineBackup/Default
  ```

La herramienta cuenta con los siguientes comandos:

- list backups
- list content
- get content
- calculate hash

list backups

Enumera los puntos de recuperación de una copia de seguridad.

RESUMEN:

```
tibxread list backups --loc=URI --arc=BACKUP_NAME --raw
```

Opciones

```
--loc=URI
--arc=BACKUP_NAME
--raw
--utc
--log=PATH
```

```
Output template:
```

```
GUID   Date   Date timestamp
----   ------ --------------
<guid> <date> <timestamp>
```

<guid>: el GUID de copia de seguridad.

<date>: la fecha de creación de la copia de seguridad. Su formato es: DD.MM.YYYY HH24:MM:SS. En la zona horaria local predeterminada (se puede cambiar mediante la opción --utc).

Ejemplo de salida:

```
GUID   Date   Date timestamp
----   ------ --------------
516FCE73-5E5A-49EF-B673-A9EACB4093B8 18.12.2019 16:01:05 1576684865
516FCE73-5E5A-49EF-B673-A9EACB4093B9 18.12.2019 16:02:05 1576684925
```

list content

Enumera el contenido de un punto de recuperación.

RESUMEN:

```
tibxread list content --loc=URI --arc=BACKUP_NAME --password --backup=RECOVERY_POINT_ID
--raw --log=PATH
```

Opciones

```
--loc=URI
--arc=BACKUP_NAME
--password
--backup=RECOVERY_POINT_ID
--raw
--log=PATH
```

Plantilla de salida:

```
Disk     Size   Notarization status
-------- ------ --------------------
<number> <size> <notarization_status>
```

<number>: identificador del disco.

<size>: tamaño en bytes.

<notarization_status>: se pueden dar los siguientes estados: Sin certificación, Certificada y Siguiente copia de seguridad.

Ejemplo de salida:

```
Disk     Size   Notary status
-------- ------ --------------
1        123123465798 Notarized
2        123123465798 Notarized
```

get content

Escribe contenido del disco especificado del punto de recuperación en la salida estándar.

RESUMEN:

```
tibxread get content --loc=URI --arc=BACKUP_NAME --password --backup=RECOVERY_POINT_ID -
-disk=DISK_NUMBER --raw --log=PATH --progress
```

Opciones

```
--loc=URI
--arc=BACKUP_NAME
--password
--backup=RECOVERY_POINT_ID
--disk=DISK_NUMBER
--raw
--log=PATH
--progress
```

calculate hash

Calcula el hash del disco especificado del punto de recuperación mediante el uso del algoritmo de SHA-256 y lo escribe en la salida estándar.

RESUMEN:

```
tibxread calculate hash --loc=URI --arc=BACKUP_NAME --password --backup=RECOVERY_POINT_
ID --disk=DISK_NUMBER --raw --log=PATH --progress
```

Opciones

```
--loc=URI
--arc=BACKUP_NAME
--password
--backup=RECOVERY_POINT_ID
--disk=DISK_NUMBER
--raw
--log=PATH
```

Descripción de la opción

Opción	Descripción
--arc=BACKUP_NAME	Nombre del archivo de la copia de seguridad que puede obtener de las propiedades de la copia de seguridad en la consola web. El archivo de la copia de seguridad se debe especificar con la extensión .tibx.
--backup=RECOVERY_POINT_ID	Identificador del punto de recuperación
--disk=DISK_NUMBER	Número del disco (el mismo que se escribió en la salida del comando "get content")

--loc=URI	URI de la ubicación de una copia de seguridad. Los posibles formatos de la opción "--loc" son:
	• Nombre de la ruta local (Windows)
	`c:/upload/backups`
	• Nombre de la ruta local (Linux)
	`/var/tmp`
	• SMB/CIFS
	`\\server\folder`
	• Almacenamiento en la cloud
	`--loc=<IP_address>:443 --cert=<path_to_certificate> [--storage_path=/1]`
	`<IP_address>`: puede encontrarla en la clave de registro en Windows: HKEY_LOCAL_

	MACHINE\SOFTWARE\Acronis\BackupAndRecovery\Settings\OnlineBackup\FesAddressCache\Default\<tenant_login>\FesUri `<path_to_certificate>`: ruta al archivo del certificado para acceder a Cyber Protect Cloud. Por ejemplo, en Windows este certificado se encuentra en `C:\ProgramData\Acronis\BackupAndRecovery\OnlineBackup\Default\<username>.crt` donde <username> es su nombre de cuenta para acceder a Cyber Protect Cloud.
--log=PATH	Habilita que se pueda escribir en los registros mediante la RUTA especificada (únicamente la ruta local, el formato es el mismo que para el parámetro `--loc=URI`). El nivel de registro es DEPURACIÓN.
--password=CONTRASEÑA	Contraseña de cifrado para su copia de seguridad. Si la copia de seguridad no está cifrada, deje este valor vacío.

--raw	Oculta los encabezados (2 primeras filas) de la salida del comando. Se usa cuando se debe transmitir la salida del comando.
	Ejemplo de salida sin "`--raw`":
	`GUID Date Date timestamp`
	`---- ------ --------------`
	`516FCE73-5E5A-49EF-B673-A9EACB4093B8 18.12.2019 16:01:05 1576684865`
	`516FCE73-5E5A-49EF-B673-A9EACB4093B9 18.12.2019 16:02:05 1576684925`
	Salida con "`--raw`":
	`516FCE73-5E5A-49EF-B673-A9EACB4093B8 18.12.2019 16:01:05 1576684865`
	`516FCE73-5E5A-49EF-B673-A9EACB4093B9 18.12.2019 16:02:05 1576684925`

--utc	Muestra fechas en UTC.

--progress	Muestra el progreso de la operación.
	Por ejemplo:
	`1%`
	`2%`
	`3%`
	`4%`
	`...`
	`100%`

Truncamiento de registros

Esta opción funciona para la copia de seguridad de bases de datos de Microsoft SQL Server y para la copia de seguridad a nivel de disco con la copia de seguridad de aplicaciones de Microsoft SQL Server habilitada.

Esta opción define si los registros de transacción de SQL Server se truncan tras una copia de seguridad correcta.

El valor predeterminado es el siguiente: **Habilitado**.

Cuando está opción está habilitada, una base de datos solo se puede recuperar a un momento específico de una copia de seguridad que haya creado este software. Deshabilite esta opción si realiza copias de seguridad de los registros de transacción usando el motor nativo de copia de seguridad de Microsoft SQL Server. Podrá aplicar los registros de transacción después de una recuperación y, por lo tanto, recuperar una base de datos a cualquier momento específico.

Toma de instantáneas de LVM

Esta opción solo sirve para los equipos físicos.

Esta opción solo sirve para la copia de seguridad a nivel de disco de los volúmenes gestionados por Logical Volume Manager (LVM) de Linux. Dichos volúmenes también se llaman volúmenes lógicos.

Esta opción define cómo se toma una instantánea de un volumen lógico. El software de copia de seguridad puede hacerlo por sí mismo o recurrir a Logical Volume Manager (LVM) de Linux.

El valor predeterminado es el siguiente: **Con el software de copia de seguridad**.

- **Con el software de copia de seguridad**. Los datos de la instantánea se guardan, principalmente, en RAM. La copia de seguridad es más rápida y no se necesita espacio no asignado en el grupo del volumen. Por lo tanto, recomendamos cambiar el valor predeterminado solo si experimenta problemas al crear copias de seguridad de volúmenes lógicos.
- **Con LVM**. La instantánea se almacena en espacio no asignado del grupo del volumen. Si falta espacio no asignado, la instantánea la realizará el software de copia de seguridad.

La instantánea se utiliza solo durante la operación de copia de seguridad y se elimina automáticamente cuando se completa dicha operación. No se conservan archivos temporales.

Puntos de montaje

Esta opción solo se aplica en Windows a la copia de seguridad a nivel de archivos de un origen de datos que incluye volúmenes montados o volúmenes compartidos del clúster.

Esta opción es eficaz solo cuando selecciona realizar una copia de seguridad a una carpeta que se encuentra en un nivel superior en la jerarquía que el punto de montaje. (Un punto de montaje es una carpeta que posee un volumen adicional que está conectado lógicamente.)

- Si dicha carpeta (o carpeta principal) se selecciona para la copia de seguridad y la opción **Puntos de montaje** está seleccionada, todos los archivos en el volumen montado se incluirán en la copia de seguridad. Si la opción **Puntos de montaje** está deshabilitada, el punto de montaje en la copia de seguridad estará vacío.

  Durante la recuperación de una carpeta principal, el contenido del punto de montaje se recuperará o no según si la opción para la recuperación de Puntos de montaje está habilitada o deshabilitada.

- Si selecciona un punto de montaje directamente o selecciona cualquier carpeta dentro del volumen montado, las carpetas seleccionadas se considerarán como carpetas normales. Se incluirán en la copia de seguridad sin importar el estado de la opción **Puntos de montaje** y se recuperarán sin importar el estado de la opción para la recuperación de **Puntos de montaje**.

El valor predeterminado es el siguiente: **Deshabilitado**.

Nota
Puede realizar copias de seguridad de equipos virtuales de Hyper-V en un volumen compartido del clúster al realizar la copia de seguridad de los archivos necesarios o de todo el volumen con la copia de seguridad a nivel de archivo. Solo apague los equipos virtuales para asegurarse que se incluyen en la copia de seguridad en el estado consistente.

Ejemplo

Supongamos que la carpeta **C:\Datos1** es un punto de montaje para el volumen montado. El volumen contiene las carpetas **Carpeta1** y **Carpeta2**. Puede crear un plan de protección para realizar la copia de seguridad a nivel de archivos de sus datos.

Si selecciona la casilla de verificación para el volumen C y habilita la opción **Puntos de montaje**, la carpeta **C:\Datos1** en su copia de seguridad contendrá la **Carpeta1** y **Carpeta2**. Al recuperar los datos incluidos en la copia de seguridad, tenga en cuenta de utilizar adecuadamente la opción para la recuperación de Puntos de montaje.

Si selecciona la casilla de verificación para el volumen C y deshabilita la opción **Puntos de montaje**, la carpeta **C:\Datos1** en su copia de seguridad estará vacía.

Si selecciona la casilla de verificación para la carpeta **Datos1**, **Carpeta1** o **Carpeta2**, las carpetas marcadas se incluirán en la copia de seguridad como carpetas normales, sin importar el estado de la opción de los **Puntos de montaje**.

Instantánea multivolumen

Esta opción sirve para las copias de seguridad de equipos físicos que ejecutan Windows o Linux.

Esta opción se aplica a la copia de seguridad de nivel del disco. Esta opción también se aplica a la copia de seguridad a nivel de archivo cuando se realiza una copia de seguridad a nivel de archivo al tomar una instantánea. (La opción "Instantánea de la copia de seguridad a nivel de archivo" determina si se tomará una instantánea durante la copia de seguridad a nivel de archivo).

Esta opción determina si se tomarán las instantáneas de varios volúmenes al mismo tiempo o una a una.

El valor predeterminado es el siguiente:

- Si se selecciona al menos un equipo que ejecute Windows para la copia de seguridad: **Habilitado**.
- Si no se selecciona ningún equipo (este es el caso cuando se empieza a crear un plan de

protección desde la página **Planes** > **Copia de seguridad**): **Habilitado**.

- De lo contrario: **Deshabilitado**.

  Cuando esta opción está habilitada, se crean simultáneamente instantáneas de todos los volúmenes de los que se hace la copia de seguridad. Utilice esta opción para crear una copia de seguridad consistente en el tiempo de datos que abarcan varios volúmenes, por ejemplo, para una base de datos de Oracle.

  Cuando esta opción está deshabilitada, las instantáneas de los volúmenes se toman una después de la otra. Como resultado, si los datos abarcan varios volúmenes, puede que la copia de seguridad obtenida no sea consistente.

Recuperación con un clic

Recuperación con un clic permite a los usuarios recuperar automáticamente la última copia de seguridad del disco de sus equipos. Puede ser una copia de seguridad de todo el equipo, o de discos o volúmenes específicos de este equipo.

Se puede acceder a esta característica en el equipo de un usuario una vez que un administrador la activa, junto con Startup Recovery Manager. El administrador solo puede realizar esta operación mediante la interfaz de la línea de comandos. Para obtener más información sobre cómo activar Startup Recovery Manager y Recuperación con un clic, consulte la referencia de la línea de comandos.

Recuperación con un clic admite los siguientes tipos de almacenamiento de copias de seguridad:

1. Secure Zone
2. Almacenamiento en red
3. Almacenamiento en la cloud

Si un tipo de almacenamiento específico no está disponible o no contiene copias de seguridad de disco, se indicará al usuario que utilice el tipo siguiente.

Si en el tipo de almacenamiento hay disponible más de un conjunto de copias de seguridad (lo que también se denomina un *archivo comprimido*) que contienen copias de seguridad de disco, Recuperación con un clic selecciona el conjunto que se actualizó más recientemente. El usuario no puede seleccionar un conjunto de copias de seguridad diferente.

Recuperación con un clic admite las siguientes operaciones:

- Recuperación automática desde la copia de seguridad más reciente
- Recuperación desde una copia de seguridad específica (lo que también se denomina *punto de recuperación*) dentro del conjunto de copias de seguridad seleccionado automáticamente

Recuperar un equipo con Recuperación con un clic

Requisitos previos

- Un administrador ha activado Recuperación con un clic en el equipo seleccionado.
- Existe al menos una copia de seguridad del disco del equipo seleccionado.

Para recuperar un equipo

1. Reinicie el equipo que desea recuperar.
2. Durante el reinicio, pulse F11 para entrar en Startup Recovery Manager.
3. Seleccione la opción de Recuperación con un clic que desee:
   - Para recuperar automáticamente la copia de seguridad más reciente, pulse 1 en el teclado.
   - Para recuperar una copia de seguridad distinta dentro del conjunto de copias de seguridad actualizado más recientemente, pulse 2 en el teclado.
     - Para seleccionar la copia de seguridad deseada (lo que también se denomina un *punto de recuperación*), pulse el número correspondiente en el teclado.

La interfaz gráfica de usuario se inicia y luego desaparece. El procedimiento de recuperación continúa sin ella. Una vez que la recuperación se completa, el equipo se reinicia.

Ventana de copia de seguridad y rendimiento

Esta opción le sirve para establecer uno de los tres niveles de rendimiento de copia de seguridad (alto, bajo o sin permiso) para cada hora durante una semana. De esta forma, puede definir un intervalo de tiempo en el que las copias de seguridad se puedan iniciar y ejecutar. El nivel de rendimiento alto y el bajo se pueden configurar en lo que respecta a la velocidad de salida y prioridad del proceso.

Esta opción no está disponible para copias de seguridad que ejecutan agentes en el cloud, como copias de seguridad de sitios web o de servidores alojados en el sitio web de recuperación en el cloud.

Puede configurar esta opción de forma independiente para cada ubicación especificada en el plan de protección. Para configurar esta opción para una ubicación de réplica, haga clic en el icono del engranaje que se encuentra junto al nombre de la ubicación y, luego, en **Ventana de copia de seguridad y rendimiento**.

Esta opción es válida únicamente para los procesos de copia de seguridad y réplicas de copias de seguridad. Los comandos posteriores a la copia de seguridad y otras operaciones incluidas en un plan de protección (validación y conversión a un equipo virtual) se ejecutarán independientemente de si esta opción está habilitada.

El valor predeterminado es el siguiente:**Deshabilitado**.

Cuando esta opción está deshabilitada, las copias de seguridad se pueden ejecutar en cualquier momento con los siguientes parámetros (no importa si los parámetros se cambiaron sin respetar el valor predeterminado):

- Prioridad de la CPU: **Baja** (en Windows corresponde a **Por debajo de lo normal**).
- Velocidad de salida: **Ilimitada**.

Cuando esta opción está habilitada, se permiten o bloquean las copias de seguridad planificadas según los parámetros de rendimiento especificados para la hora actual. Cuando comienza una hora en la que las copias de seguridad están bloqueadas, se detiene automáticamente el proceso de copia de seguridad y aparece una alerta.

Aunque las copias de seguridad planificadas estén bloqueadas, se puede iniciar una manualmente. Esta usará los parámetros de rendimiento de la hora más reciente en la que estaban permitidas las copias de seguridad.

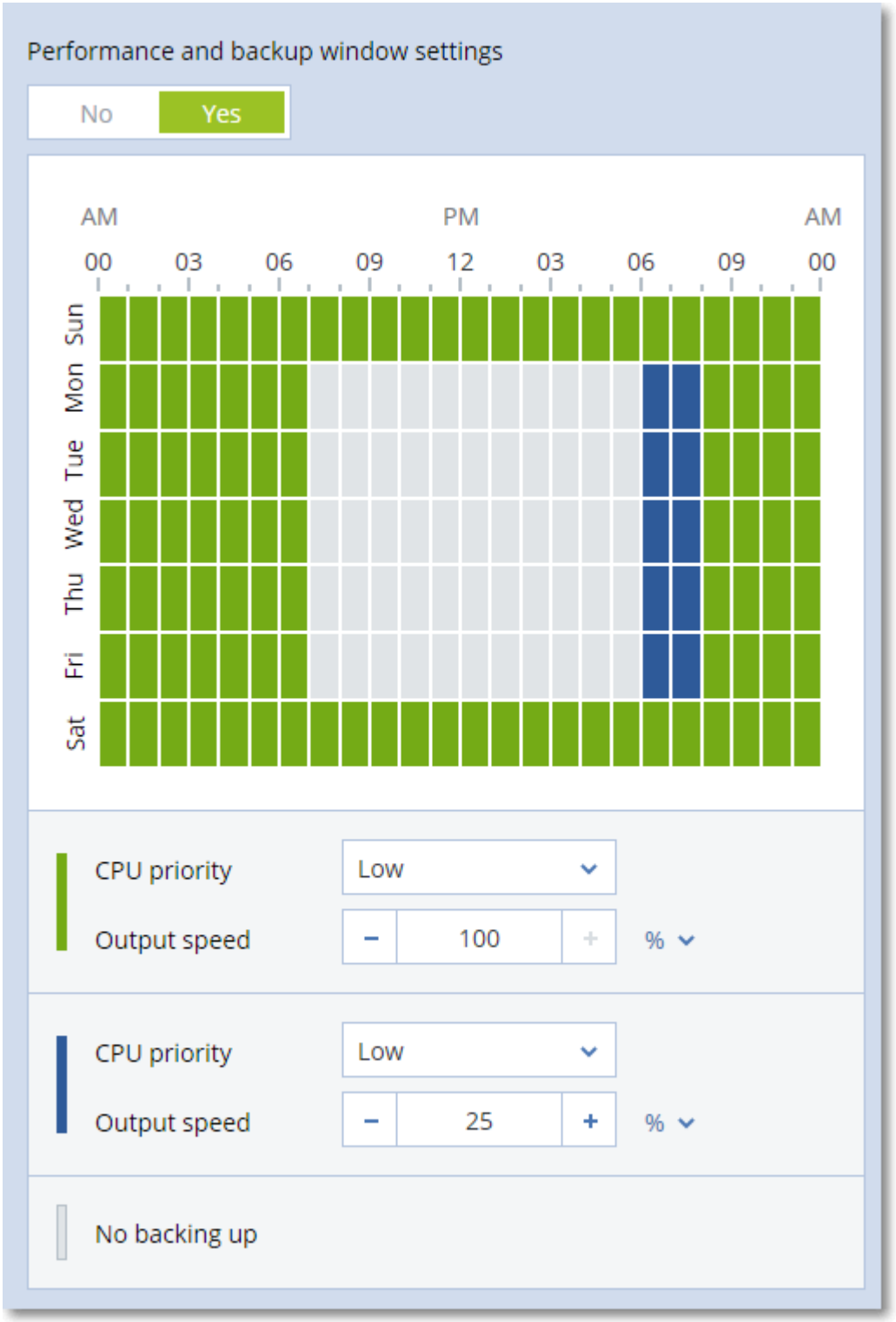
Ventana de copias de seguridad

Cada rectángulo representa una hora de un día de la semana. Haga clic en un rectángulo para desplazarse por los siguientes estados:

- **Verde:** se permite la realización de copias de seguridad con los parámetros especificados en la sección verde que aparece a continuación.
- **Azul:** se permite la realización de copias de seguridad con los parámetros especificados en la sección azul que aparece a continuación.

  Este estado no está disponible si el formato de copia de seguridad está establecido en la **versión 11**.
- **Gris:** la realización de copias de seguridad está bloqueada.

Puede hacer clic y arrastrar para cambiar el estado de varios rectángulos de forma simultánea.



Prioridad de la CPU

Este parámetro define la prioridad del proceso de copia de seguridad en el sistema operativo.

Los ajustes disponibles son:

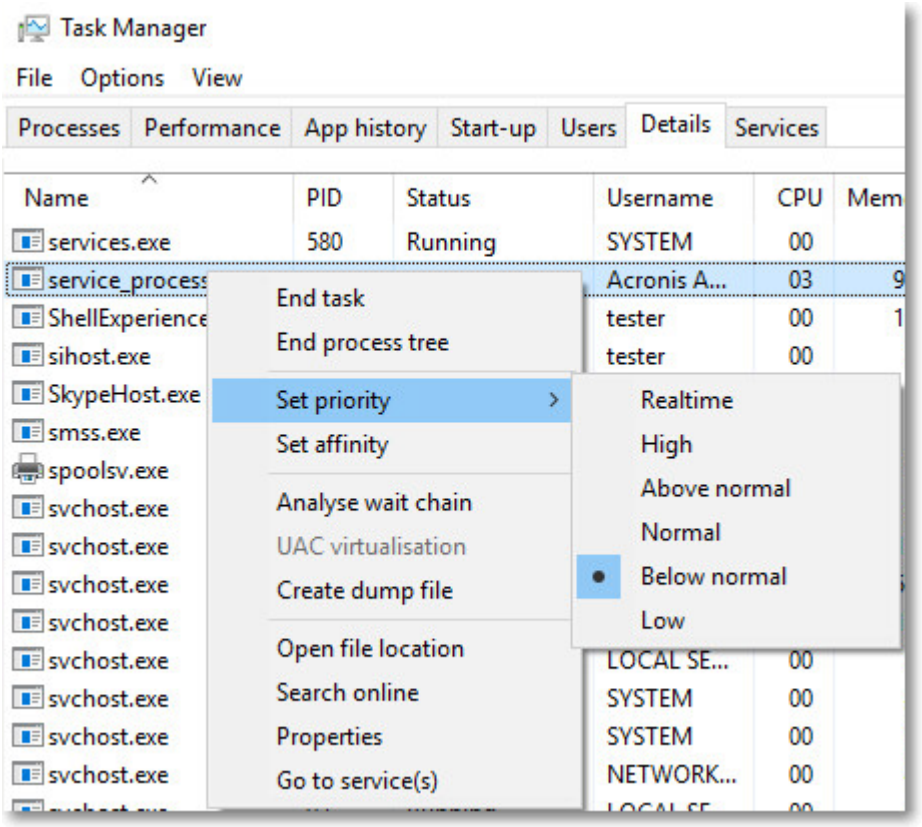
Baja: en Windows corresponde a **Por debajo de lo normal**.

Normal: en Windows corresponde a **Normal**.

Alta: en Windows corresponde a **Alta**.

La prioridad de un proceso que se ejecute en un sistema determina la cantidad de uso de la CPU y los recursos del sistema que se asignan a dicho proceso. La disminución de la prioridad de la copia de seguridad liberará más recursos para otras aplicaciones. El aumento de la prioridad podría acelerar el proceso de copia de seguridad al solicitar que el sistema operativo asigne más recursos, como CPU, a la aplicación de copia de seguridad. Sin embargo, el efecto resultante dependerá del uso total de CPU y otros factores, como la velocidad de salida o entrada del disco, o el tráfico en la red.

Esta opción define la prioridad de un proceso de copia de seguridad (**service_process.exe)** en Windows y la perfección de este proceso (**service_process)** en Linux y en OS X.



Velocidad de salida durante la copia de seguridad

Este parámetro permite limitar la velocidad de escritura en el disco duro (al hacer copias de seguridad en una carpeta local) o la velocidad de transferencia de los datos de la copia de seguridad a través de la red (al hacer copias de seguridad en un recurso compartido de red o en el almacenamiento en cloud).

Cuando esta opción está habilitada, puede especificar la velocidad de salida máxima permitida:

- Como porcentaje de la velocidad de escritura estimada del disco rígido de destino (al hacer copias de seguridad en una carpeta local) o la velocidad máxima estimada de la conexión de red

(al hacer copias de seguridad en un recurso compartido de red o en el almacenamiento en cloud. Esta configuración solo funciona si el agente se ejecuta en Windows.

- En KB/segundo (para todos los destinos).

Envío de datos físicos

Esta opción se aplica si el destino de la copia de seguridad es el almacenamiento en la cloud y el formato de la copia de seguridad está establecido en la **Versión 12**.

Esta opción se aplica a las copias de seguridad de discos y archivos creadas por los agentes para Windows, Linux, Mac, VMware y Hyper-V. No se admiten copias de seguridad creadas en dispositivos de arranque.

Esta opción determina si la primera copia de seguridad completa creada por el plan de protección se enviará al almacenamiento en la nube en una unidad de disco rígido mediante el servicio de envío de datos físicos. Las copias de seguridad incrementales posteriores se pueden transferir a través de la red.

El valor predeterminado es el siguiente: **Deshabilitado**

Acerca del servicio de envío de datos físicos

La interfaz web del servicio de envío de datos físicos solo está disponible para administradores de la organización en implementaciones locales y administradores en implementaciones en la nube.

Para obtener instrucciones detalladas acerca del uso del servicio de envío de datos físicos y la herramienta de creación de pedidos, consulte la Guía del administrador para el envío de datos físicos. Para acceder a este documento en la interfaz web del servicio de envío de datos físicos, haga clic en el icono de signo de interrogación.

Información general acerca del proceso de envío de datos físicos

1. Cree un nuevo plan de protección. En este plan, habilite la opción de copia de seguridad **Envío de datos físicos**.

   Puede realizar la copia de seguridad directamente en la unidad, o bien realizarla en una carpeta local o de red y, a continuación, copiarla o moverla a la unidad.

   Importante
   Tras finalizar la primera copia de seguridad completa, las copias de seguridad posteriores deben realizarse en el mismo plan de protección. Cualquier otro plan de protección, incluso uno con los mismos parámetros y para el mismo equipo, requerirá otro ciclo de envío de datos físicos.

2. Tras completar la primera copia de seguridad, use la interfaz web del servicio de envío de datos físicos para descargar la herramienta de creación de pedidos y cree uno.

   Realice una de las siguientes acciones para acceder a esta interfaz web:

   - En implementaciones locales: inicie sesión en su cuenta de Acronis y luego haga clic en **Ir a la Consola de seguimiento** que encontrará en **Envío de datos físicos**.

- En implementaciones en el cloud: inicie sesión en el portal de gestión, haga clic en **Información general** > **Uso** y, a continuación, en **Gestionar servicio**, que encontrará en **Envío de datos físicos**.

3. Empaquete las unidades y envíelas al centro de datos.

   Importante
   Asegúrese de seguir las instrucciones de empaquetado que se proporcionan en la Guía del administrador para el envío de datos físicos.

4. La interfaz web del servicio de envío de datos físicos permite realizar el seguimiento del estado del pedido. Tenga en cuenta que las copias de seguridad posteriores generarán un error hasta que la primera copia de seguridad se cargue en el almacenamiento en la cloud.

Comandos previos/posteriores

Esta opción le permite definir los comandos a ejecutar automáticamente antes y después del proceso de copia de seguridad.

El siguiente esquema describe cuando se ejecutan los comandos pre/post.

Comando de precopia de seguridad	Copia de seguridad	Comando de Post-copia de seguridad

Ejemplos de como se pueden usar los comandos pre/post:

- Eliminación de archivos temporales antes de comenzar la copia de seguridad.
- Configuración de un producto antivirus de terceros antes de comenzar la copia de seguridad.
- Copia selectiva de copias de seguridad en otra ubicación. Esta opción puede ser útil porque la replicación configurada en un plan de protección copia *todas* las copias de seguridad a ubicaciones posteriores.

El programa realiza la replicación *después* de ejecutar el comando posterior a la copia de seguridad.

El programa no admite comandos interactivos, es decir, comandos que requieran la intervención del usuario (por ejemplo, “pausa”).

Comando de precopia de seguridad

Para especificar un comando o archivo por lotes para que se ejecute antes de que comience el proceso de copia de seguridad

1. Habilite el conmutador **Ejecutar un comando antes de la copia de seguridad**.
2. En el campo **Comando...**, escriba un comando o busque un archivo de proceso por lotes. El programa no admite comandos interactivos, es decir, comandos que requieran la intervención del usuario (por ejemplo, “pausa”).

3. En el campo **Directorio de trabajo**, especifique una ruta en donde se ejecutará el comando o archivo de proceso por lotes.
4. En el campo **Argumentos**, especifique los argumentos de ejecución del comando, si fuera necesario.
5. Dependiendo del resultado que desee obtener, seleccione la opción apropiada tal y como se describe en la siguiente tabla.
6. Haga clic en **Realizado**.

Casilla de verificación	**Selección**			
Hacer que la copia de seguridad falle si falla la ejecución del comando*	Seleccionado	Borrado	Seleccionado	Borrado
No realizar la copia de seguridad hasta que finalice la ejecución de comandos	Seleccionado	Seleccionado	Borrado	Borrado
Resultado				
	Valor predeterminado Realizar la copia de seguridad solo después de que se ejecute el comando correctamente. Hacer que la copia de seguridad falle si falla la ejecución del comando.	Realizar la copia de seguridad después de que se ejecute el comando a pesar del éxito o fallo de la ejecución	N/D	Realizar la copia de seguridad al mismo tiempo que se ejecuta el comando, independientemente del resultado de la ejecución del comando.

* Un comando se considerará fallido si su código de salida no es igual a cero.

Comando de Post-copia de seguridad

Para especificar un comando o archivo que se ejecute después de completar la copia de seguridad

1. Habilite el conmutador **Ejecutar un comando tras la copia de seguridad**.
2. En el campo **Comando...**, escriba un comando o busque un archivo de proceso por lotes.
3. En el campo **Directorio de trabajo**, especifique una ruta en donde se ejecutará el comando o archivo de proceso por lotes.
4. En el campo **Argumentos**, especifique los argumentos de ejecución del comando, si fuera necesario.
5. Active la casilla de verificación **Hacer que la copia de seguridad falle si falla la ejecución del comando** si cree que la ejecución correcta del comando es fundamental. El comando se considerará fallido si su código de salida no es igual a cero. Si la ejecución del comando falla, el estado de la copia de seguridad será **Error**.

   Cuando no se marca la casilla de verificación, los resultados de la ejecución del comando no afectarán al éxito o fallo de la copia de seguridad. Puede realizar un seguimiento de la ejecución de comandos desde la pestaña **Actividades**.
6. Haga clic en **Realizado**.

Comandos previos o posteriores a la captura de datos

La opción le permite definir los comandos que se ejecutarán automáticamente antes y después de la captura de datos (es decir, tomar la instantánea de los datos). La captura de datos se realiza al comienzo del procedimiento de copia de seguridad.

El siguiente esquema describe cuando se ejecutan los comandos pre/post de la captura de datos.

<table>
<tr><td></td><td colspan="4"><---------- Copia de seguridad ----------></td><td></td></tr>
<tr><td>Comando de precopia de seguridad</td><td>Comandos antes de la captura de datos</td><td>Captura de datos</td><td>Comandos Post de la captura de datos</td><td></td><td>Comando de Post-copia de seguridad</td></tr>
</table>

Si la opción Volume Shadow Copy Service está habilitada, la ejecución de los comandos y las acciones de Microsoft VSS se sucederán tal y como se indica a continuación:

Comandos "Antes de la captura de datos" -> Suspensión de VSS -> Captura de datos -> Reanudación de VSS -> Comandos "Después de la captura de datos".

El uso de comandos previos y posteriores a la captura de datos permite suspender y reanudar una base de datos o una aplicación que no sean compatibles con VSS. Como la captura de datos tarda unos segundos, el tiempo de inactividad de la base de datos o la aplicación será mínimo.

Comandos antes de la captura de datos

Para especificar un comando o archivo por lotes para que se ejecute antes de la captura de datos

1. Habilite el conmutador **Ejecutar un comando antes de la captura de datos**.
2. En el campo **Comando...**, escriba un comando o busque un archivo de proceso por lotes. El programa no admite comandos interactivos, es decir, comandos que requieran la intervención del usuario (por ejemplo, "pausa").
3. En el campo **Directorio de trabajo**, especifique una ruta en donde se ejecutará el comando o archivo de proceso por lotes.
4. En el campo **Argumentos**, especifique los argumentos de ejecución del comando, si fuera necesario.
5. Dependiendo del resultado que desee obtener, seleccione la opción apropiada tal y como se describe en la siguiente tabla.
6. Haga clic en **Realizado**.

Casilla de verificación	**Selección**			
Hacer que la copia de seguridad falle si falla la ejecución del comando*	Seleccionado	Borrado	Seleccionado	Borrado
No realizar la captura de datos hasta que finalice la ejecución de comandos	Seleccionado	Seleccionado	Borrado	Borrado
Resultado				
	Valor predeterminado Realizar la captura de datos solo después de que se ejecute el comando correctamente. Hacer que la copia de seguridad falle si falla la ejecución	Realizar la captura de datos después de que se ejecute el comando a pesar del éxito o fallo de la ejecución	N/D	Realizar la captura de datos al mismo tiempo que se ejecuta el comando, independientemente del resultado de la ejecución del comando.

	del comando.			

* Un comando se considerará fallido si su código de salida no es igual a cero.

Comandos Post de la captura de datos

Para especificar un comando o archivo por lotes para que se ejecute después de la captura de datos

1. Habilite el conmutador **Ejecutar un comando tras la captura de datos**.
2. En el campo **Comando...**, escriba un comando o busque un archivo de proceso por lotes. El programa no admite comandos interactivos, es decir, comandos que requieran la intervención del usuario (por ejemplo, “pausa”).
3. En el campo **Directorio de trabajo**, especifique una ruta en donde se ejecutará el comando o archivo de proceso por lotes.
4. En el campo **Argumentos**, especifique los argumentos de ejecución del comando, si fuera necesario.
5. Dependiendo del resultado que desee obtener, seleccione la opción apropiada tal y como se describe en la siguiente tabla.
6. Haga clic en **Realizado**.

Casilla de verificación	**Selección**			
Hacer que la copia de seguridad falle si falla la ejecución del comando*	Seleccionado	Borrado	Seleccionado	Borrado
No realizar la copia de seguridad hasta que finalice la ejecución de comandos	Seleccionado	Seleccionado	Borrado	Borrado
Resultado				
	Valor predeterminado Continúe la copia de seguridad solo después de que se	Continúe la copia de seguridad después de que se ejecute	N/D	Continuar la copia de seguridad al mismo tiempo que se ejecuta el comando, independientemente

	ejecute el comando correctamente.	el comando a pesar del éxito o fallo de su ejecución.		del resultado de la ejecución del comando.

***** Un comando se considerará fallido si su código de salida no es igual a cero.

Instantáneas de hardware SAN

Esta opción es eficaza para copias de seguridad de equipos virtuales VMware ESXi.

El valor predeterminado es el siguiente: **Deshabilitado**.

Esta opción determina si se deben usar instantáneas SAN cuando se realiza una copia de seguridad.

Si esta opción está deshabilitada, el contenido de la unidad de disco virtual se leerá desde una instantánea VMware. La instantánea se conservará durante todo el tiempo que tarde la copia de seguridad.

Si esta opción está habilitada, el contenido de la unidad de disco virtual se leerá desde una instantánea SAN. Se creará una instantánea de VMware y se conservará poco tiempo para poner la unidad de los discos virtuales en un estado coherente. Si no es posible leer desde una instantánea SAN, la copia de seguridad fallará.

Antes de habilitar esta opción, compruebe y lleve a cabo los requisitos enumerados en "Uso de instantáneas de hardware SAN".

Planificación

Esta opción define si las copias de seguridad empiezan según lo planificado o con demora, así como la cantidad de equipos virtuales de los que se hace copia de seguridad simultáneamente.

Para obtener más información sobre cómo configurar la planificación de las copias de seguridad, consulte "Planificación" (p. 282).

El valor predeterminado es el siguiente:

- Implementación local: **Iniciar todas las copias de seguridad según lo planificado**
- Despliegue en la nube: **Distribuya las horas de inicio de la copia de seguridad en un período de tiempo. Retraso máximo: 30 minutos**

Puede seleccionar una de las siguientes opciones:

- **Iniciar todas las copias de seguridad según lo planificado**.
  Las copias de seguridad de los equipos físicos empezarán exactamente según la planificación. Las copias de seguridad de los equipos virtuales se harán una a una.
- **Distribuir las horas de inicio en una ventana de tiempo**
  Las copias de seguridad de los equipos físicos empezarán con demora respecto a la hora planificada. El valor de demora de cada equipo se selecciona de forma aleatoria y oscila entre

cero y el valor máximo que especifique. Puede resultarle útil para evitar una carga excesiva de la red al realizar copias de seguridad de varios equipos simultáneamente en una misma ubicación de red. El valor de demora de cada equipo se determina cuando se aplica el plan de protección en el equipo y permanece igual hasta que se edita el plan de protección y se modifica el valor máximo de demora.

Las copias de seguridad de los equipos virtuales se harán una a una.

- **Limitar el número de copias de seguridad ejecutadas a la vez a**

  Utilice esta opción para gestionar la copia de seguridad paralela de las máquinas virtuales de las que se hace una copia de seguridad a nivel del hipervisor (copia de seguridad sin agente).

  Los planes de protección en los que está seleccionada esta opción se pueden ejecutar con otros planes de protección que el agente esté operando simultáneamente. Cuando seleccione esta opción, debe especificar el número de copias de seguridad paralelas por plan. El número total de equipos de los que se hace una copia de seguridad simultáneamente por todos los planes se limita a 10 por agente. Para saber cómo cambiar el límite predeterminado, consulte "Limitar el número total de equipos virtuales que se incluyen en la copia de seguridad al mismo tiempo" (p. 565).

  Los planes de protección en los que no está seleccionada esta opción ejecutan operaciones de copia de seguridad de forma secuencial en una máquina virtual tras otra.

Copia de seguridad sector por sector

La opción es eficaz solo para la copia de seguridad a nivel del disco.

Esta opción define si se crea una copia exacta de un disco o volumen en un nivel físico.

El valor predeterminado es el siguiente: **Deshabilitado**.

Si esta opción está habilitada, se hará copia de seguridad de todos los sectores del disco o volumen, incluido el espacio no asignado y los sectores que no tengan datos. La copia de seguridad resultante tendrá el mismo tamaño que el disco objeto de la copia de seguridad (si la opción "Nivel de compresión" se establece en **Ninguno**). El software cambia automáticamente al modo sector por sector al hacer copias de seguridad de unidades con sistemas de archivos no reconocidos o incompatibles.

Nota

Será imposible realizar una recuperación de datos de aplicaciones desde las copias de seguridad creadas en el modo sector por sector.

División

Esta opción se aplica a los esquemas de copias de seguridad **Siempre completas**, **Completa semanal, incremental diaria**, **Completa mensual, diferencial semanal, incremental diaria (GFS)** y **Personalizada**.

Esta opción permite seleccionar el método de división de las copias de seguridad de gran tamaño en archivos más pequeños.

El valor predeterminado es el siguiente: **Automático**.

Están disponibles las siguientes configuraciones:

- **Automático**
  La copia de seguridad se dividirá si supera el tamaño de archivo máximo que admite el sistema de archivos.
- **Tamaño fijo**
  Introduzca el tamaño de archivo deseado o selecciónelo de la lista desplegable.

Gestión de cintas

Estas opciones son eficaces cuando el destino de la copia de seguridad es un dispositivo de cintas.

Habilite la recuperación de archivos de las copias de seguridad del disco almacenadas en cintas

El valor predeterminado es el siguiente: **Deshabilitado**.

Si esta casilla está seleccionada, en cada copia de seguridad el software crea archivos complementarios en el disco duro del equipo donde está conectado el dispositivo de cintas. La recuperación desde las copias de seguridad de discos es posible siempre y cuando estos archivos complementarios estén intactos. Los archivos se eliminan automáticamente cuando la cinta que almacena las copias de seguridad correspondientes se borran, eliminan o sobrescriben.

Las ubicaciones de los archivos complementarios son las siguientes:

- En Windows XP y Server 2003: **%ALLUSERSPROFILE%\Application Data\Acronis\BackupAndRecovery\TapeLocation**.
- En Windows 7 y versiones posteriores de Windows: **%PROGRAMDATA%\Acronis\BackupAndRecovery\TapeLocation**.
- En Linux: **/var/lib/Acronis/BackupAndRecovery/TapeLocation**.

El espacio ocupado por estos archivos complementarios depende de la cantidad de archivos en la copia de seguridad correspondiente. Para obtener una copia de seguridad completa de un disco que contenga aproximadamente 20.000 archivos (la copia de seguridad de disco de estación de trabajo típica), los archivos complementarios ocupan alrededor de 150 MB. La copia de seguridad completa de un servidor que contiene 250.000 archivos puede producir alrededor de 700 MB de archivos complementarios. Por lo tanto, si está seguro de que no necesitará recuperar archivos individuales, puede dejar la casilla de verificación sin marcar para ahorrar el espacio en el disco.

Si los archivos complementarios no se crearon durante la copia de seguridad o si se eliminaron, puede crearlos al volver a examinar las cintas donde se almacena la copia de seguridad.

Mover la cinta de nuevo a la ranura de la unidad después de cada copia de seguridad correcta de cada equipo

El valor predeterminado es el siguiente: **Habilitado**.

Si deshabilita esta opción, la cinta permanecerá en la unidad después de que la operación con la cinta haya finalizado. En caso contrario, el software devolverá la cinta a la ranura de la unidad en la que se encontraba antes de la operación. Si, de acuerdo con el plan de protección, se deben realizar otras operaciones después de la copia de seguridad (tales como la validación de la copia de seguridad o la replicación en otra ubicación), la cinta se devolverá a su ranura de la unidad después de finalizar estas operaciones.

Si esta opción y la opción **Expulsar la cinta después de cada copia de seguridad correcta de cada equipo** están habilitadas, se expulsará la cinta.

Expulsar la cinta después de cada copia de seguridad correcta de cada equipo

El valor predeterminado es el siguiente: **Deshabilitado**.

Cuando esta casilla de verificación está seleccionada, el software expulsa las cintas después de crear correctamente una copia de seguridad de cada equipo. Si, de acuerdo con el plan de protección, se deben realizar otras operaciones después de la copia de seguridad (tales como la validación de la copia de seguridad o la replicación en otra ubicación), las cintas se expulsarán después de finalizar estas operaciones.

Sobrescribir una cinta en la unidad de cinta independiente al crear una copia de seguridad completa

El valor predeterminado es el siguiente: **Deshabilitado**.

La opción se aplica solo a unidades de cintas autónomas. Cuando esta opción está habilitada, una cinta insertada en una cinta se sobrescribirá cada vez que se cree una copia de seguridad completa.

Utilice los siguientes dispositivos de cintas y unidades

Esta opción le permite especificar los dispositivos de cintas y las unidades de cinta que se utilizarán en el plan de protección.

Un pool de cintas contiene las cintas de todos los dispositivos de cintas conectados a un equipo, ya sea un nodo de almacenamiento o un equipo donde haya instalado un agente de protección o ambos. Al seleccionar un pool de cintas como ubicación de la copia de seguridad, indirectamente selecciona el equipo al que se conectará el dispositivo de cintas. De forma predeterminada, las copias de seguridad se pueden escribir en cintas mediante el uso de cualquier unidad de cinta y dispositivo de cintas conectado al equipo. Si algunos dispositivos o unidades faltan o no están operativos, el plan de protección utilizará los que estén disponibles.

Puede hacer clic en **Solo los dispositivos y unidades seleccionados** y, a continuación, elegir los dispositivos y las unidades de cinta de la lista. Al seleccionar el dispositivo entero, selecciona todas sus unidades. Esto significa que el plan de protección puede utilizar cualquiera de estas unidades. Si la unidad o el dispositivo seleccionado falta o no está operativo, y no hay otros dispositivos seleccionados, la copia de seguridad fallará.

Mediante el uso de esta opción, puede controlar las copias de seguridad realizadas por distintos agentes en una gran biblioteca de cintas con varias unidades. Por ejemplo, puede que la copia de seguridad de un servidor de archivos o recurso compartido de archivos de gran tamaño no comience si varios agentes realizan copias de seguridad de sus equipos en la misma ventana de copia de seguridad, ya que los agentes ocupan todas las unidades. Si permite que los agentes utilicen, por ejemplo, las unidades 2 y 3, la unidad 1 queda reservada para el agente que realiza la copia de seguridad del recurso compartido.

Multitransmisión

El valor predeterminado es el siguiente: **Deshabilitado**.

La multitransmisión le permite partir los datos de un agente en múltiples transmisiones y escribirlas en distintas cintas a la vez. Esto implica copias de seguridad más rápidas y es especialmente útil cuando el agente tiene más rendimiento que la unidad de cinta.

La casilla de verificación **Multitransmisión** solo estará disponible si selecciona más de una unidad de cinta en la opción **Solo los dispositivos y unidades seleccionados**. La cantidad de unidades seleccionadas es igual a la cantidad de transmisiones simultáneas de un agente. Si alguna de las unidades seleccionadas no está disponible al iniciar la copia de seguridad, esta copia de seguridad dará error.

Para recuperar una copia de seguridad con múltiples transmisiones o con múltiples transmisiones y con multiplex, como mínimo deberá disponer de la misma cantidad de unidades utilizadas para crear la copia de seguridad.

No puede cambiar la configuración de multitransmisión de un plan de protección existente. Si desea utilizar una configuración diferente o cambiar las unidades de cinta seleccionadas, cree un nuevo plan de protección.

La multitransmisión está disponible tanto para las unidades de cinta conectadas localmente como para las unidades de cinta conectadas a un nodo de almacenamiento.

Multiplex

El valor predeterminado es el siguiente: **Deshabilitado**.

El multiplex le permite escribir transmisiones de datos de múltiples agentes en una única cinta. Esto implica un mejor uso de las unidades de cinta rápidas. De forma predeterminada, el factor multitransmisión (o sea, la cantidad de agentes que envían datos a una única cinta) está configurado en dos. Lo puede aumentar hasta diez.

El multiplex es útil para entornos grandes con muchas operaciones de copia de seguridad. No mejora el rendimiento de una copia de seguridad simple.

Para alcanzar la máxima velocidad de copia de seguridad en un entorno grande, debe analizar el rendimiento de sus agentes, la red y las unidades de cinta. Entonces configure el factor multiplex adecuadamente, sin asignar un valor demasiado elevado. Por ejemplo, si sus agentes proporcionan datos a 70 Mbit/s, su unidad de cinta escribe a 250 Mbit/s y su red no presenta cuellos de botella,

configure el factor multiplex en tres. Configurar el factor multiplex en cuatro implicará un multiplex excesivo y el rendimiento de copia de seguridad disminuirá. El factor multiplex suele estar entre dos y cinco.

Por su estructura, las copias de seguridad multiplex son más lentas de recuperar. Cuanto mayor el factor multiplex, más lenta es la recuperación. No es compatible la recuperación simultánea de múltiples copias de seguridad escritas en una única cinta con multiplex.

Puede seleccionar una o diversas unidades de cinta para el multiplex o usar la opción multiplex con cualquier unidad de cinta disponible. El multiplex no está disponible unidades de cinta conectadas localmente.

No puede cambiar la configuración de multiplex de un plan de protección existente. Para usar una configuración diferente, cree un nuevo plan de protección.

En un plan de protección, son posibles estas combinaciones de multitransmisión y multiplex:

- **Tanto la opción de multitransmisión como la de multiplex están sin marcar.**
  Cada agente envía datos a una sola unidad de cinta.
- **Solo está seleccionada la opción de multitransmisión.**
  Cada agente envía datos a un mínimo de dos unidades de cinta simultáneamente.
- **Solo está seleccionada la opción de multiplex.**
  Cada agente envía datos a una unidad de cinta que acepta transmisiones de varios agentes simultáneamente. El número máximo de transmisiones que una unidad de cinta puede aceptar va en función del plan de protección y no se puede modificar sobre la marcha.
- **Tanto la opción de multitransmisión como la de multiplex están seleccionadas.**
  Cada agente envía datos a un mínimo de dos unidades de cinta que aceptan transmisiones de varios agentes simultáneamente.

Una unidad de cinta solo puede escribir un tipo de copia de seguridad a la vez (con o sin multiplex, en función de qué plan de protección haya empezado primero).

Usar juego de cintas en el grupo de cintas seleccionado para realizar copias de seguridad

El valor predeterminado es el siguiente: **Deshabilitado**.

Las cintas dentro de un grupo pueden agruparse en los llamados **juegos de cintas**.

Si deja esta opción deshabilitada, se realizará la copia de seguridad de los datos en todas las cintas que pertenezcan a un pool. Si esta opción se habilita, puede separar las copias de seguridad siguiendo reglas predefinidas o reglas personalizadas.

- **Usar un juego de cintas diferente para cada uno** (elija una regla: **tipo de copia de seguridad**, **tipo de dispositivo**, **nombre del dispositivo**, **día del mes**, **día de la semana**, **mes del año**, **año**, **fecha**).

Si selecciona esta variante, puede organizar los juegos de cintas siguiendo una regla predefinida. Por ejemplo, puede tener juegos de cintas distintos para cada día de la semana o guardar las copias de seguridad de cada equipo en un juego de cintas distinto.

- **Especificar una regla personalizada para juegos de cintas**

  Si selecciona esta variante, especifique su propia regla para organizar juegos de cintas. La regla puede incluir las variables siguientes:

Sintaxis de la variable	Descripción de la variable	Valores disponibles
`[Resource Name]`	Las copias de seguridad de cada equipo se almacenarán en un juego de cintas separado.	Nombres de los equipos registrados en el servidor de gestión.
`[Backup Type]`	Las copias de seguridad completas, incrementales y diferenciales se guardarán en juegos de cintas distintos.	`full`, `inc`, `diff`
`[Resource Type]`	Las copias de seguridad de los equipos de cada tipo se almacenarán en un juego de cintas distinto.	`Server essentials`, `Server`, `Workstation`, `Physical machine`, `VMware Virtual Machine`, `Virtual-PC Virtual Machine`, `Virtual Server Virtual Machine`, `Hyper-V Virtual Machine`, `Parallels Virtual Machine`, `XEN Virtual Machine`, `KVM Virtual Machine`, `RHEV Virtual Machine`, `Parallels Cloud Virtual Machine`
`[Day]`	Las copias de seguridad creadas cada día del mes se almacenarán en un juego de cintas separado.	`01`, `02`, `03`, ..., `31`
`[Weekday]`	Las copias de seguridad creadas cada día de la semana se almacenarán en un juego de cintas separado.	`Sunday`, `Monday`, `Tuesday`, `Wednesday`, `Thursday`, `Friday`, `Saturday`
`[Month]`	Las copias de seguridad creadas durante cada mes del año se almacenarán en un juego de cintas separado.	`January`, `February`, `March`, `April`, `May`, `June`, `July`, `August`, `September`, `October`, `November`, `December`
`[Year]`	Las copias de seguridad creadas cada año se almacenarán en un juego de cintas separado.	`2017`, `2018`...

- Por ejemplo, si especifica como regla `[Resource Name]-[Backup Type]`, tendrá un juego de cintas distinto para cada copia de seguridad completa, incremental y diferencial de cada equipo al que

se aplique el plan de protección.

También puede especificar juegos de cintas para cintas individuales. En tal caso, el software escribirá primero las copias de seguridad en las cintas cuyo valor de juego de cintas coincida con el valor de la expresión especificada en el plan de protección. Luego, si es necesario, se escribirán otras cintas del mismo pool. Después de eso, si el pool es rellenable, se usarán las cintas del pool de **Cintas disponibles**.

Por ejemplo, si especifica el juego de cintas `Monday` para Cinta 1, `Tuesday` para Cinta 2, etc. y especifica `[Weekday]` en las opciones de copia de seguridad, se usará la cinta correspondiente al día de la semana en cuestión.

Manejo de fallos de la tarea

Esta acción determina el comportamiento del programa cuando falle la ejecución planificada de un plan de protección. Esta opción no se aplica si se inicia un plan de protección manualmente.

Si esta opción está habilitada, el programa intentará ejecutar de nuevo el plan de protección. Puede especificar el número de intentos y el intervalo de tiempo entre los intentos. El programa dejará de intentar tan pronto como un intento finalice correctamente o se haya realizado el número de intentos especificados, lo que suceda primero.

El valor predeterminado es el siguiente: **Deshabilitado**.

Condiciones de inicio de la tarea

Esta opción es eficaz tanto para los sistemas operativos de Windows como de Linux.

Esta opción determina el comportamiento del programa si hay una tarea que esté a punto de iniciarse (cuando llegue el momento programado o cuando ocurra el evento especificado en el programa), pero no se cumple con la condición (o cualquiera de las condiciones). Para obtener más información acerca de las condiciones, consulte "Condiciones de inicio".

El valor predeterminado es el siguiente: **Esperar hasta que se cumplan las condiciones de la planificación**.

Esperar hasta que se cumplan las condiciones de la planificación

Con esta configuración, el Programador comienza a supervisar las condiciones e inicia la tarea cuando se cumplen las condiciones. Si no se cumplen las condiciones, la tarea no comenzará nunca.

Para manejar la situación cuando no se cumplen con las condiciones por mucho tiempo y el retraso de la tarea se vuelve peligroso, puede definir el intervalo en el cual la tarea se ejecutará independientemente de la condición. Seleccione la casilla de verificación **Ejecutar la tarea de todos modos después** y especifique el intervalo de tiempo. La tarea comenzará tan pronto como se cumpla con las condiciones O pase el período máximo de tiempo, lo que suceda primero.

Omitir la ejecución de tarea

El retraso de una tarea puede ser inadmisible, por ejemplo, cuando necesite ejecutar una tarea estrictamente a la hora especificada. Entonces parece sensato omitir la tarea en vez de esperar a que se cumplan las condiciones, en especial si las tareas son frecuentes.

Servicio de instantáneas de volumen (VSS)

Esta opción es eficaz solo en los sistemas operativos de Windows.

La opción define si un proveedor de servicio de instantáneas de volumen de Microsoft (VSS) debe notificar a las aplicaciones compatibles con VSS que se comenzará a realizar la copia de seguridad. Esto garantiza el estado coherente de todos los datos que usan las aplicaciones, en particular la finalización de todas las transacciones de bases de datos en el momento en que el software de copia de seguridad realiza la instantánea de los datos. En cambio, la consistencia de los datos garantiza que la aplicación se recuperará en el estado correcto y será operativa inmediatamente después de la recuperación.

La instantánea se utiliza solo durante la operación de copia de seguridad y se elimina automáticamente cuando se completa dicha operación. No se conservan archivos temporales.

El valor predeterminado es el siguiente: **Habilitado**. **Seleccione automáticamente el proveedor de instantáneas**.

Puede seleccionar una de las siguientes opciones:

- **Seleccione automáticamente el proveedor de instantáneas**
  Seleccione automáticamente entre el proveedor de instantáneas de hardware, los proveedores de instantáneas de software y Microsoft Software Shadow Copy Provider.
- **Usar Microsoft Software Shadow Copy Provider**
  Recomendamos seleccionar esta opción cuando realice una copia de seguridad de los servidores de la aplicación (Microsoft Exchange Server, Microsoft SQL Server, Microsoft SharePoint o Active Directory).

Deshabilite esta opción si la base de datos es incompatible con VSS. Las instantáneas se realizan con más rapidez, pero no es posible garantizar la coherencia de los datos de aplicaciones cuyas transacciones no se hayan completado en el momento de la toma de la instantánea. Puede usar los comandos previos o posteriores a la captura de datos para garantizar que se haga una copia de seguridad de los datos con un estado coherente. Por ejemplo, especifique los comandos de captura anterior a los datos que suspenderán la base de datos y vacía la memoria caché para garantizar que se completen todos las transacciones, y especificar los comandos Post de la captura de datos que reanudarán las operaciones después de tomar las instantáneas.

Nota
Si se habilita esta opción, no se crearán copias de seguridad de las carpetas ni de los archivos especificados en la clave de registro **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToSnapshot**. En concreto, no se crean copias de seguridad de los archivos de datos fuera de línea de Outlook (.ost), porque se especifican en el valor **OutlookOST** de esta clave.

Habilitar la copia de seguridad completa de VSS

Al habilitar esta opción, se truncarán los registros de Microsoft Exchange Server y de las demás aplicaciones compatibles con VSS (excepto para Microsoft SQL Server) después de cada copia de seguridad completa, incremental o diferencial a nivel de disco.

El valor predeterminado es el siguiente: **Deshabilitado**.

Mantenga esta opción deshabilitada en los siguientes casos:

- Si utiliza Agent for Exchange o un software de terceros para realizar una copia de seguridad de los datos de Exchange Server. Esto se debe a que el truncamiento de registros interferirá con las copias de seguridad consecutivas de los registros de las transacciones.
- Si utiliza un software de terceros para realizar una copia de seguridad de los datos de SQL Server. El motivo es que el software de terceros tomará la copia de seguridad a nivel de discos resultante para su "propia" copia de seguridad completa. Como consecuencia, no se podrá realizar la siguiente copia de seguridad diferencial de los datos de SQL Server. No se podrán realizar copias de seguridad hasta que el software de terceros cree la siguiente copia de seguridad completa "propia".
- Si en el equipo se están ejecutando otras aplicaciones que reconocen la característica VSS y debe mantener sus registros por cualquier motivo.

Al habilitar esta opción, no se truncan los registros de Microsoft SQL Server. Para truncar el registro de SQL Server después de una copia de seguridad, habilite la opción de copia de seguridad Truncamiento de registros.

Volume Shadow Copy Service (VSS) para equipos virtuales

Esta opción señala si se van a realizar instantáneas inactivas de los equipos virtuales. Para realizar una instantánea inactiva, el software de copia de seguridad aplica VSS dentro de un equipo virtual usando las herramientas de VMware o Hyper-V Integration Services.

El valor predeterminado es el siguiente: **Habilitado**.

Si esta opción está habilitada, las transacciones de todas las aplicaciones compatibles con VSS y que ejecutan un equipo virtual se completan antes de realizar la instantánea. Si una instantánea inactiva falla tras el número de reintentos indicado en la opción "Manejo de errores" y la copia de seguridad de aplicaciones está deshabilitada, se realiza una copia de seguridad activa. Si la copia de seguridad de aplicaciones está habilitada, la copia de seguridad falla.

Si esta opción está deshabilitada, se realiza una instantánea activa. Se hará una copia de seguridad del equipo virtual en un estado de coherencia con bloqueos. Le recomendamos que tenga activada esta opción en todo momento, incluso para las máquinas virtuales que no ejecutan aplicaciones compatibles con VSS. De lo contrario, ni siquiera se puede garantizar la coherencia del sistema de archivos dentro de la copia de seguridad capturada.

Nota
Esta opción no afecta a los equipos virtuales de Scale Computing HC3. En estos equipos, la inactividad depende de si las herramientas de Scale están instaladas en el equipo virtual o no.

Copia de seguridad semanal

Esta opción determina las copias de seguridad que se consideran "semanales" en las reglas de retención y los esquemas de copias de seguridad. Una copia de seguridad "semanal" es la primera copia de seguridad creada una vez comenzada la semana.

El valor predeterminado es el siguiente: **Lunes**.

Registro de eventos de Windows

Esta opción sólo funciona en los sistemas operativos de Windows.

Esta opción define si los agentes tienen que recopilar los eventos de las operaciones de copia de seguridad en el registro de eventos de aplicación de Windows (para ver este registro, ejecute eventvwr.exe o seleccione **Panel de control** > **Herramientas administrativas** > **Visor de eventos**). Puede filtrar los sucesos a ser recopilados.

El valor predeterminado es el siguiente: **Deshabilitado**.

Recuperación

Recuperación de apuntes

La siguiente tabla resume los métodos de recuperación disponibles. Use la tabla para elegir el método de recuperación que más le convenga.

Qué recuperar	Método de recuperación
Equipo físico (Windows o Linux)	Uso de la interfaz web Uso de dispositivos de arranque
Equipo físico (Mac)	Uso de dispositivos de arranque
Equipo virtual (VMware, Hyper-V o Scale Computing HC3)	Uso de la interfaz web Uso de dispositivos de arranque
Configuración de ESXi	Uso de dispositivos de arranque
Archivos/Carpetas	Uso de la interfaz web 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 interfaz web
Bases de datos SQL	Uso de la interfaz web
Bases de datos de Exchange	Uso de la interfaz web
Buzones de correo de Exchange	Uso de la interfaz web
Buzones de correo de Microsoft 365	Uso de la interfaz web
Bases de datos de Oracle	Uso de la herramienta Oracle Explorer

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

Una imagen de la que se haya creado una copia de seguridad en un sistema operativo podría estar infectada con un malware y reinfectar el equipo que se está recuperando.

La recuperación segura sirve para evitar que se repitan estas infecciones. Para ello emplea el análisis antimalware y la eliminación de malware integrados durante el proceso de recuperación.

Limitaciones:

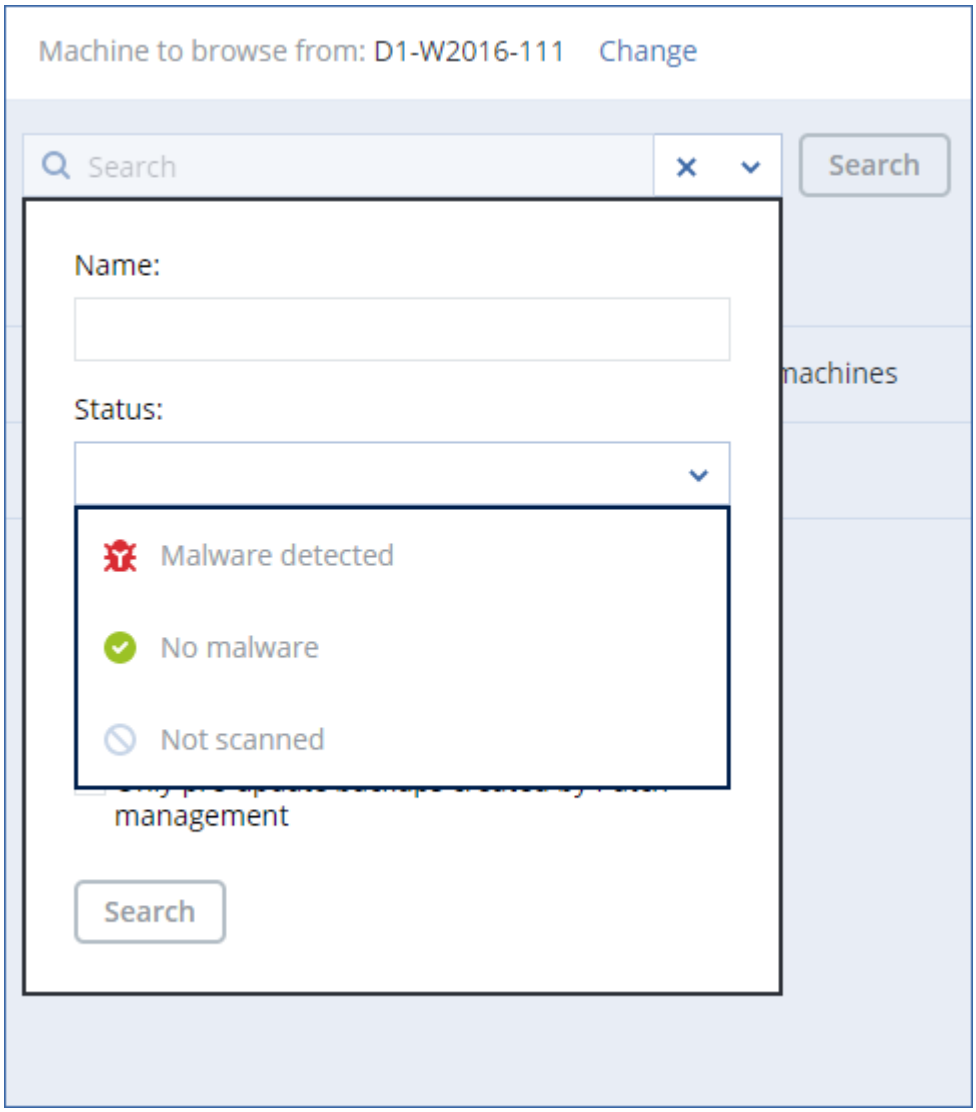
- La recuperación segura es compatible únicamente con equipos físicos y virtuales Windows en los que esté instalado el agente para Windows.
- Solo son compatibles las copias de seguridad de tipo **Todo el equipo** o **Discos/volúmenes**.
- Solo son compatibles volúmenes con el sistema de archivos NTFS. Las particiones que no son NTFS se recuperarán sin realizar ningún análisis antimalware.
- La recuperación segura no es compatible con las copias de seguridad de la protección de datos continua (CDP). Un equipo se recuperará en función de la última copia de seguridad regular sin los datos de la copia de seguridad de la CDP. Para recuperar los datos de la CDP, ejecute una recuperación de **archivos/carpetas**.

Cómo funciona

Si habilita la opción de recuperación segura durante el proceso de recuperación, el sistema llevará a cabo las siguientes acciones:

1. Al analizar la copia de seguridad de imágenes en busca de malware y marcar los archivos infectados. A la copia de seguridad se le asignará uno de los siguientes estados:
   - **Sin malware**: no se ha detectado malware durante el análisis de la copia de seguridad.
   - **Malware detectado**: se ha detectado malware durante el análisis de la copia de seguridad.
   - **No analizado**: la copia de seguridad no se ha analizado en busca de malware.
2. Recuperar la copia de seguridad en el equipo seleccionado.
3. Eliminar el malware detectado.

Puede filtrar las copias de seguridad usando el parámetro **Estado**.



Crear dispositivos de inicio

El dispositivo de inicio es un CD, DVD, unidad flash USB u otro dispositivo extraíble que le permite ejecutar el Agente sin la ayuda de un sistema operativo. El objetivo principal del dispositivo de inicio es recuperar un sistema operativo que no se pueda iniciar.

Recomendamos especialmente que cree y compruebe un dispositivo de inicio en cuanto empiece a usar copias de seguridad a nivel de discos. Además, es conveniente volver a crear el dispositivo después de cada actualización importante del agente de protección.

Puede recuperar tanto Windows como Linux con el mismo dispositivo. Para recuperar macOS, cree un dispositivo independiente en un equipo que ejecute macOS.

Para crear dispositivos de inicio en Windows o Linux

1. Descargue el archivo ISO de dispositivo de arranque. Para descargar el archivo, haga clic en el icono de la cuenta en la esquina superior derecha > **Descargas** > **Dispositivo de arranque**.
2. Realice una de las siguientes operaciones:

- Grabe un CD/DVD utilizando el archivo ISO.
- Cree una unidad flash USB de arranque utilizando el archivo ISO y una de las muchas herramientas gratuitas disponibles en línea.

  Para iniciar un equipo UEFI, use `ISO a USB` o `RUFUS`. Para un equipo BIOS, use `Win32DiskImager`. En Linux, puede usar la utilidad `dd`.
- Conecte el archivo ISO como una unidad de CD/DVD al equipo virtual que desea recuperar.

Como alternativa, puede crear un dispositivo de arranque con Bootable Media Builder.

Para crear un dispositivo de arranque en macOS

1. En un equipo donde esté instalado Agente para Mac, haga clic en **Aplicaciones** > **Generador de Medios de rescate**.
2. El software muestra los dispositivos extraíbles conectados. Seleccione el que desee convertir en un dispositivo de inicio.

   Advertencia.
   Toda la información del disco se borrará.
3. Haga clic en **Crear**.
4. Espere mientras el software crea el dispositivo de inicio.

Recuperar un equipo

Recuperación en un equipo físico

En esta sección se describe cómo recuperar un equipo físico mediante la consola web de Cyber Protect.

Use el dispositivo de arranque en vez de la consola web de Cyber Protect si necesita recuperar cualquiera de los siguientes:

- Un sistema operativo macOS
- 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.

Es necesario reiniciar para la recuperación de un sistema operativo y de volúmenes que están cifrados con BitLocker o CheckPoint. Para obtener más información, consulte "Recuperación con reinicio" (p. 371).

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.

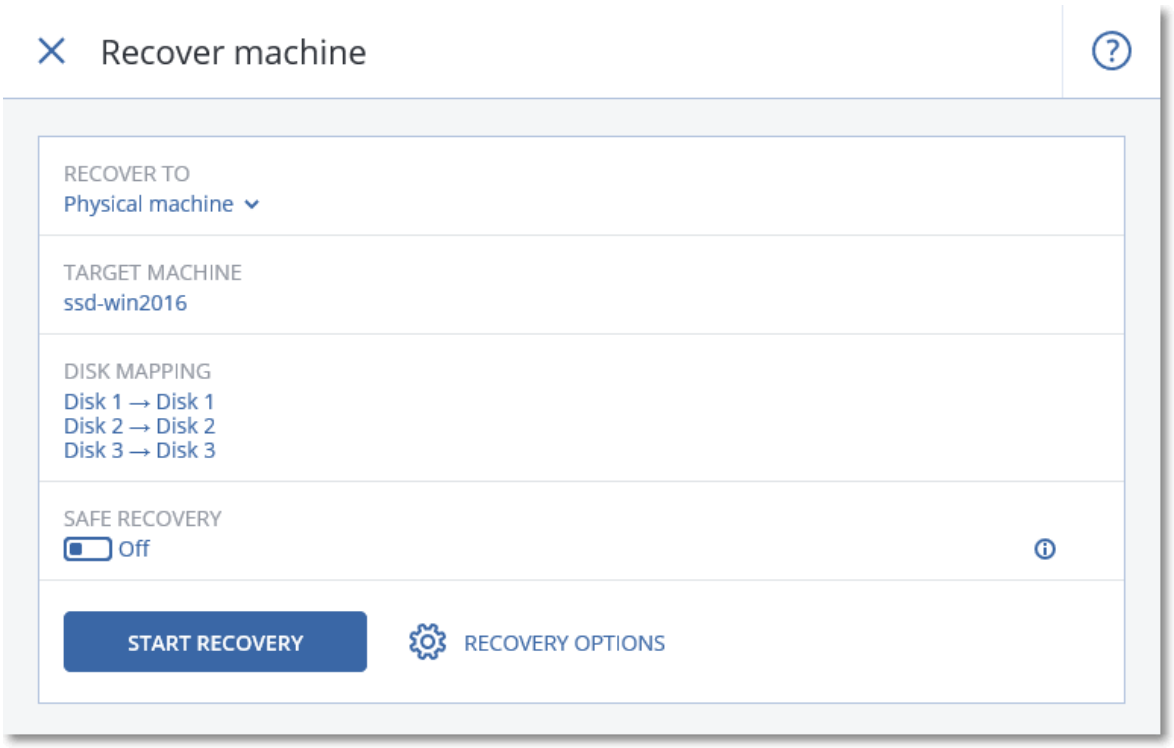
   Si el equipo no está conectado a Internet, no se muestran los puntos de recuperación. Realice una de las siguientes operaciones:

   - 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**.

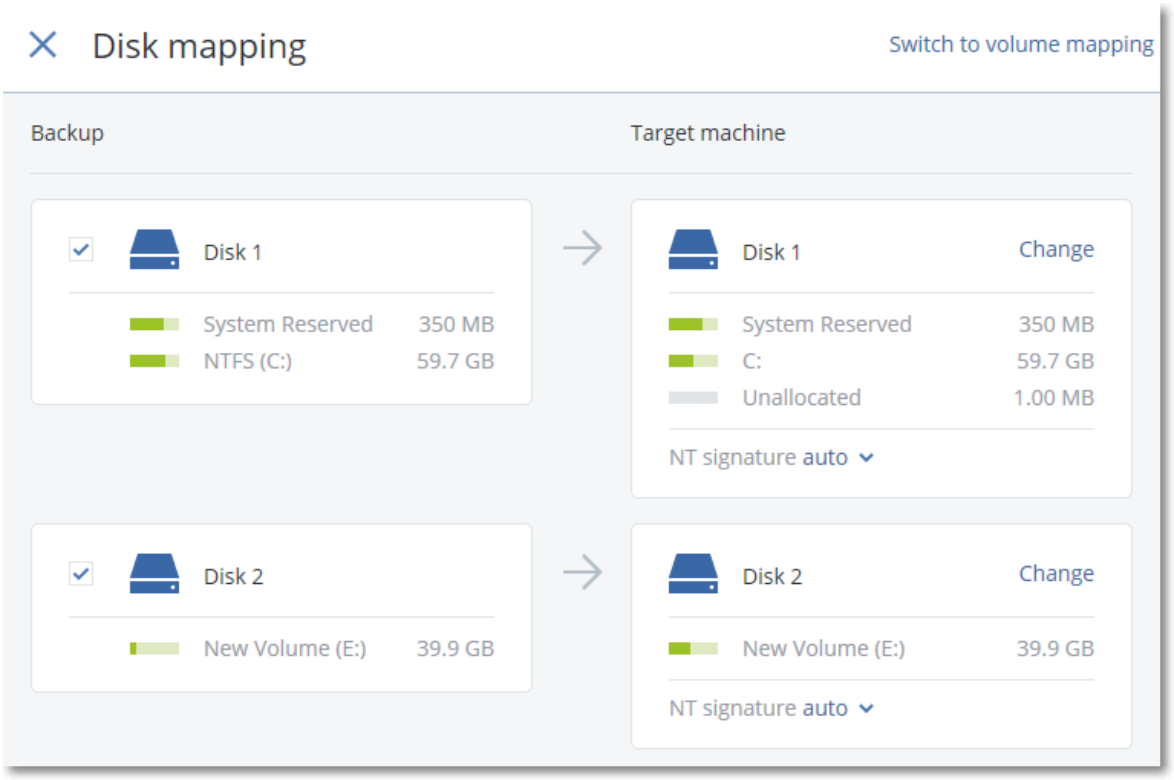
   El software asigna automáticamente los discos de las copias de seguridad a los discos del equipo de destino.

   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 discos** puede volver a asignar los discos manualmente.

   De manera adicional, en la sección de asignación, puede elegir discos o volúmenes individuales para la recuperación. Podrá cambiar entre recuperar discos y volúmenes utilizando el enlace **Cambiar a...** ubicado en la esquina posterior derecha.



6. [Opcional] Habilite el conmutador **Recuperación segura** para analizar la copia de seguridad en busca de malware. Si se detecta algún malware, se marcará en la copia de seguridad y se eliminará en cuanto termine el proceso de recuperación.
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**.

Recuperación de un equipo físico en una máquina virtual

Puede recuperar una copia de seguridad de un equipo físico en una máquina virtual.

Es posible recuperar en una máquina virtual si hay instalado por lo menos un agente para el correspondiente hipervisor de destino en su entorno y se ha registrado en el servidor de administración. Por ejemplo, para la recuperación en VMware ESXi, se necesita que el agente para VMware esté instalado en el entorno y registrado en el servidor de administración.

Algunas opciones solo están disponibles con el despliegue en la nube.

Para obtener más información sobre las rutas compatibles para la migración de equipos físicos en máquinas virtuales (P2V), consulte "Migración de equipos" (p. 567).

Nota
No puede recuperar copias de seguridad de equipos físicos de macOS como 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.

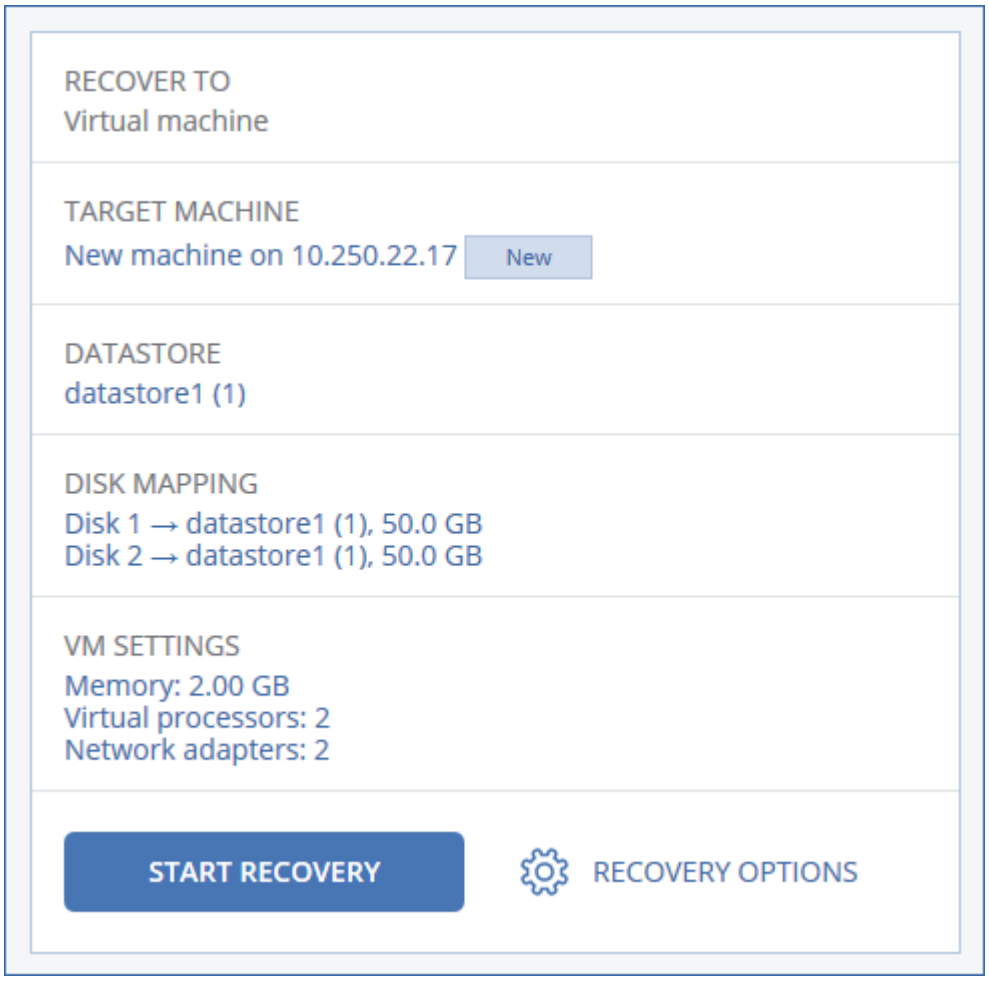
   Si el equipo no está conectado a Internet, no se muestran los puntos de recuperación. Realice una de las siguientes operaciones:
   - Si la ubicación de la copia de seguridad se encuentra en la nube o en un almacenamiento compartido (es decir, otros agentes pueden acceder a ella), haga clic en **Seleccionar equipo**, seleccione un equipo que esté en línea y luego 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 y volúmenes usando dispositivos de arranque" (p. 372).
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 ese hipervisor instalado en su entorno y registrado en el servidor de administración.

   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 la máquina virtual** y luego seleccione **Variante**. De manera opcional, puede cambiar el tamaño de la memoria, el número de procesadores y las conexiones de red de la máquina virtual.
8. [Opcional] [Durante la recuperación a un nuevo equipo] Configure las opciones de recuperación adicionales que necesita:
   - [No disponible para Virtuozzo Hybrid Infrastructure ni para Scale Computing HC3] Haga clic en **Almacén de datos** para ESXi, **Ruta** para Hyper-V y Virtuozzo o **Dominio de almacenamiento** para Red Hat Virtualization (oVirt). A continuación, seleccione el almacén de datos (almacenamiento) para la máquina virtual.
   - Para seleccionar el almacén de datos (almacenamiento), la interfaz y el modo de aprovisionamiento para cada unidad de disco virtual, haga clic en **Asignación de discos**. En la sección de asignación, puede elegir discos individuales para la recuperación.

Nota
No puede modificar esta configuración si está recuperando un contenedor de Virtuozzo o una máquina 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**.

- [Disponible para VMware ESXi, Hyper-V, Virtuozzo y Red Hat Virtualization/oVirt] Para cambiar el tamaño de la memoria, el número de procesadores y las conexiones de red del equipo virtual, haga clic en **Configuración de máquina virtual**.



9. Haga clic en **Iniciar recuperación**.
10. [Al realizar la recuperación en una máquina 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 una copia de seguridad de una máquina virtual a un equipo físico o a otra máquina virtual.

Es posible recuperar en una máquina virtual si hay instalado por lo menos un agente para el correspondiente hipervisor de destino en su entorno y se ha registrado en el servidor de administración. Por ejemplo, para la recuperación en VMware ESXi, se necesita que el agente para VMware esté instalado en el entorno y registrado en el servidor de administración.

Algunas opciones solo están disponibles con el despliegue en la nube.

Para obtener más información sobre las rutas compatibles para la migración de máquinas virtuales a equipos físicos (V2P) o de máquinas virtuales a virtuales (V2V), consulte "Migración de equipos" (p. 567).

Nota
No puede recuperar máquinas virtuales macOS en servidores Hyper-V porque Hyper-V no es compatible con macOS. Puede recuperar equipos virtuales MacOS en un servidor VMware que esté instalado en un hardware de Mac.

Importante
Una máquina virtual debe estar parada cuando recupera otra máquina en esta. 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**).

Para recuperar un equipo virtual

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. [Durante la recuperación en un equipo físico] En **Recuperar en**, seleccione **Equipo físico**.
   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 en "Recuperación en un equipo físico" (p. 364). En caso contrario, le recomendamos que realice la migración virtual a físico (V2P) mediante un soporte de arranque.
4. [Opcional] De manera predeterminada, se selecciona 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.

Nota
Debe haber al menos un agente para ese hipervisor instalado en su entorno y registrado en el servidor de administración.

b. Seleccione si desea realizar la recuperación en un equipo nuevo o en otro ya existente.

c. Seleccione el host y especifique el nuevo nombre de equipo, o bien seleccione un equipo de destino existente.

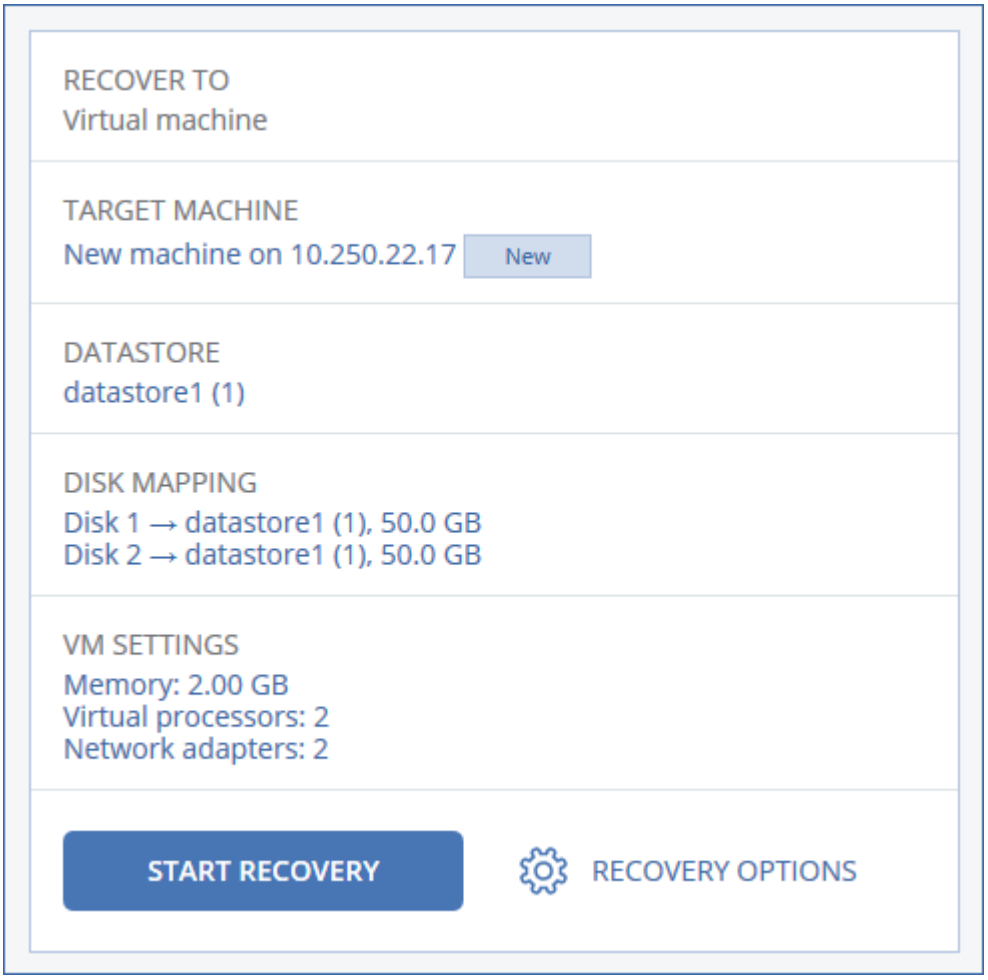
d. Haga clic en **Aceptar**.

5. [Para Virtuozzo Hybrid Infrastructure] Haga clic en **Configuración de la máquina virtual** y luego seleccione **Variante**. De manera opcional, puede cambiar el tamaño de la memoria, el número de procesadores y las conexiones de red de la máquina virtual.
6. [Opcional] [Durante la recuperación a un nuevo equipo] Configure las opciones de recuperación adicionales que necesita:
   - [No disponible para Virtuozzo Hybrid Infrastructure ni para Scale Computing HC3] Haga clic en **Almacén de datos** para ESXi, **Ruta** para Hyper-V y Virtuozzo o **Dominio de almacenamiento** para Red Hat Virtualization (oVirt). A continuación, seleccione el almacén de datos (almacenamiento) para la máquina virtual.
   - Para seleccionar el almacén de datos (almacenamiento), la interfaz y el modo de aprovisionamiento para cada unidad de disco virtual, haga clic en **Asignación de discos**. En la sección de asignación, puede elegir discos individuales para la recuperación.

     Nota
     No puede modificar esta configuración si está recuperando un contenedor de Virtuozzo o una máquina 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**.

   - [Disponible para VMware ESXi, Hyper-V, Virtuozzo y Red Hat Virtualization/oVirt] Para cambiar el tamaño de la memoria, el número de procesadores y las conexiones de red del equipo

virtual, haga clic en **Configuración de máquina virtual**.



7. Haga clic en **Iniciar recuperación**.
8. [Al realizar la recuperación en una máquina virtual existente] Confirme que desea sobrescribir los discos.

El proceso de recuperación se muestra en la pestaña **Actividades**.

Recuperación con reinicio

Es necesario reiniciar al recuperar lo siguiente:

- Un sistema operativo
- Volúmenes cifrados con BitLocker o CheckPoint

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

Requisitos

- La recuperación de los volúmenes cifrados requiere que haya un volumen no cifrado en el mismo equipo y que dicho volumen tenga al menos 1 GB de espacio libre. De lo contrario, la tarea de recuperación fallará.
- La recuperación de un volumen del sistema cifrado no requiere ninguna acción adicional. Para recuperar un volumen cifrado que no es del sistema, primero debe bloquearlo, por ejemplo, abriendo un archivo que resida en ese volumen. De lo contrario, la recuperación continuará sin reiniciarse y Windows podría no reconocer el volumen recuperado.

Solución de problemas

Si la recuperación falla y su equipo se reinicia con el error `No puede obtenerse el archivo de la partición`, deshabilite el arranque seguro. Para obtener más información sobre cómo hacerlo, consulte Deshabilitación del arranque seguro en la documentación de Microsoft.

Recuperar discos y volúmenes usando dispositivos de arranque

Para obtener información sobre cómo crear dispositivos de inicio, consulte "Crear dispositivos de inicio" (p. 363).

Pasos para recuperar discos o volúmenes usando dispositivos de arranque

1. Inicie el equipo de destino usando dispositivos de arranque.
2. [Solo para macOS] Si recupera volúmenes 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. Vuelva a crear la configuración del disco original. Para obtener instrucciones, consulte https://support.apple.com/guide/disk-utility/welcome.
   c. Haga clic en **Disk Utility** > **Salir de Disk Utility**.

   Nota
   A partir de macOS 11 Big Sur, no se puede hacer copia de seguridad del volumen del sistema ni recuperarlo. Para recuperar un sistema macOS de arranque, debe recuperar el volumen de datos y, a continuación, instalar macOS en él.
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 nombre de servidor/dirección IP y puerto del servidor proxy. De lo contrario, omita este paso.
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 cloud**. Especifique las credenciales de la cuenta a la que está asignado el equipo del que se hizo la copia de seguridad.
   - Para recuperar datos desde una carpeta local o de red, vaya a la carpeta ubicada en **Carpetas locales** o **Carpetas de red**.

   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 las copias de seguridad**, seleccione **Discos** o **Volúmenes** y, a continuación, seleccione los elementos que desea recuperar. Haga clic en **Aceptar** para confirmar su selección.

   Importante
   Si el equipo que se incluye en la copia de seguridad tiene discos dinámicos o volúmenes lógicos (LVM), seleccione **Volúmenes**.
10. 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.
11. [Solo para macOS] Para recuperar un volumen de datos con formato APFS como sistema macOS de arranque, en la **sección Instalación de macOS** deje seleccionada la casilla de verificación **Instalar macOS en el volumen de datos macOS recuperado**.

    Tras la recuperación, el sistema se reinicia y la instalación de macOS empieza automáticamente. Necesita una conexión a internet para que el programa de instalación descargue los archivos necesarios.

    Si no necesita recuperar el volumen de datos con formato APFS como sistema de arranque, quite la marca de la casilla de verificación **Instalar macOS en el volumen de datos macOS recuperado**. Todavía podrá convertirlo en volumen de arranque más tarde instalándole macOS de forma manual.
12. [Solo para Linux] Si el equipo que se incluye en la copia de seguridad tiene volúmenes lógicos (LVM) y desea 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.

c. Confirme su elección.

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 usando la interfaz web

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 uno de los siguientes procedimientos:

   - [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 búsqueda para obtener la lista de archivos y carpetas deseados.

   Puede utilizar uno o más caracteres comodín (* y ?). Para obtener más información sobre el uso de los caracteres comodín, consulte la sección "Filtros de archivo".

   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.

8. Haga clic en **Recuperar**.

   En **Recuperar en**, verá una de las opciones siguientes:

   - El equipo que contenía originalmente los archivos que quiere recuperar (si hay un agente instalado en este equipo).
   - El equipo donde está instalado Agente para VMware, Agente para Hyper-V o Agente para Scale Computing HC3 (si los archivos proceden de un equipo virtual ESXi, Hyper-V o Scale Computing HC3).

   Este es el equipo de destino para la recuperación. Si es necesario, puede seleccionar otro equipo.

9. En **Ruta**, seleccione el destino de la recuperación. Puede seleccionar una de las siguientes opciones:

   - La ubicación original (al recuperar en el equipo original)
   - Una carpeta local de un equipo de destino

     Nota
     No se pueden usar vínculos simbólicos.

   - Una carpeta de red accesible desde el equipo de destino

10. Haga clic en **Iniciar recuperación**.

11. Seleccione una de las opciones de sobreescritura de archivos:

    - **Sobrescribir archivos existentes**
    - **Sobrescribir un archivo existente si es más antiguo**
    - **No sobrescribir archivos existentes**

El proceso de recuperación se muestra en la pestaña **Actividades**.

Descargar archivos del almacenamiento en la cloud

En la consola de Web Restore, puede navegar por el almacenamiento en la nube, ver el contenido de las copias de seguridad, y descargar archivos y carpetas con copia de seguridad.

No puede navegar por las copias de seguridad del estado del sistema, las bases de datos SQL ni las bases de datos de Exchange.

No puede descargar discos con copia de seguridad, volúmenes ni puntos de recuperación completos.

Para descargar archivos y carpetas del almacenamiento en la nube

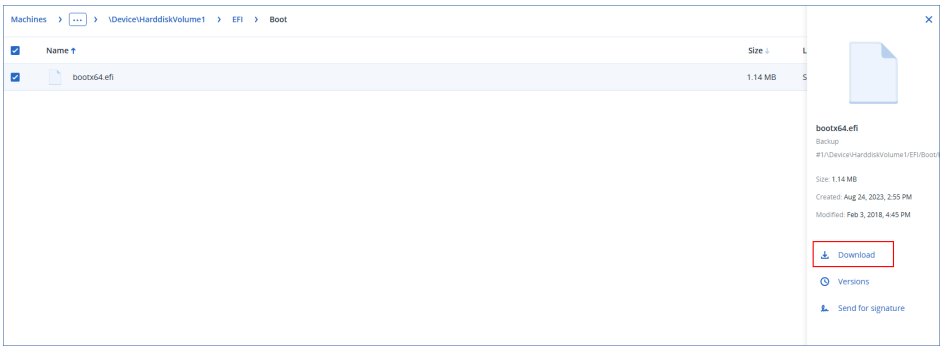
1. Inicie sesión en su cuenta de Acronis en https://account.acronis.com.
2. En la consola de Cyber Protect, seleccione la carga de trabajo requerida y haga clic en **Recuperación**.

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**.
5. [Si se le solicita] Inicie sesión en la consola de Cyber Protect Cloud utilizando las credenciales de su cuenta de Acronis.
6. 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).
7. 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.
8. Seleccione las casillas de verificación junto a los elementos que desee descargar.

   Nota
   Si selecciona varios elementos, se descargarán como archivo ZIP.

9. 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

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 web".
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 inicio, 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 nombre de servidor/dirección IP y puerto del servidor proxy. De lo contrario, omita este paso.
4. En la pantalla de inicio, haga clic en **Recuperar**.
5. Haga clic en **Seleccionar datos** y después haga clic en **Examinar**.
6. Especifique la ubicación de la copia de seguridad:
   - Para recuperar datos desde un almacenamiento en la cloud, seleccione **Almacenamiento en la cloud**. Especifique las credenciales de la cuenta a la que está asignado el equipo del que se hizo la copia de seguridad.
   - Para recuperar datos desde una carpeta local o de red, vaya a la carpeta ubicada en **Carpetas locales** o **Carpetas de red**.

   Haga clic en **Aceptar** para confirmar su selección.
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. En **Contenido de la copia de seguridad**, seleccione **Carpetas/archivos**.

9. Seleccione los datos que desea recuperar. Haga clic en **Aceptar** para confirmar su selección.
10. En **Dónde recuperar**, especifique una carpeta. Opcionalmente, puede prohibir la sobrescritura de versiones de archivos más recientes o excluir algunos archivos de la recuperación.
11. [Opcional] Haga clic en **Opciones de recuperación** para especificar configuraciones adicionales.
12. Haga clic en **Aceptar** para comenzar la recuperación.

Nota
La ubicación de cinta ocupa mucho espacio y podría no adecuarse a la RAM cuando lleve a cabo de nuevo el análisis y la recuperación con un dispositivo de arranque Linux y uno WinPE. Para Linux, debe montar otra ubicación para guardar los datos en el disco o recurso compartido. Consulte Acronis Cyber Backup Advanced: Cambiar la carpeta de ubicación de cinta (KB 27445). Para Windows PE, no hay ninguna solución alternativa en estos momentos.

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.
- Debe instalarse un agente de protección en el equipo desde donde buscará una copia de seguridad.
- 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+.
- La copia de seguridad debe almacenarse en una carpeta local o una red compartida (SMB/CIFS).

Para extraer archivos desde una copia de seguridad

1. Busque la ubicación de la copia de seguridad utilizando el Explorador de archivos.
2. Haga doble clic en el archivo de copia de seguridad. Los nombres de los archivos se basan en la siguiente plantilla:
   `<machine name> - <protection plan GUID>`
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.

Recuperación del estado del sistema

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 arranque, consulte "Crear dispositivos de arranque".

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 HC3	Windows
Validación de la copia de	+	+	+	+	+	+	+	+	+

seguridad									
Modo de arranque	+	-	-	-	-	-	-	+	-
Fecha y hora de los archivos	-	-	-	+	+	+	+	-	-
Manejo de errores	+	+	+	+	+	+	+	+	+
Exclusiones de archivos	-	-	-	+	+	+	+	-	-
Flashback	+	+	+	-	-	-	-	+	-
Recuperación de ruta completa	-	-	-	+	+	+	+	-	-
Puntos de montaje	-	-	-	+	-	-	-	-	-
Rendimiento	+	+	-	+	+	+	-	+	+
Comandos previos/posteriores	+	+	-	+	+	+	-	+	+
Cambios en el identificador de seguridad (SID)	+	-	-	-	-	-	-	-	-
Gestión de energía de VM	-	-	-	-	-	-	-	+	-
"Gestión de cintas" (p. 392) > Utilizar caché de disco para	-	-	-	+	+	+	-	-	-

acelerar la recuperación									
Registro de eventos de Windows	+	-	-	+	-	-	-	Solo Hyper-V	+
Encender después de la recuperación	-	-	-	-	-	-	+	-	-

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**.

La validación calcula una suma de comprobación por cada bloque de datos guardado en la copia de seguridad. La única excepción es la validación de las copias de seguridad a nivel de archivo que se encuentran en el almacenamiento en la nube. Estas copias de seguridad se validan comprobando la coherencia de la metainformación guardada en la copia de seguridad.

La validación lleva bastante tiempo, incluso cuando se trata de copias de seguridad incrementales o diferenciales, que son de pequeño tamaño. Esto se debe a que la operación valida no solo los datos contenidos físicamente en la copia de seguridad, sino también todos los datos recuperables al seleccionar la copia de seguridad. Esto exige acceso a las copias de seguridad creadas anteriormente.

Nota
La validación está disponible para un almacenamiento en la nube ubicado en un centro de datos de Acronis y proporcionado por partners de Acronis.

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**.

Manejo 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.

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 datos en el mismo disco de la copia de seguridad, sobre todo si el diseño del volumen del disco no ha cambiado. Los datos se comparan en el nivel de bloque.

En equipos físicos, comparar datos en el nivel de bloques es una operación laboriosa. Si la conexión al almacenamiento de copias de seguridad es rápida, llevará menos tiempo recuperar todo el disco que calcular las diferencias de datos. Por tanto, se recomienda habilitar esta acción únicamente si la conexión al almacenamiento de copias de seguridad es lenta (por ejemplo, si la copia de seguridad está almacenada en un almacenamiento en la cloud o en una carpeta de red remota).

Al recuperar un equipo físico, el preajuste depende de la ubicación de la copia de seguridad:

- Si la ubicación de copia de seguridad es un almacenamiento en la cloud, el preajuste es: **Habilitado**.
- Para otras ubicaciones de copia de seguridad, el preajuste 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 **Realizado**.

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 **Realizado**.

Nota
No se ejecutará un comando de recuperación posterior si la recuperación sucede como reinicio.

Gestión de cintas

Puede utilizar las siguientes opciones de recuperación de gestión de cintas.

Utilizar caché de disco para acelerar la recuperación

El valor predeterminado es el siguiente: **Deshabilitado**.

Le recomendamos encarecidamente que utilice la opción **Utilizar caché de disco para acelerar la recuperación** cuando recupere archivos desde un archivo comprimido de imagen. De lo contrario, la operación de restauración podría llevar mucho tiempo. Con esta opción, la lectura de cintas se lleva a cabo de forma secuencial, sin interrupciones ni rebobinado.

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 o Agente para Scale Computing HC3 realizan la recuperación en un equipo virtual.

El valor predeterminado es el siguiente: **Deshabilitado**.

El software puede generar un identificador de seguridad (SID del equipo) único para el sistema operativo recuperado. Solo necesita esta opción para garantizar la operatividad del software de terceros que depende del SID del equipo.

Microsoft no ofrece soporte técnico para cambiar el SID de un sistema implementado o recuperado. Deberá usar esta opción bajo su propia cuenta y riesgo.

Gestión de energía de VM

Estas opciones son efectivas cuando Agente para VMware, Agente para Hyper-V o Agente para Scale Computing HC3 realizan la recuperación en un equipo 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**.

Encender después de la recuperación

Esta opción está disponible cuando se trabaja desde dispositivos de inicio.

El valor predeterminado es el siguiente: **Deshabilitado**.

Esta opción permite que el equipo se reinicie con el sistema operativo recuperado sin interacción con el usuario.

Recuperación ante desastres

Esta opción está disponible solamente en las implementaciones en la nube de Acronis Cyber Protect. Para obtener una descripción detallada de esta funcionalidad, consulte https://www.acronis.com/support/documentation/DisasterRecovery/index.html#43224.html.

Operaciones con copias de seguridad

Pestaña Almacenamiento de copias de seguridad

La pestaña **Almacenamiento de la copia de seguridad** muestra las copias de seguridad de todos los equipos que se han registrado en el servidor de gestión. Esto incluye equipos fuera de línea y equipos que ya no están registrados.

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. En una implementación en la nube, un administrador puede ver las copias de seguridad en nombre de cualquier cuenta que pertenezca al mismo grupo y a sus grupos secundarios. Esta cuenta se elige indirectamente en **Equipo desde el cual examinar**. La pestaña **Almacenamiento de copias de seguridad** muestra las copias de seguridad de todos los equipos que se han registrado a lo largo de la historia de una misma cuenta, al registrar este equipo.

Las ubicaciones de copia de seguridad que se usan en los planes de protección se añaden automáticamente a la pestaña **Almacenamiento de copias 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.

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 exporte las copias de seguridad o utilice la replicación de copia de seguridad en lugar de mover los archivos de copia de seguridad de forma manual.

Pasos para seleccionar un punto de recuperación desde la pestaña Almacenamiento de copias de seguridad

1. En la pestaña **Almacenamiento de copias 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:
   `<machine name> - <protection plan name>`
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.

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. De forma predeterminada, los nombres de los archivos se basan en la siguiente plantilla:

   `<machine name> - <protection plan GUID>`
3. Si la copia de seguridad está cifrada, introduzca la contraseña de cifrado. De lo contrario, omita este paso.

   El Explorador de archivos muestra los puntos de recuperación.
4. Haga doble clic en el punto de recuperación.

   El Explorador de archivos muestra los volúmenes objeto de la copia de seguridad.

   Nota
   Haga doble clic en un volumen para buscar su contenido. Puede copiar archivos y carpetas desde la copia de seguridad a cualquier carpeta del sistema de archivos.
5. Haga clic con el botón derecho en un volumen que desee montar y, a continuación, haga clic en uno de los siguientes:
   - **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.
   - **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. 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

La validación es una operación que verifica la posibilidad de recuperación de datos en una copia de seguridad. Para obtener más información sobre esta operación, consulte "Validación" (p. 406).

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 Almacenamiento de copia de seguridad. Para obtener más información sobre las copias de seguridad ahí, consulte "Pestaña Almacenamiento de copias de seguridad" (p. 396).
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 se especifique. La copia de seguridad original permanece intacta. La exportación le permite separar una copia de seguridad específica de una cadena de copias de seguridad incrementales y diferenciales para una rápida recuperación, escribir sobre dispositivos extraíbles u otros propósitos.

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.

El nombre del archivo de la copia de seguridad de una copia de seguridad exportada depende del valor de la opción formato de copia de seguridad:

- Para el formato **Versión 12** con cualquier esquema de copias de seguridad, el nombre del archivo de la copia de seguridad 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.
- Para el formato **Versión 11** con el esquema de copias de seguridad **Siempre incremental (archivo único)**, el nombre del archivo de la copia de seguridad coincide exactamente con el nombre del archivo de copia de seguridad de la copia de seguridad original. Si se exportan varias copias de seguridad de la misma cadena de copia de seguridad en la misma ubicación, en cada operación de exportación se sobrescribe la copia de seguridad exportada previamente.
- Para el formato **Versión 11** con otro esquema de copias de seguridad, el nombre del archivo de la copia de seguridad es el mismo que el de la copia de seguridad original, excepto en la marca de hora y fecha. Las marcas de tiempo de las copias de seguridad exportadas hacen referencia al momento en que se realizó la exportación.

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 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.
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

Advertencia.
Al eliminar una copia de seguridad, todos sus datos se borran permanentemente. Los datos eliminados no se pueden recuperar.

Para eliminar las copias de seguridad de un equipo que esté conectado y presente en la consola web de Cyber Protect

1. En la pestaña **Todos los dispositivos**, seleccione el equipo del que desee eliminar las copias de seguridad.
2. Haga clic en **Recuperación**.
3. Seleccione la ubicación en la que se encuentran las copias de seguridad que desea borrar.
4. Realice uno de los siguientes procedimientos:
   - Para eliminar una sola copia de seguridad, seleccione la que desea eliminar y haga clic en el icono de engranaje y, a continuación, en **Eliminar**.
   - Para eliminar todas las copias de seguridad de la ubicación seleccionada, haga clic en **Eliminar todo**.
5. Confirme su decisión.

Para eliminar las copias de seguridad de cualquier equipo

1. En la pestaña **Almacenamiento de copias de seguridad**, seleccione la ubicación en la que desea eliminar 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:

   ```
   <machine name> - <protection plan name>
   ```
2. Seleccione un grupo.
3. Realice uno de los siguientes procedimientos:
   - Para eliminar una sola copia de seguridad, haga clic en **Mostrar copias de seguridad**, seleccione la que desea eliminar y haga clic en el icono de engranaje y, a continuación, en **Eliminar**.
   - Para eliminar el grupo seleccionado, haga clic en **Eliminar**.
4. Confirme su decisión.

Cómo eliminar copias de seguridad directamente desde el almacenamiento en la nube

1. Inicie sesión en el almacenamiento en la nube, tal y como se describe en "Descarga de archivos desde el almacenamiento en la nube".

2. Haga clic en el nombre del equipo cuyas copias de seguridad desea eliminar.
   El software muestra uno o más grupos de copias de seguridad.
3. Haga clic en el icono de engranaje que hay al lado del grupo de copias de seguridad que desea eliminar.
4. Haga clic en **Quitar**.
5. Confirme la operación.

La pestaña Planes

Puede gestionar los planes de protección y otros planes por medio de la pestaña **Planes**.

Cada sección de la pestaña **Planes** contiene todos los planes de un tipo concreto. Están disponibles las siguientes secciones:

- **Protección**
- **Análisis de copia de seguridad**
- **Réplica de copia de seguridad**
- **Validación**
- **Limpieza**
- **Conversión a equipo virtual**
- **Replicación de equipos virtuales**
- **Dispositivo de arranque**. Esta sección muestra los planes de protección que se han creado para equipos que se inician desde dispositivos de arranque y solo pueden aplicarse a esos equipos.

En cada sección puede crear, editar, deshabilitar, habilitar, eliminar, iniciar y supervisar la ejecución de un plan.

La clonación y la detención solo están disponibles en planes de protección. A diferencia de cuando detiene las copias de seguridad desde la pestaña **Dispositivos**, al detener un plan de protección se detendrán las copias de seguridad en todos los dispositivos en los que se aplique el plan. Si los tiempos de inicio de copia de seguridad para múltiples dispositivos están distribuidos en un espacio de tiempo, al detener un plan de protección se detendrán las copias de seguridad en curso o se impedirá que empiece cualquier copia de seguridad.

También puede exportar un plan a un archivo e importar un plan previamente exportado.

Cómo supervisar el estado de sus planes

Para algunos planes, por ejemplo, planes de protección, planes de replicación de máquinas virtuales y otros, está disponible una barra de estado codificada por colores. Indica el estado del plan en los recursos informáticos que se asignan a este plan:

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

Puede hacer clic en una sección de la barra de estado para ver el número de equipos que tienen ese estado.

Nota
El estado de un plan aplicado en un recurso informático puede no corresponderse con su estado. Por ejemplo, un plan de protección puede aplicarse correctamente en un recurso informático, por lo que su estado aparecerá como **CORRECTO**(verde). Al mismo tiempo, el recurso informático podría estar sin conexión, por lo que su estado en la pestaña **Dispositivos** será rojo.

Procesamiento de datos fuera del host

La mayoría de acciones que son parte de un plan de protección tales como replicación, validación y aplicar normas de retención se realizan por el agente que realiza la copia de seguridad. Esto coloca una carga de trabajo adicional en el equipo en el que este se está ejecutando, incluso después de que el proceso de la copia de seguridad haya finalizado.

Separar los planes de análisis antimalware, replicación, validación, limpieza y conversión de los planes de protección le da flexibilidad:

- Para seleccionar otros agentes para que realicen estas operaciones
- Para programar estas operaciones durante horas de menor actividad y minimizar así el consumo del ancho de banda de red
- Para cambiar estas operaciones fuera de las horas de oficina en caso de que configurar un agente dedicado no forme parte de su planificación

Si está usando un nodo de almacenamiento, instalar un agente dedicado en el mismo equipo es lo más lógico.

A diferencia de los planes de copias de seguridad y de replicación de equipos virtuales, que emplean la configuración de hora de los equipos que ejecutan los agentes, los planes de procesamiento de datos fuera del host se ejecutan según la configuración de hora del equipo en el Management Server.

Análisis de planes de copia de seguridad

El análisis antimalware de las copias de seguridad está disponible si el componente Scan Service está instalado con el servidor de administración Cyber Protect. Para obtener más información, consulte "Scan Service" (p. 112).

Los planes de escaneo de copias de seguridad son compatibles con las copias de seguridad de **equipo completo** y **disco/volumen** de equipos Windows. Solo se analizan los volúmenes con el sistema de archivos NTFS y particionado GPT o MBR.

Pasos para crear un plan de análisis de copias de seguridad

1. En la consola web de Cyber Protect, vaya a **Planes** > **Análisis de copia de seguridad**.
2. Haga clic en **Crear plan**.
3. [Opcional] Para modificar el nombre del plan, haga clic en el icono del lápiz al lado del nombre predeterminado.

4. Seleccione el agente de análisis.
5. Seleccione las copias de seguridad o las ubicaciones de copia de seguridad que desea escanear.
   Para incluir varias copias de seguridad en el plan, añádalas una a una.
6. [Para copias de seguridad en el almacenamiento en la nube o en una carpeta de red] Si se le solicita, especifique las credenciales de acceso para el almacenamiento.
7. [Para copias de seguridad cifradas] Especifique la contraseña de cifrado.
   Puede especificar una contraseña para todas las copias de seguridad o ubicaciones de copia de seguridad seleccionadas. Si la contraseña no coincide con una copia de seguridad específica, se mostrará una alerta. Solo se analizan las copias de seguridad con contraseñas coincidentes.
8. Configure el programa de escaneo.
9. Haga clic en **Crear**.

Replicación de copias de seguridad

Ubicaciones compatibles

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

Ubicación de la copia de seguridad	Admitido como origen	Admitido como destino
Almacenamiento en la cloud	+	+
Carpeta local	+	+
Carpeta de red	+	+
Carpeta NFS	–	–
Secure Zone	–	–
Servidor SFTP	–	–
Ubicación gestionada*	+	+
Dispositivo de cintas	–	+

* Compruebe las restricciones indicadas en el tema "Consideraciones para usuarios con licencias de Advanced" (p. 307).

Pasos para crear un plan de replicación de copias de seguridad

1. Haga clic en **Planes** > **Replicación de copia de seguridad**.
2. Haga clic en **Crear plan**.
   El software muestra una nueva plantilla de plan.
3. [Opcional] Para modificar el nombre del plan, haga clic en el nombre predeterminado.

4. Haga clic en **Agente** y, a continuación, seleccione el agente que realizará la replicación.

   Puede seleccionar cualquier agente que tenga acceso a las ubicaciones de origen y destino de la copia de seguridad.
5. Haga clic en **Elementos para replicar** y seleccione las copias de seguridad que se replicarán en este plan.

   Puede alternar entre la selección de copias de seguridad y la selección de ubicaciones enteras mediante el enlace **Ubicaciones** / **Copias de seguridad** ubicado en la esquina superior derecha.

   Si las copias de seguridad seleccionadas están cifradas, todas deben usar la misma contraseña de cifrado. En el caso de las copias de seguridad que utilizan contraseñas de cifrado diferentes, cree planes independientes.
6. Haga clic en **Destino** y especifique la ubicación de destino.
7. [Opcional] En **Cómo replicar**, seleccione qué copias de seguridad hay que replicar. Puede seleccionar una de las siguientes opciones:
   - **Todas las copias de seguridad** (opción predeterminada)
   - **Solo las copias de seguridad completas**
   - **Solo la última copia de seguridad**
8. [Opcional] Haga clic en **Planificación** y, a continuación, cambie la planificación.
9. [Opcional] Haga clic en **Reglas de retención** y, a continuación, especifique las reglas de retención para la ubicación de destino, como se indica en "Reglas de retención".
10. Si las copias de seguridad seleccionadas en **Elementos para replicar** están cifradas, active la opción **Contraseña de la copia de seguridad** y, a continuación, introduzca la contraseña de cifrado. De lo contrario, omita este paso.
11. [Opcional] Para modificar las opciones del plan, haga clic en el icono de engranaje.
12. Haga clic en **Crear**.

Validación

La validación es una operación que verifica la posibilidad de recuperación de datos en una copia de seguridad.

La validación de una ubicación de copia de seguridad valida todas las copias de seguridad almacenadas en la ubicación.

Cómo funciona

Un plan de validación ofrece dos métodos de validación. Si selecciona ambos métodos, las operaciones se realizarán de forma consecutiva.

- **Cálculo de una suma de comprobación para cada bloque de datos guardado en una copia de seguridad**

  Para obtener más información sobre la validación mediante el cálculo de una suma de comprobación, consulte "Validación de la copia de seguridad".

- **Ejecución de un equipo virtual desde una copia de seguridad**

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

  El agente ejecuta un equipo virtual desde una copia de seguridad y luego se conecta a las herramientas de VMware o a Hyper-V Heartbeat Service para garantizar que el sistema operativo se ha iniciado correctamente. Si la conexión falla, el agente intentará conectarse cada dos minutos en un máximo de cinco intentos. Si no se conecta en ninguno de estos intentos, la validación falla.

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

Si la validación falla, podrá ver todos los detalles en la sección **Actividades** de la pestaña **Resumen**.

Ubicaciones compatibles

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

Ubicación de la copia de seguridad	Calcular una suma de comprobación	Ejecutar un VM
Almacenamiento en la cloud	+	+
Carpeta local	+	+
Carpeta de red	+	+
Carpeta NFS	–	–
Secure Zone	–	–
Servidor SFTP	–	–
Ubicación gestionada	+	+
Dispositivo de cintas	+	–

Pasos para crear un nuevo plan de validación

1. Haga clic en **Planes** > **Validación**.
2. Haga clic en **Crear plan**.

   El software muestra una nueva plantilla de plan.
3. [Opcional] Para modificar el nombre del plan, haga clic en el nombre predeterminado.
4. Haga clic en **Agente** y, a continuación, seleccione el agente que realizará la validación.

   Si desea realizar la validación ejecutando un equipo virtual desde una copia de seguridad, debe seleccionar Agente para VMware o Agente para Hyper-V. De lo contrario, seleccione cualquier

agente registrado en el servidor de gestión que tenga acceso a la ubicación de copia de seguridad.

5. Haga clic en **Elementos para validar** y seleccione las copias de seguridad que se validarán en este plan.

   Puede alternar entre la selección de copias de seguridad y la selección de ubicaciones enteras mediante el enlace **Ubicaciones** / **Copias de seguridad** ubicado en la esquina superior derecha.

   Si las copias de seguridad seleccionadas están cifradas, todas deben usar la misma contraseña de cifrado. En el caso de las copias de seguridad que utilizan contraseñas de cifrado diferentes, cree planes independientes.
6. [Opcional] En **Qué validar**, seleccione las copias de seguridad que desea validar. Puede seleccionar una de las siguientes opciones:
   - **Todas las copias de seguridad**
   - **Solo la última copia de seguridad**
7. [Opcional] Haga clic en **Cómo validar** y elija uno de los métodos siguientes:
   - **Verificación de suma de comprobación**

     El software calculará una suma de comprobación para cada bloque de datos guardado en una copia de seguridad.
   - **Ejecutar como equipo virtual**

     El software ejecuta un equipo virtual para cada copia de seguridad.
8. Si ha elegido **Ejecutar como equipo virtual**:
   a. Haga clic en **Equipo de destino** y, a continuación, seleccione el tipo de equipo virtual (ESXi o Hyper-V), el servidor y la plantilla del nombre del equipo.

      El nombre predeterminado es **[Nombre del equipo]_validate**.
   b. Haga clic en **Almacén de datos** para ESXi o **Ruta** para Hyper-V y, a continuación, seleccione el almacén de datos para el equipo virtual.
   c. [Opcional] Cambie el modo de aprovisionamiento de disco.

      La configuración predeterminada es **Fina** para VMware ESXi y **Expansión dinámica** para Hyper-V.
   d. [Opcional] Haga clic en **Configuración de máquina virtual** para modificar el tamaño de la memoria y las conexiones de red de la máquina virtual.

      De forma predeterminada, el equipo virtual *no* está conectado a una red y el tamaño de la memoria del equipo virtual es igual a la memoria del equipo original.

   Nota
   La opción **Latido de la máquina virtual** siempre está habilitada para validar el estado de la máquina virtual transmitida por las herramientas del hipervisor en el sistema operativo invitado (Herramientas de VMware o Servicios de integración de Hyper-V) mediante una máquina virtual desde la copia de seguridad. Esta opción se ha diseñado para versiones futuras, por lo que no puede interactuar con ella.
9. [Opcional] Haga clic en **Planificación** y, a continuación, cambie la planificación.

10. Si las copias de seguridad seleccionadas en **Elementos para validar** están cifradas, active la opción **Contraseña de la copia de seguridad** y, a continuación, introduzca la contraseña de cifrado. De lo contrario, omita este paso.
11. [Opcional] Para modificar las opciones del plan, haga clic en el icono de engranaje.
12. Haga clic en **Crear**.

Limpieza

La limpieza es una operación que elimina copias de seguridad desactualizadas según las reglas de retención.

Ubicaciones compatibles

Los planes de limpieza admiten todas las ubicaciones de copias de seguridad, salvo para las carpetas NFS, los servidores SFTP y Secure Zone.

Pasos para crear un nuevo plan de limpieza

1. Haga clic en **Planes** > **Limpieza**.
2. Haga clic en **Crear plan**.
   El software muestra una nueva plantilla de plan.
3. [Opcional] Para modificar el nombre del plan, haga clic en el nombre predeterminado.
4. Haga clic en **Agente** y, a continuación, seleccione el agente que realizará la limpieza.
   Puede seleccionar cualquier agente que tenga acceso a la ubicación de la copia de seguridad.
5. Haga clic en **Elementos para limpiar** y seleccione las copias de seguridad que limpiar con este plan.
   Puede alternar entre la selección de copias de seguridad y la selección de ubicaciones enteras mediante el enlace **Ubicaciones** / **Copias de seguridad** ubicado en la esquina superior derecha.
   Si las copias de seguridad seleccionadas están cifradas, todas deben usar la misma contraseña de cifrado. En el caso de las copias de seguridad que utilizan contraseñas de cifrado diferentes, cree planes independientes.
6. [Opcional] Haga clic en **Planificación** y, a continuación, cambie la planificación.
7. [Opcional] Haga clic en **Reglas de retención** y, a continuación, especifique las reglas de retención como se indica en "Reglas de retención".
8. Si las copias de seguridad seleccionadas en **Elementos para limpiar** están cifradas, active la opción **Contraseña de la copia de seguridad** y, a continuación, introduzca la contraseña de cifrado. De lo contrario, omita este paso.
9. [Opcional] Para modificar las opciones del plan, haga clic en el icono de engranaje.
10. Haga clic en **Crear**.

Conversión a equipo virtual

Puede crear un plan independiente para la conversión a un equipo virtual y ejecutarlo manualmente o de forma planificada.

Nota
No pueden hacerse copias de seguridad de máquinas virtuales replicadas a través de la funcionalidad de replicación nativa de máquinas virtuales de Scale Computing.

Para obtener más información sobre los requisitos previos y las limitaciones, consulte "Lo que necesita saber sobre conversión".

Pasos para crear un plan de conversión a equipo virtual

1. Haga clic en **Planes** > **Conversión a equipo virtual**.
2. Haga clic en **Crear plan**.
   El software muestra una nueva plantilla de plan.
3. [Opcional] Para modificar el nombre del plan, haga clic en el nombre predeterminado.
4. En **Convertir a**, seleccione el tipo de equipo virtual de destino. Puede seleccionar una de las siguientes opciones:
   - **VMware ESXi**
   - **Microsoft Hyper-V**
   - **Scale Computing HC3**
   - **VMware Workstation**
   - **Archivos VHDX**

     Nota
     Para ahorrar espacio de almacenamiento, cada conversión a archivos VHDX sobrescribe los archivos VHDX que se encuentran en la ubicación de destino que se creó durante la conversión anterior.
5. Realice uno de los siguientes procedimientos:
   - [Para VMware ESXi, Hyper-V y Scale Computing HC3] Haga clic en **Servidor**, seleccione el servidor de destino y, a continuación, especifique la nueva plantilla del nombre del equipo.
   - [Para otros tipos de equipos virtuales] En **Ruta**, especifique el lugar en que guardar los archivos de la máquina virtual y la plantilla de los nombres de los archivos.

   El nombre predeterminado es **[Machine Name]_converted**.
6. Haga clic en **Agente** y, a continuación, seleccione el agente que realizará la conversión.
7. Haga clic en **Elementos para convertir** y seleccione las copias de seguridad que este plan convertirá en equipos virtuales.

Puede alternar entre la selección de copias de seguridad y la selección de ubicaciones enteras mediante el enlace **Ubicaciones** / **Copias de seguridad** ubicado en la esquina superior derecha.

Si las copias de seguridad seleccionadas están cifradas, todas deben usar la misma contraseña de cifrado. En el caso de las copias de seguridad que utilizan contraseñas de cifrado diferentes, cree planes independientes.

8. [Únicamente para VMware ESXi y Hyper-V] Haga clic en **Almacén de datos** para ESXi o **Ruta** para Hyper-V y, a continuación, seleccione el almacén de datos (almacenamiento) para el equipo virtual.
9. [Solo para VMware ESXi y Hyper-V] Seleccione el modo de aprovisionamiento de disco. La configuración predeterminada es **Fina** para VMware ESXi y **Expansión dinámica** para Hyper-V.
10. [Opcional] [Para VMware ESXi, Hyper-V y Scale Computing HC3] Haga clic en **Configuración de máquina virtual** para cambiar el tamaño de la memoria, el número de procesadores o las conexiones de red de la máquina virtual.
11. [Opcional] Haga clic en **Planificación** y, a continuación, cambie la planificación.
12. Si las copias de seguridad seleccionadas en **Elementos para convertir** están cifradas, active la opción **Contraseña de la copia de seguridad** y, a continuación, introduzca la contraseña de cifrado. De lo contrario, omita este paso.
13. [Opcional] Para modificar las opciones del plan, haga clic en el icono de engranaje.
14. Haga clic en **Crear**.

Dispositivo de arranque

Importante
Algunas de las funciones descritas en esta sección solo están disponibles en implementaciones locales.

Dispositivo de arranque

Los dispositivos de arranque son un dispositivo físico (CD, DVD, unidad flash USB u otro dispositivo extraíble compatible con BIOS del equipo como dispositivo de arranque) que permite ejecutar el agente de protección tanto en un entorno basado en Linux como en un entorno de preinstalación de Windows (WinPE), sin la ayuda de un sistema operativo.

Los dispositivo de arranque se usan con frecuencia para:

- Recuperar un sistema operativo que no puede iniciar
- Acceder a los datos que sobrevivieron en un sistema dañado y realizar copias de seguridad de éstos
- Implementar un sistema operativo desde cero
- Crear volúmenes básicos o dinámicos desde cero
- Realizar copias de seguridad sector por sector de un disco con un sistema de archivos incompatible
- Realizar copias de seguridad fuera de línea de cualquier dato que no se puede incluir en la copia de seguridad en línea, por ejemplo, porque los datos están bloqueados por una aplicación en ejecución o porque el acceso a los mismos está restringido.

También se puede iniciar un equipo desde la red con Acronis PXE Server, Windows Deployment Services (WDS) o Servicios de Instalación Remota (RIS). Estos servidores con componentes de arranque cargados también puede considerarse un tipo de dispositivo de arranque. Puede crear dispositivos de arranque o configurar el servidor PXE o WDS/RIS con el mismo asistente.

¿Crear un medio de inicio o descargar uno disponible?

Con Bootable Media Builder, puede crear su propio dispositivo de arranque (basado en Linux o basado en WinPE) para ordenadores Windows, Linux o macOS. Para crear un dispositivo de arranque con todas las funciones, especifique su clave de licencia de Acronis Cyber Protect. Sin esta clave, su dispositivo de arranque solo podrá llevar a cabo operaciones de recuperación.

Nota
El dispositivo de arranque no es compatible con unidades híbridas.

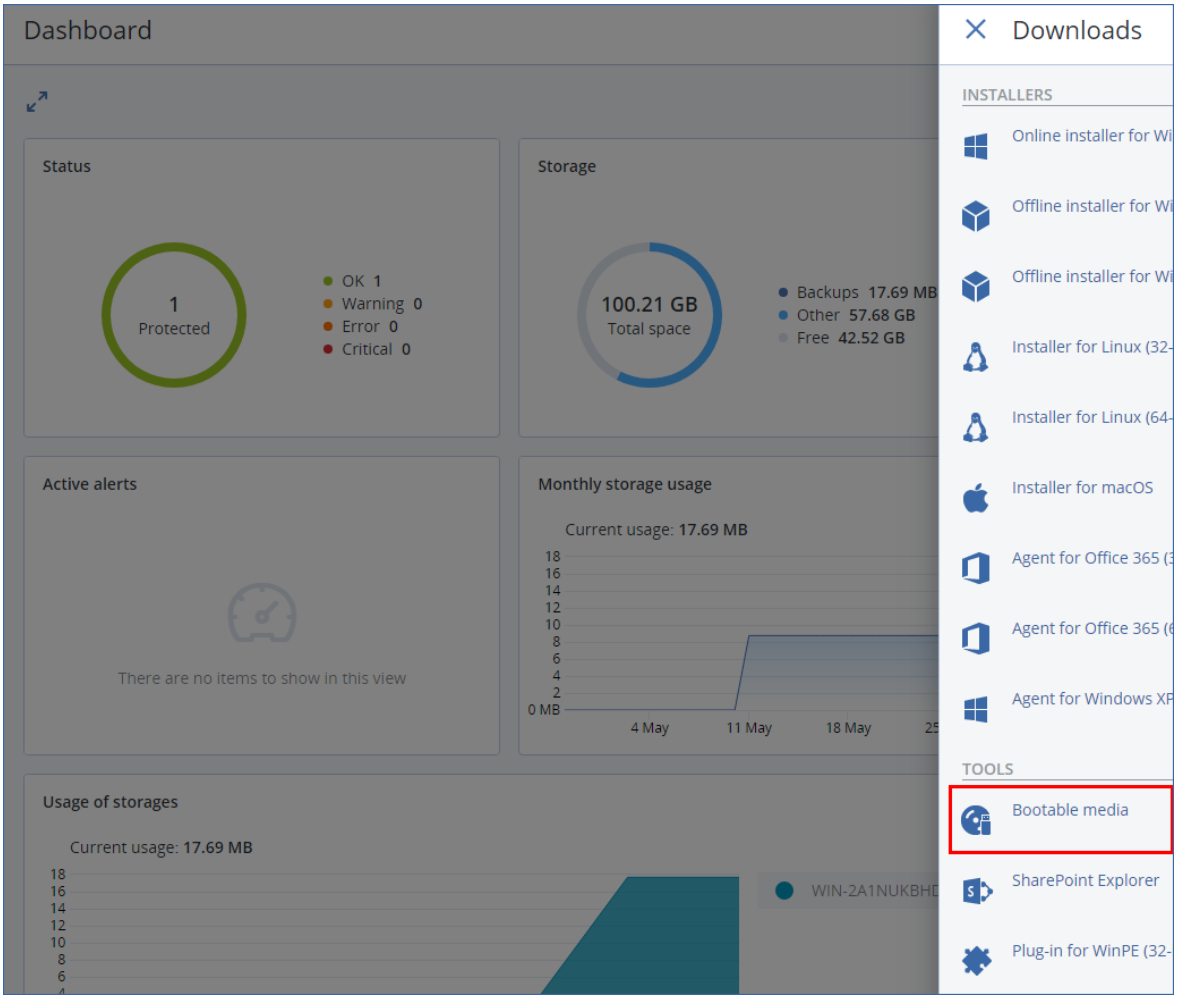
También puede descargar un dispositivo de arranque disponible (solo los basados en Linux). El dispositivo de arranque descargado solo se usará para operaciones de recuperación y para acceder a Acronis Universal Restore. No podrá realizar una copia de seguridad de datos, validar o exportar

copias de seguridad, gestionar discos ni utilizar scripts con él. Los dispositivos de arranque descargados no son adecuados para ordenadores macOS.

Nota
El dispositivo de arranque disponible no es compatible con nodos de almacenamiento, ubicaciones de cinta y ubicaciones SFTP. Si desea utilizar estas ubicaciones de almacenamiento en su implementación local, debe crear un dispositivo de arranque con Bootable Media Builder. Consulte https://kb.acronis.com/content/61566.

Pasos para descargar un dispositivo de arranque disponible

1. En la consola web de Cyber Protect, haga clic en el icono de la cuenta en la esquina superior derecha y, a continuación, haga clic en **Descargas**.
2. Seleccione **Dispositivo de arranque**.



Puede grabar el archivo ISO descargado en un CD/DVD o crear una unidad flash USB de arranque utilizando una de las muchas herramientas gratuitas disponibles en línea. Para iniciar un equipo UEFI, use `ISO a USB` o `RUFUS`, y para un equipo BIOS, use `Win32DiskImager`. En Linux, puede usar la utilidad `dd`.

Si no se puede acceder a la consola web de Cyber Protect, puede descargar el dispositivo de arranque disponible desde su cuenta del portal de clientes de Acronis:

1. Vaya a https://account.acronis.com.
2. Localice Acronis Cyber Protect y haga clic en **Descargas**.
3. En la página que se abra, localice **Descargas adicionales** y haga clic en **Bootable Media ISO (para Windows y Linux)**.

¿Dispositivos de arranque basados en Linux o en WinPE?

Basado en Linux

Los dispositivos de arranque basados en Linux contienen un agente de protección basado en un kernel Linux. El agente puede iniciar y realizar las operaciones en cualquier hardware compatible con PC, incluyendo desde cero y los equipos con sistemas de archivos dañados o incompatibles. Se pueden configurar y controlar las operaciones tanto a nivel local como remoto en la consola web de Cyber Protect.

Puede consultar una lista de hardware compatible con dispositivos basados en Linux en: http://kb.acronis.com/content/55310.

Basado en WinPE

El soporte de arranque basado en WinPE contiene un sistema Windows mínimo llamado entorno de preinstalación de Windows (WinPE) y un complemento de Acronis para WinPE, que es una modificación del agente de protección que puede ejecutarse en el entorno de preinstalación.

Se comprobó que WinPE es la solución de arranque más conveniente en entornos grandes con hardware heterogéneo.

Ventajas:

- El uso de Acronis Cyber Protect con el entorno de preinstalación de Windows proporciona más funcionalidad que el uso de dispositivos de arranque basados en Linux. Como se inició un hardware compatible con PC en WinPE, no solo puede utilizar un agente de protección, sino también los comandos, secuencias y otros complementos de PE que haya añadido.
- Los dispositivos de arranque basados en PE ayudan a superar los problemas de los dispositivos de arranque basados en Linux compatibles con ciertos controladores RAID de ciertos niveles de conjuntos de RAID solos. Los medios basados en WinPE 2.x y versiones posteriores permiten la carga dinámica de los controladores de dispositivos necesarios.

Limitaciones:

- Los medios de arranque basados en versiones de WinPE anteriores a la versión 4.0 no pueden iniciarse en equipos con la interfaz Unified Extensible Firmware Interface (UEFI).

- Cuando un equipo se arranca con un dispositivo de arranque basado en PE, no se pueden seleccionar medios ópticos como CD, DVD o discos Blu-ray (BD) como el destino de la copia de seguridad.

Bootable Media Builder

Bootable Media Builder es una herramienta dedicada para la creación de dispositivos de arranque. Solo está disponible para implementaciones locales.

Bootable Media Builder se instala de forma predeterminada al instalar el servidor de gestión. Puede instalar Media Builder por separado o en cualquier equipo que ejecute Windows o Linux. Los sistemas operativos compatibles son los mismos que para los agentes correspondientes.

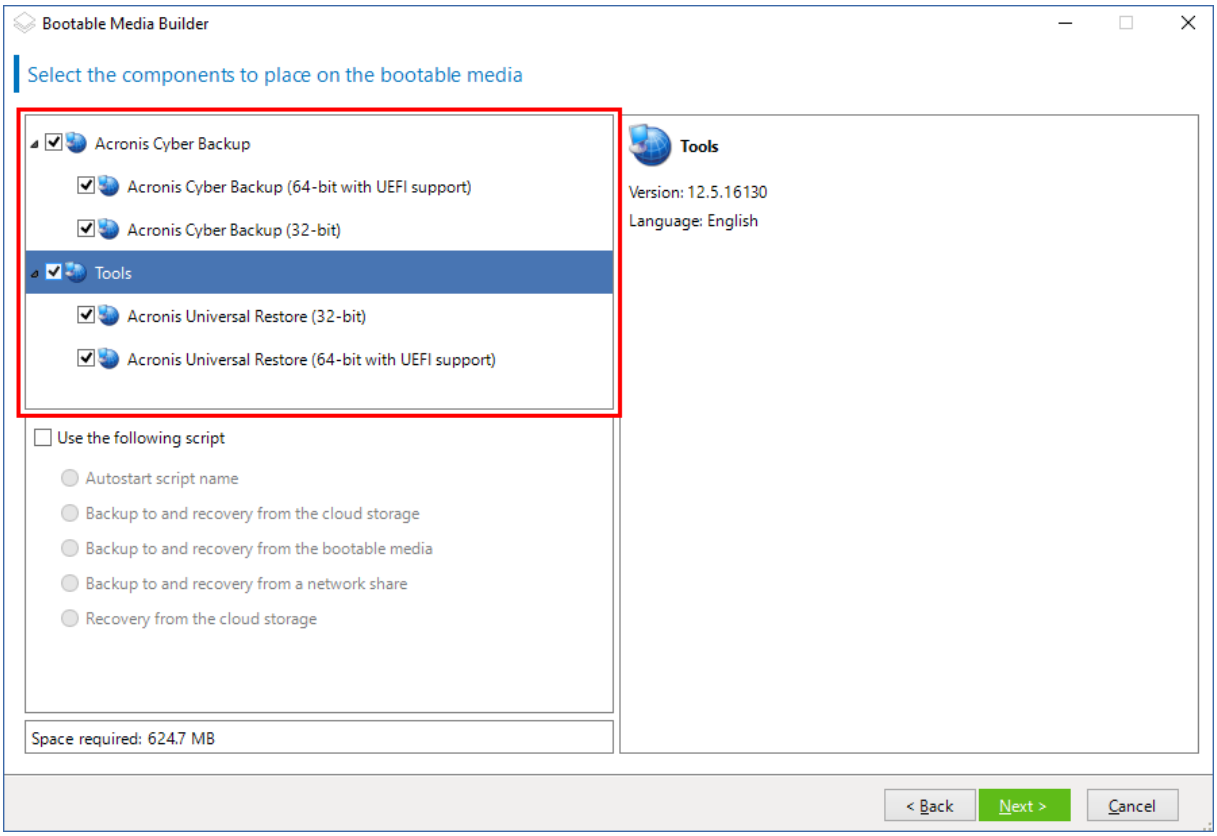
¿Por qué utilizar Media Builder?

El dispositivo de arranque disponible para su descarga en la consola web de Cyber Protect solo se puede utilizar para recuperación. Este medio se basa en un kernel Linux. A diferencia de Windows PE, no permite inyectar controladores personalizados sobre la marcha.

- Media Builder le permite crear un dispositivo de arranque personalizado con todas las funciones basado en Linux y basado en WinPE, con la funcionalidad de las copias de seguridad.
- Aparte de crear dispositivos de arranque físicos, puede cargar sus componentes en Windows Deployment Services (WDS) y usar un arranque de red.
- El dispositivo de arranque disponible no es compatible con nodos de almacenamiento, ubicaciones de cinta y ubicaciones SFTP. Si desea utilizar estas ubicaciones de almacenamiento en su implementación local, debe crear un dispositivo de arranque con Bootable Media Builder. Consulte https://kb.acronis.com/content/61566.

¿32 o 64 bits?

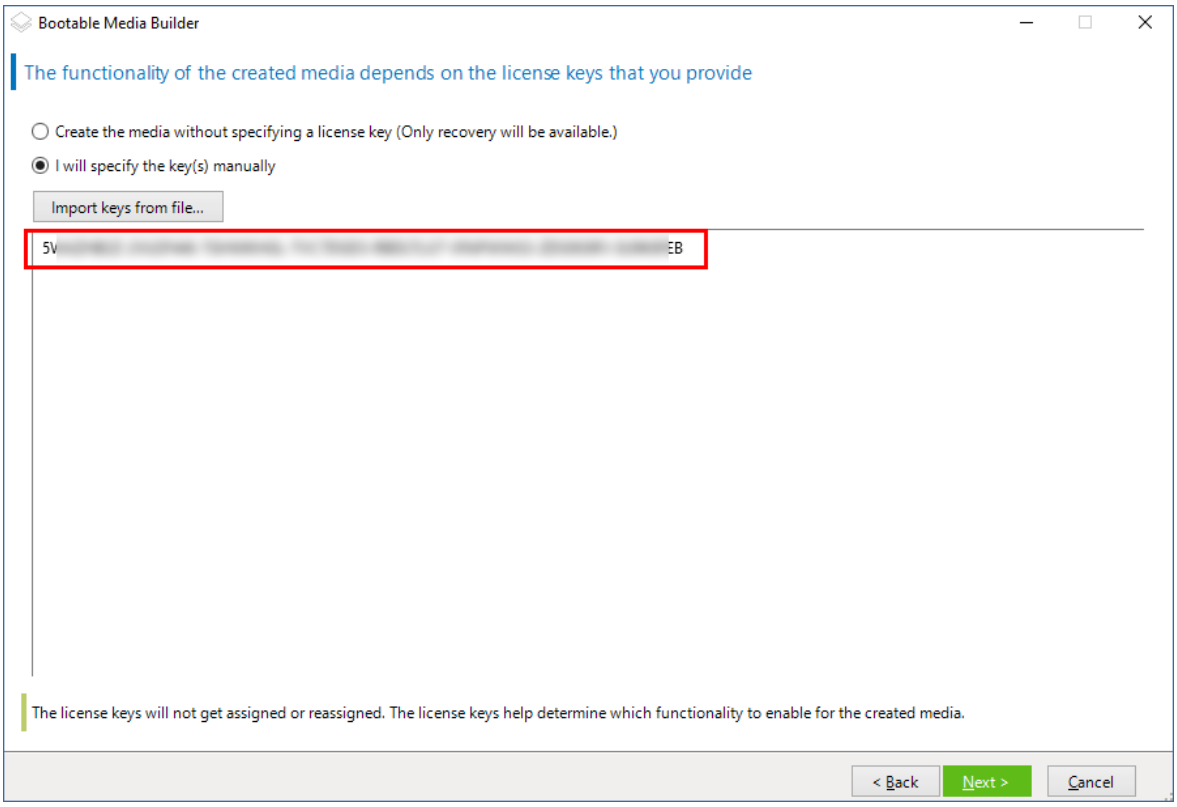
Bootable Media Builder crea medios con componentes de 32 bits y 64 bits. En la mayoría de los casos, necesitará un medio de 64 bits para arrancar un equipo que utiliza la interfaz extensible del firmware unificada (UEFI).



Dispositivos de arranque basados en Linux

Para crear un dispositivo de arranque basado en Linux

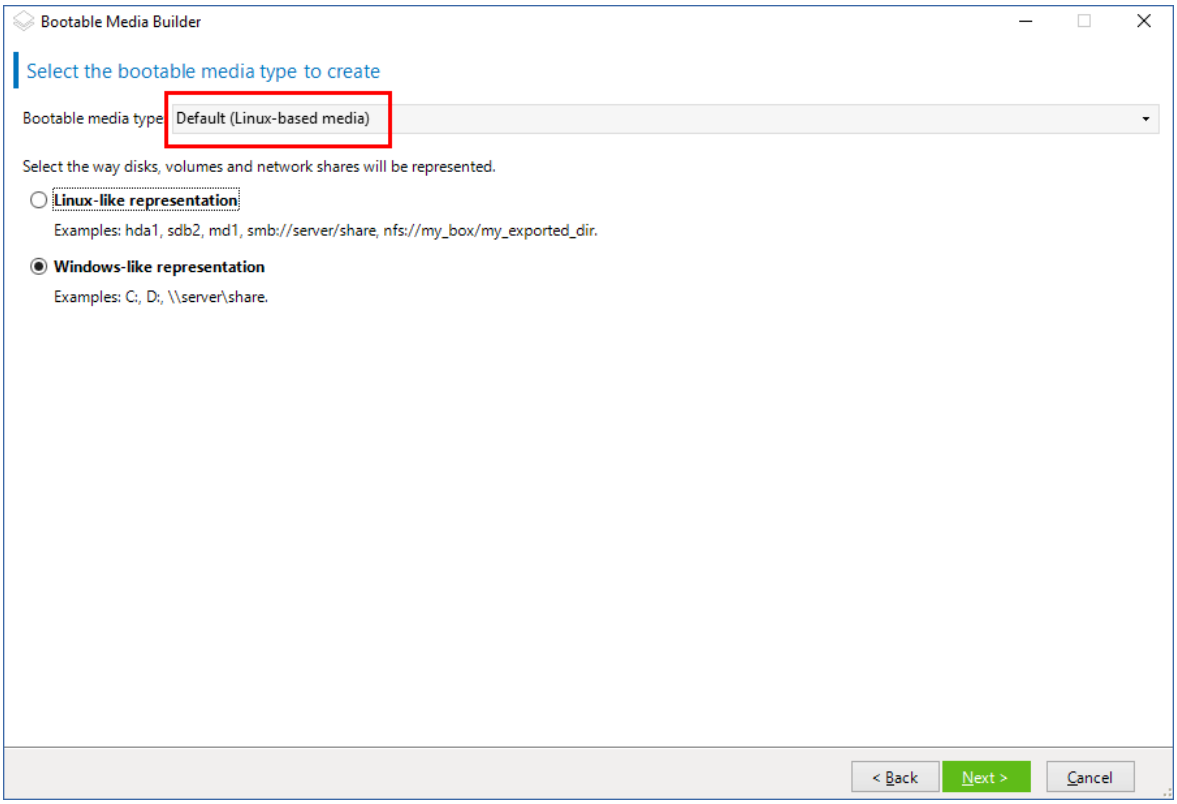
1. Inicie **Bootable Media Builder**.
2. Para crear un dispositivo de arranque con todas las funciones, especifique una clave de licencia Acronis Cyber Protect. Esta clave se utiliza para determinar las funciones que se incluirán en el dispositivo de arranque. No se revocarán las licencias de ningún equipo.
   Si no especifica una clave de licencia, el dispositivo de arranque resultante solo se usará para operaciones de recuperación.



3. Seleccione **Tipo de dispositivo de arranque: Predeterminado (dispositivo de arranque basado en Linux)**.

   Seleccione cómo se representarán los volúmenes y recursos de red:

   - Una representación de un dispositivo con un manejo de volúmenes estilo Linux muestra los volúmenes como, por ejemplo, hda1 y sdb2. Intenta reconstruir los dispositivos MD y los volúmenes lógicos (LVM) antes de comenzar una recuperación.
   - Una representación de un dispositivo con una gestión de volúmenes tipo Windows muestra los volúmenes, por ejemplo, como C: y D:. Proporciona acceso a los volúmenes dinámicos (LDM).



4. [Opcional] Especifique los parámetros del kernel Linux. Separe los diferentes parámetros con espacios.

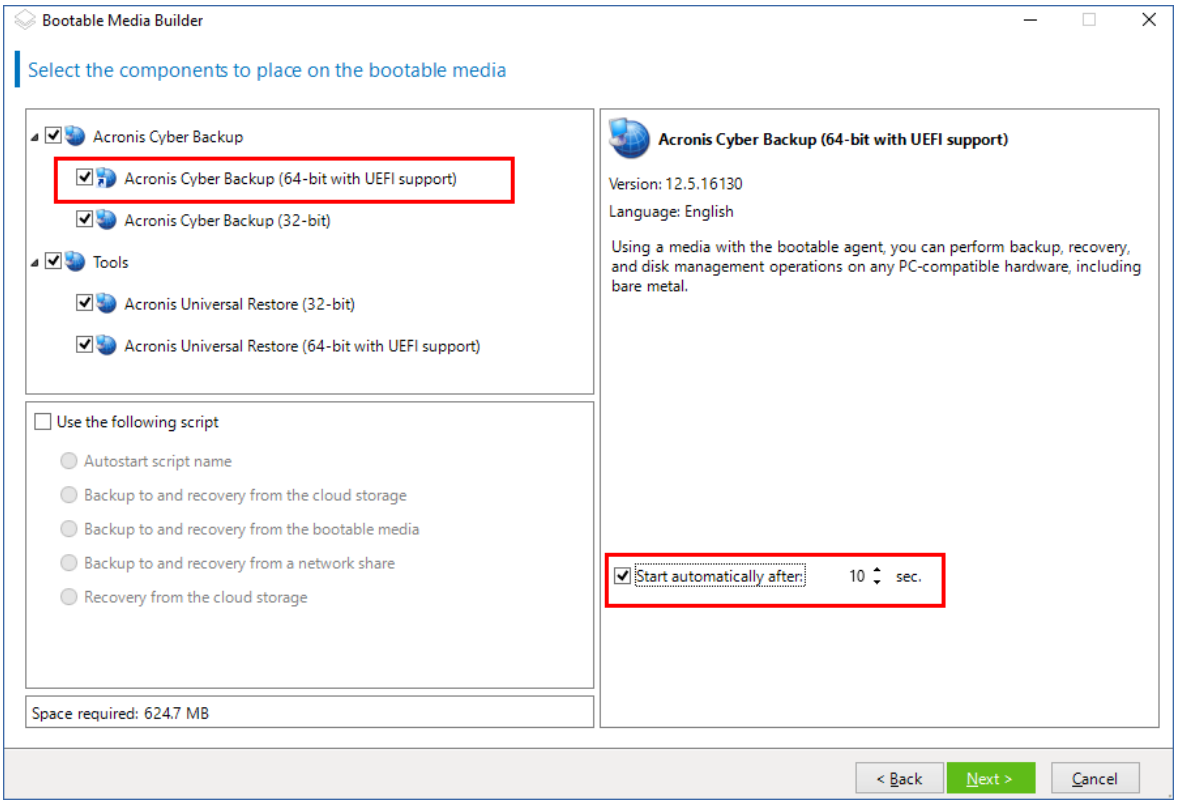
   Por ejemplo, para poder seleccionar un modo de visualización para el agente de arranque cada vez que se inicia el dispositivo, escriba: **vga=ask**.

   Para obtener más información sobre los parámetros disponibles, consulte Parámetros de kernel.
5. [Opcional] Seleccione el idioma que se utilizará en el dispositivo de arranque.
6. Seleccione los componentes que se ubicarán en el dispositivo: el agente de arranque Acronis Cyber Protect y/o Universal Restore si desea restaurar el sistema en un hardware diferente.

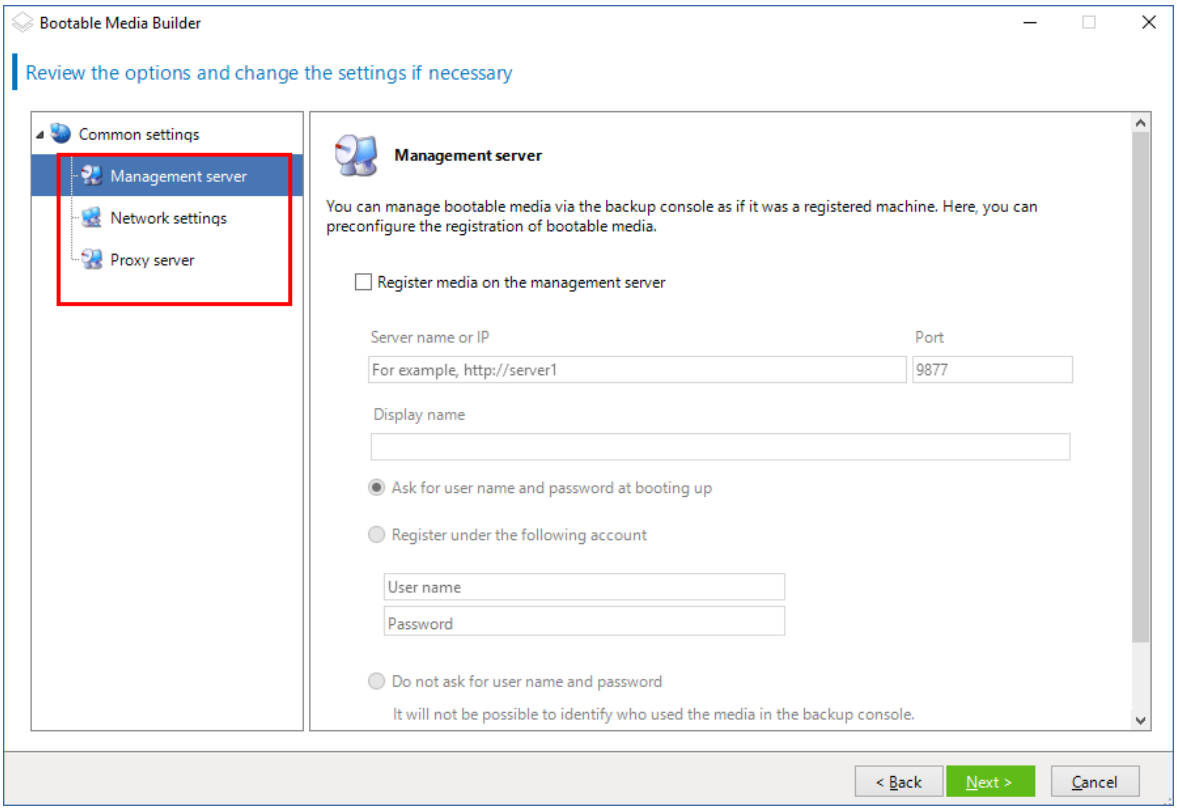
   Con el agente de arranque puede realizar operaciones de copia de seguridad, recuperación y gestión del disco en cualquier hardware compatible con PC, incluyendo recuperación de cero.

   Universal Restore le permite arrancar un sistema operativo recuperado en un hardware diferente o en un equipo virtual. La herramienta localiza e instala los controladores de dispositivos que son críticos para iniciar el sistema operativo, como los controladores de almacenamiento, placa madre o conjunto de chips.
7. [Opcional] Especifique el intervalo de tiempo de espera para el menú de arranque además del componente que se iniciará automáticamente en el tiempo de espera. Para ello, haga clic en el componente que desee en el panel superior izquierdo y establezca el intervalo. Esto habilita el funcionamiento in situ sin interacción al arrancar desde WDS/RIS.

   Si no se configura este ajuste, el cargador esperará a que seleccione si iniciar desde el sistema operativo (de estar presente) o el componente.



8. [Opcional] Si desea automatizar las operaciones del agente de arranque, seleccione la casilla de verificación **Utilizar el script siguiente**. A continuación, seleccione uno de los scripts y especifique los parámetros del script.
9. [Opcional] Seleccione cómo deben registrarse los dispositivos en el servidor de gestión al arrancar. Para obtener más información sobre la configuración de registro, consulte la sección Servidor de gestión.



10. [Opcional] Especifique la configuración de red: La configuración TCP/IP que será asignada a los adaptadores de red del equipo. Para obtener más información, consulte "Configuraciones de red" (p. 432).
11. [Opcional] Especifique un puerto de red: El puerto TCP que el agente de arranque escucha para una conexión entrante.
12. [Opcional] Si hay un servidor proxy habilitado en la red, especifique su nombre de servidor/dirección IP y puerto.
13. Seleccione el tipo de dispositivo. Puede:
    - Cree una imagen ISO. Podrá grabarla en un CD/DVD; utilícela para crear una unidad flash USB de arranque; o conéctela a un equipo virtual.
    - Cree un archivo ZIP.
    - Cargar los componentes seleccionados en Acronis PXE Server.
    - Cargar los componentes seleccionados A WDS/RIS.
14. [Opcional] Añada controladores del sistema Windows que usará Universal Restore. Esta ventana aparece si se añade Universal Restore al medio y se selecciona otro medio que no sea WDS/RIS.
15. Si así se le indica, especifique el nombre del servidor/dirección IP y las credenciales de WDS/RIS, o una ruta al archivo ISO del medio.
16. Compruebe su configuración en la pantalla de resumen y haga clic en **Continuar**.

Parámetros de kernel

Esta ventana le permite especificar uno o más parámetros del kernel de Linux. Se aplicarán automáticamente cuando se ejecute el dispositivo de arranque.

Estos parámetros se utilizan comúnmente cuando hay problemas mientras se trabaja con el dispositivo de arranque. Normalmente, puede dejar este campo vacío.

También puede especificar cualquiera de estos parámetros pulsando F11 mientras está en el menú de arranque.

Parámetros

Cuando especifique varios parámetros, sepárelos con espacios.

acpi=desactivada

Desactiva la interfaz de alimentación de configuración avanzada (ACPI). Puede utilizar este parámetro cuando experimente problemas con la configuración de un hardware en particular.

noapic

Desactiva el Controlador de interrupciones programable avanzado (APIC). Puede utilizar este parámetro cuando experimente problemas con la configuración de un hardware en particular.

vga=ask

Solicita que seleccione el modo de video que utilizará la interfaz gráfica de usuario del dispositivo de arranque. Sin el parámetro **vga**, el modo vídeo se detecta automáticamente.

vga= *mode_number*

Especifica el modo de video que utilizará la interfaz gráfica de usuario del dispositivo de arranque. El número de modo aparece en *mode_number* en formato hexadecimal, por ejemplo: **vga=0x318**

La resolución de la pantalla y el número de colores correspondiente a un número de modo puede ser diferente en equipos diferentes. Recomendamos utilizar primero el parámetro **vga=ask** para seleccionar un valor para *mode_number*.

silencio

Desactiva la muestra de mensajes de inicio cuando el kernel de Linux se está cargando y ejecuta la consola de gestión una vez que el kernel está cargado.

Este parámetro está especificado implícitamente cuando crea el dispositivo de arranque, pero puede borrar este parámetro mientras esté en el menú de inicio.

Sin este parámetro, se mostrarán todos los mensajes de inicio, seguidos de una entrada de comandos. Para iniciar la consola de gestión desde la entrada de comandos, ejecute el comando: **/bin/product**

nousb

Desactiva la carga del subsistema del USB (bus universal en serie).

nousb2

Desactiva la compatibilidad con USB 2.0. No obstante, los dispositivos USB 1.1 trabajan con este parámetro. Este parámetro le permite utilizar algunas unidades USB en el modo USB 1.1 si no funcionan en el modo USB 2.0.

nodma

Desactiva el acceso directo a memoria (DMA) para todas las unidades del disco duro IDE. Evita que el kernel se congele en algún hardware.

nofw

Desactiva la compatibilidad con la interfaz de FireWire (IEEE1394).

nopcmcia

Desactiva la detección del hardware PCMCIA.

nomouse

Desactiva la compatibilidad con el ratón.

module_name **=off**

Desactiva el módulo cuyo nombre aparece en *module_name*. Por ejemplo, para desactivar el uso del módulo SATA, especifique: **sata_sis=off**

pci=bios

Obliga al uso de PCI BIOS en vez de acceder directamente al dispositivo del hardware. Es conveniente que utilice este parámetro si el equipo tiene un puente PCI no estándar de host.

pci=nobios

Desactiva el uso de PCI BIOS; solo se pueden utilizar métodos de acceso directo al hardware. Es conveniente que utilice este parámetro cuando el dispositivo de arranque no puede iniciarse, lo que puede deberse a la BIOS.

pci=biosirq

Utiliza las alertas PCI BIOS para obtener la tabla de rutas de interrupción. Es conveniente que utilice este parámetro si el kernel no puede asignar solicitudes de interrupción (IRQ) o descubrir enlaces secundarios de PCI en la placa madre.

Estas llamadas pueden no funcionar correctamente en algunos equipos. Pero puede ser la única manera de obtener la tabla de rutas de interrupción.

LAYOUTS=en-US, de-DE, fr-FR, ...

Especifica las disposiciones del teclado que se pueden utilizar en la interfaz gráfica de usuario del dispositivo de arranque.

Sin este parámetro, solo se pueden utilizar dos disposiciones: Inglés (EE. UU.) y la disposición correspondiente al idioma seleccionado en el menú del dispositivo de arranque.

Puede especificar cualquiera de las siguientes disposiciones:

Belga: **be-BE**

Checo: **cz-CZ**

Inglés: **en-GB**

Inglés (EE. UU.): **en-US**

Francés: **fr-FR**

Francés (Suiza): **fr-CH**

Alemán: **de-DE**

Alemán (Suiza): **de-CH**

Italiano: **it-IT**

Polaco **pl-PL**

Portugués **pt-PT**

Portugués (Brasil): **pt-BR**

Ruso: **ru-RU**

Serbio (cirílico): **sr-CR**

Serbio (latino): **sr-LT**

Español: **es-ES**

Al trabajar con dispositivos de arranque, utilice CTRL + MAYÚS para desplazarse por las disposiciones disponibles.

Scripts en dispositivo de arranque

Si desea que el dispositivo de arranque lleve a cabo un conjunto de operaciones determinado, puede especificar un script mientras crea el dispositivo en Bootable Media Builder. Cada vez que arranque el dispositivo, ejecutará este script en lugar de mostrar la interfaz del usuario.

Puede seleccionar uno de los scripts predefinidos o crear un script personalizado siguiendo las convenciones de scripts.

Scripts predefinidos

Bootable Media Builder proporciona los siguientes scripts predefinidos:

- Copia de seguridad en el almacenamiento en la nube y recuperación desde este (**entire_pc_cloud**)

- Copia de seguridad en el dispositivo de arranque y recuperación desde este (**entire_pc_cloud**)
- Copia de seguridad en la red compartida y recuperación desde esta (**entire_pc_cloud**)
- Recuperación desde el almacenamiento en la nube (**golden_image**)

Los scripts pueden encontrarse en el equipo en donde se ha instalado Bootable Media Builder, en los siguientes directorios:

- En Windows: %**ProgramData%\Acronis\MediaBuilder\scripts**
- En Linux: **/var/lib/Acronis/MediaBuilder/scripts/**

Copia de seguridad en el almacenamiento en la nube y recuperación desde este

Este script realizará una copia de seguridad de un equipo en el almacenamiento en la nube o recuperará el equipo desde la copia de seguridad más reciente creada en el almacenamiento en la nube por el mismo script. Al iniciarse, el script pedirá al usuario elegir entre la copia de seguridad, recuperación e iniciar la interfaz del usuario.

En Bootable Media Builder, especifique los siguientes parámetros del script:

1. El nombre de usuario y la contraseña del almacenamiento de la nube.
2. [Opcional] Una contraseña que el script utilizará para cifrar las copias de seguridad o acceder a estas.

Copia de seguridad en el dispositivo de arranque y recuperación desde este

Este script realizará una copia de seguridad de un equipo en el dispositivo de arranque o recuperará el equipo desde la copia de seguridad más reciente creada en el dispositivo de arranque por el mismo script. Al iniciarse, el script pedirá al usuario elegir entre la copia de seguridad, recuperación e iniciar la interfaz del usuario.

En Bootable Media Builder, puede especificar una contraseña que el script utilizará para cifrar las copias de seguridad o acceder a estas.

Copia de seguridad en la red compartida y recuperación desde esta

Este script realizará una copia de seguridad de un equipo en una red compartida o recuperará el equipo desde la copia de seguridad más reciente ubicada en la red compartida. Al iniciarse, el script pedirá al usuario elegir entre la copia de seguridad, recuperación e iniciar la interfaz del usuario.

En Bootable Media Builder, especifique los siguientes parámetros del script:

1. La ruta de la red compartida.
2. El nombre de usuario y la contraseña de la red compartida.
3. [Opcional] El nombre del archivo de la copia de seguridad. El valor predeterminado es **Copia de seguridad automática**. Si quiere que el script anexe las copias de seguridad a una copia de seguridad ya existente o que las recupere de una copia de seguridad con un nombre no determinado, cambie el valor predeterminado al nombre del archivo de esta copia de seguridad.

El nombre del archivo de la copia de seguridad

a. En la consola web de Cyber Protect, vaya a **Almacenamiento de copias de seguridad** > **Ubicaciones**.

b. Seleccione la red compartida (haga clic en **Añadir ubicación** si la red compartida no aparece en la lista).

c. Seleccione la copia de seguridad.

d. Haga clic en **Detalles**. El nombre del archivo se muestra en **Nombre del archivo de la copia de seguridad**.

4. [Opcional] Una contraseña que el script utilizará para cifrar las copias de seguridad o acceder a estas.

Recuperación desde el almacenamiento en la nube

Este script recuperará el equipo desde la copia de seguridad más reciente ubicada en el almacenamiento en la nube. Al iniciarse, el script pedirá al usuario que especifique:

1. El nombre de usuario y la contraseña del almacenamiento de la nube.
2. Si la copia de seguridad está cifrada, introduzca la contraseña.

Le recomendamos almacenar sus copias de seguridad de un solo equipo en esta cuenta de almacenamiento en la nube. De no ser así, si una copia de seguridad de otro equipo es más nueva que la copia de seguridad del equipo actual, el script elegirá la copia de seguridad de ese otro equipo.

Scripts personalizados

Importante
Crear scripts personalizados requiere conocimientos de lenguaje de comandos Bash y JavaScript Object Notation (JSON). Si no está familiarizado con Bash, un buen lugar para aprender es http://www.tldp.org/LDP/abs/html. La especificación de JSON está disponible en http://www.json.org.

Archivos de un script

El script debe estar ubicado en los directorios siguientes del equipo en el que esté instalado Bootable Media Builder:

- En Windows: %**ProgramData%\Acronis\MediaBuilder\scripts**
- En Linux: **/var/lib/Acronis/MediaBuilder/scripts/**

El script debe constar de tres archivos como mínimo:

- **<script_file>.sh** - un archivo con su script Bash. Al crear el script, utilice únicamente un conjunto limitado de comandos shell, que podrá encontrar en https://busybox.net/downloads/BusyBox.html. Además, se pueden utilizar los comandos siguientes:

- `acrocmd` - la utilidad de línea de comandos para copia de seguridad y recuperación
- `product` - el comando que inicia la interfaz de usuario del dispositivo de arranque

Este archivo y cualquier otro que incluya el script (por ejemplo, utilizando el comando dot) deben ubicarse en la subcarpeta **bin**. En el script, especifique las rutas de los archivo adicionales como **/ConfigurationFiles/bin/<some_file>**.

- **autostart** - un archivo para iniciar **<script_file>.sh**. El contenido del archivo debe ser el siguiente:

```
#!/bin/sh
. /ConfigurationFiles/bin/variables.sh
. /ConfigurationFiles/bin/<script_file>.sh
. /ConfigurationFiles/bin/post_actions.sh
```

- **autostart.json** - un archivo JSON que contiene lo siguiente:
  - El nombre y la descripción del script que aparecerá en Bootable Media Builder.
  - Los nombres de las variables del script que desea configurar mediante Bootable Media Builder.
  - Los parámetros de los controles que aparecerán en Generador de dispositivos de inicio para cada variable.

Estructura de autostart.json

Objeto de nivel superior

Pareja		Obligatorio	Descripción
Nombre	**Tipo de valor**		
`displayName`	string	Sí	El nombre de script que aparecerá en el Generador de dispositivos de inicio.
`description`	string	No	La descripción del script que aparecerá en el Generador de dispositivos de inicio.
`timeout`	number	No	El tiempo de espera (en segundos) del menú de arranque antes de que se inicie el script. Si no se especifica la pareja, el tiempo de espera será de diez segundos.
`variables`	objeto	No	Las variables de **<script_file>.sh** que desee configurar a través del Generador de dispositivos de inicio. El valor debe ser un conjunto de las parejas siguientes: el identificador de la cadena de una variable y el objeto de la variable (consulte la tabla que aparece a continuación).

Objeto de variable

Pareja		Obligatorio	Descripción
Nombre	**Tipo de valor**		
`displayName`	string	Sí	El nombre de la variable utilizado en **<script_file>.sh**.
`type`	string	Sí	El tipo de control que aparece en el Generador de dispositivos de inicio. Este control se utiliza para configurar el valor de la variable. Para todos los tipos admitidos, consulte la tabla que aparece a continuación.
`description`	string	Sí	La etiqueta de control que aparece encima del control en el Generador de dispositivos de inicio.
`default`	cadena si el `type` es `string`, `multiString`, `password` o `enum` número si el `type` es `number`, `spinner` o `checkbox`	No	El valor predeterminado para el control. Si no se especifica la pareja, el valor predeterminado será una cadena vacía o un cero, dependiendo del tipo de control. El valor predeterminado de una casilla de verificación puede ser `0` (el estado borrado) o `1` (el estado seleccionado).
`order`	number (no negativo)	Sí	La petición de control en el Generador de dispositivos de inicio. Cuanto más alto sea el valor, más bajo será el control colocado en relación a otros controles definidos en **autostart.json**. El valor inicial debe ser `0`.
`min` (solo para `spinner`)	number	No	El valor mínimo del control de número en un cuadro de número. Si no se especifica la pareja, el valor será `0`.
`max` (solo para `spinner`)	number	No	El valor máximo del control de número en un cuadro de número. Si no se especifica la pareja, el valor será `100`.
`step`	number	No	El valor de paso del control de número de un cuadro de número. Si no se especifica la pareja, el valor

(solo para `spinner`)			será `1`.
`items` (solo para `enum`)	matriz de cadenas	Sí	Los valores de una lista desplegable.
`required` (para `string`, `multiString`, `password` y `enum`)	number	No	Especifica si el valor del control puede estar vacío (`0`) o no (`1`). Si no se especifica la pareja, el valor de control puede estar vacío.

Tipo de control

Nombre	Descripción
`string`	Un cuadro de texto sin límite y en una sola línea que se utiliza para introducir o modificar cadenas cortas.
`multiString`	Un cuadro de texto sin límite y en varias líneas que se utiliza para introducir o modificar cadenas largas.
`password`	Un cuadro de texto sin límite y en una sola línea que se utiliza para introducir contraseñas de forma segura.
`number`	Un cuadro de texto numérico y en una sola línea que se utiliza para introducir o modificar números.
`spinner`	Un cuadro de texto numérico y en una sola línea que se utiliza para introducir o modificar números con un control de números denominado cuadro de número.
`enum`	Una lista desplegable estándar, con un conjunto fijo de valores predeterminados.
`checkbox`	Una casilla de verificación con dos estados, el estado borrado o el estado seleccionado.

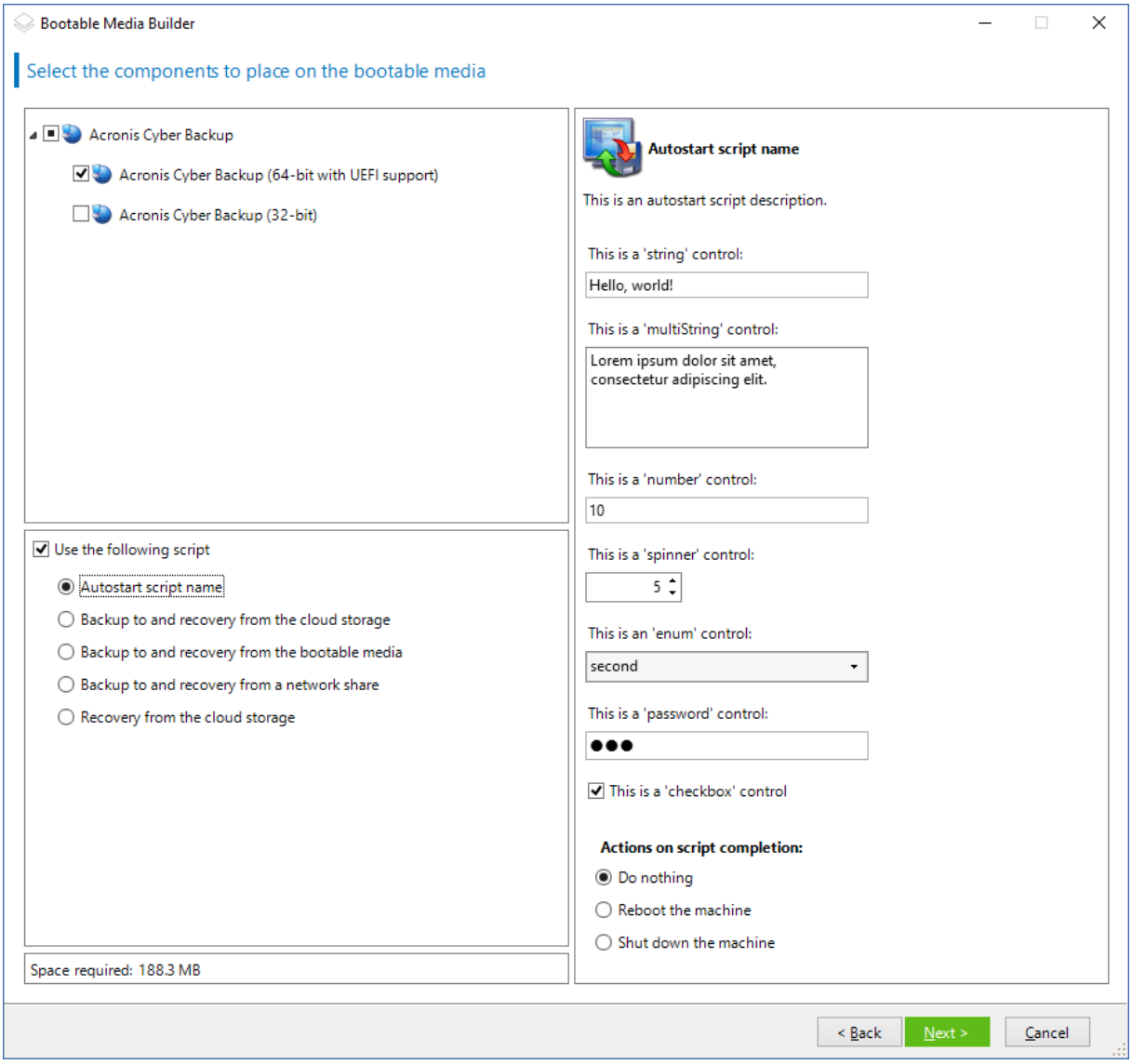
El ejemplo **autostart.json** que aparece a continuación contiene todos los tipos posibles de controles que se pueden utilizar para configurar variables para **<script_file>.sh**.

```
{
        "displayName": "Autostart script name",
        "description": "This is an autostart script description.",
        "variables": {
                "var_string": {
                        "displayName": "VAR_STRING",
```

```
                "type": "string", "order": 1,
                "description": "This is a 'string' control:", "default": "Hello,
world!"
        },
        "var_multistring": {
                "displayName": "VAR_MULTISTRING",
                "type": "multiString", "order": 2,
                "description": "This is a 'multiString' control:",
                "default": "Lorem ipsum dolor sit amet,\nconsectetur adipiscing elit."
        },
        "var_number": {
                "displayName": "VAR_NUMBER",
                "type": "number", "order": 3,
                "description": "This is a 'number' control:", "default": 10
        },
        "var_spinner": {
                "displayName": "VAR_SPINNER",
                "type": "spinner", "order": 4,
                "description": "This is a 'spinner' control:",
                "min": 1, "max": 10, "step": 1, "default": 5
        },
        "var_enum": {
                "displayName": "VAR_ENUM",
                "type": "enum", "order": 5,
                "description": "This is an 'enum' control:",
                "items": ["first", "second", "third"], "default": "second"
        },
        "var_password": {
                "displayName": "VAR_PASSWORD",
                "type": "password", "order": 6,
                "description": "This is a 'password' control:", "default": "qwe"
```

```
        },
        "var_checkbox": {
                "displayName": "VAR_CHECKBOX",
                "type": "checkbox", "order": 7,
                "description": "This is a 'checkbox' control", "default": 1
        }
    }
}
```

Este es el aspecto que tiene en el Generador de dispositivos de inicio.



Servidor de gestión

Cuando crea dispositivos de arranque, tiene la opción de preconfigurar el registro de medios en el servidor de gestión.

El registro de dispositivos le permite gestionar los dispositivos a través de la consola web de Cyber Protect como si se tratase de un equipo registrado. Además de la comodidad de disponer de acceso remoto, esto garantiza a un administrador la capacidad de rastrear todas las operaciones que se hayan llevado a cabo a partir de dispositivos de arranque. Las operaciones son **Actividades** registradas, por lo que es posible ver quién ha iniciado una operación y cuándo.

Si el registro no ha sido preconfigurado, todavía es posible registrar el dispositivo después de arrancar el equipo a partir de este.

Para preconfigurar el registro en el servidor de gestión

1. Seleccione la casilla de verificación **Registro de dispositivos en el servidor de gestión**.
2. En el **Nombre o dirección IP del servidor**, especifique el nombre del servidor o la dirección IP del equipo donde está instalado el servidor de gestión. Podrá utilizar uno de los siguientes formatos:
   - `http://<server>`. Por ejemplo, `http://10.250.10.10` o `http://server1`
   - `<IP address>`. Por ejemplo, `10.250.10.10`
   - `<host name>`. Por ejemplo, `server1` o `server1.example.com`
3. En **Puerto**, especifique el puerto que se deberá usar para acceder al servidor de gestión. El preajuste es 9877.
4. En **Mostrar nombre**, especifique el nombre que deberá mostrarse para este equipo en la consola web de Cyber Protect. Si usted deja este campo vacío, el nombre para mostrar se configurará en uno de los siguientes:
   - Si el equipo se ha registrado previamente en el servidor de gestión, tendrá el mismo nombre.
   - De lo contrario, se utilizarán el nombre de dominio completamente cualificado (FQDN) o la dirección IP del equipo
5. Seleccione qué cuenta se debe utilizar para registrar los medios en el servidor de gestión. Las siguientes opciones están disponibles:
   - **Solicitar nombre de usuario y contraseña durante el arranque**

     Las credenciales deberán proporcionarse cada vez que se arranque un equipo desde un dispositivo.

     Para un registro correcto, la cuenta debe figurar en la lista de administradores del servidor de gestión (**Configuración** > **Cuentas**). En la consola web de Cyber Protect, los dispositivos estarán disponibles bajo la organización o bajo una unidad específica, en función de los permisos otorgados a esa cuenta especificada.

     En la interfaz del dispositivo de arranque, se podrá cambiar el nombre de usuario y la contraseña haciendo clic en **Herramientas** > **Registrar dispositivo en el servidor de gestión**.

- **Registrar con la siguiente cuenta**

  El equipo se registrará automáticamente cada vez que se arranque desde un dispositivo.

  La cuenta que especifique debe figurar en la lista de administradores del servidor de gestión (**Configuración** > **Cuentas**). En la consola web de Cyber Protect, los dispositivos estarán disponibles bajo la organización o bajo una unidad específica, en función de los permisos otorgados a esa cuenta especificada.

  En la interfaz del dispositivo de arranque, *no* se podrán cambiar los parámetros de registro.

Configuraciones de red

Mientras crea el dispositivo de arranque, tiene la opción de preconfigurar las conexiones de red que usará el agente de arranque. Se pueden preconfigurar los siguientes parámetros:

- Dirección IP
- Máscara de subred
- Puertas de enlace
- Servidor DNS
- Servidor WINS.

Una vez que se inicia el agente de arranque en un equipo, se aplica la configuración en la tarjeta de interfaz de red (NIC) del equipo. Si no se preconfiguran las configuraciones, el agente usa la configuración automática del servidor DHCP. También tienen la capacidad de establecer manualmente la configuración de red cuando se ejecuta el agente de inicio en el equipo.

Preconfiguración de múltiples conexiones de red

Puede preestablecer la configuración TCP/IP de hasta 10 tarjetas de interfaz de red. Para asegurar que cada NIC tendrá asignada la configuración adecuada, cree el dispositivo en el servidor en donde se personalizan los dispositivos. Cuando seleccione la NIC existente en al agente de Windows, se selecciona su configuración para guardarlos en el dispositivo. También se guarda la dirección MAC de cada NIC en los dispositivos.

Puede cambiar la configuración, excepto por la dirección MAC, o establecer la configuración para una NIC no existente, de ser necesario.

Una vez que el dispositivo de inicio se ejecute en el servidor, recupera la lista de NIC disponibles. Esta lista está ordenada por las ranuras que ocupan las NIC: las más cercanas al procesador están en la parte superior.

El agente de inicio asigna la configuración apropiada a cada NIC conocida y las identifica por sus direcciones MAC. Después de que se configuran las NIC con direcciones MAC conocidas, se asigna la configuración que realizó para NIC no existentes a las NIC restantes, comenzando por la NIC no asignada superior.

Puede personalizar los dispositivos de arranque para cualquier equipo, y no sólo para el equipo en donde se crea el dispositivo. Para hacerlo, configure las NIC de acuerdo con el orden de ranuras del

equipo. Nic1 ocupa la ranura más cercana al procesador, NIC2 es la siguiente ranura. Cuando el agente de inicio se ejecuta en el equipo, no encontrará NIC con direcciones MAC conocidas y configurará las NIC en el mismo orden que usted.

Ejemplo

El agente de arranque podría usar uno de los adaptadores de red para la comunicación con la consola de administración por medio de la red de producción. Se podría establecer la configuración automática para esta conexión. Se pueden transferir los datos que se pueden dividir para su recuperación por la segunda NIC, incluida en la red de copia de seguridad por medio de la configuración TCP/IP.

Puerto de red

Cuando crea un dispositivo de arranque, tiene la opción de preconfigurar el puerto de red que el agente de arranque escuchará para la conexión entrante desde la utilidad `acrocmd`. Puede elegir entre:

- el puerto predeterminado
- el puerto usado actualmente
- el puerto nuevo (introduzca el número de puerto)

Si no se preconfiguró el puerto, el agente usa el puerto 9876.

Controladores para Universal Restore

Cuando crea dispositivos de arranque, tiene la opción de agregar controladores para Windows al dispositivo. Universal Restore utilizará los controladores para arrancar el sistema operativo Windows migrado a un hardware diferente.

Entonces podrá configurar Universal Restore:

- para buscar los controladores en los dispositivos que mejor se ajustan con el hardware de destino.
- para obtener los controladores de almacenamiento masivo que especifica desde el dispositivo. Esto debe hacerse cuando el hardware de destino tiene el controlador para almacenamiento masivo (como adaptador SCSI, RAID, o Fiber Channel) para el disco duro.

Los controladores serán ubicados en la carpeta de controladores visibles en el dispositivo de arranque. No se cargan los controladores en la memoria RAM del equipo de destino, el dispositivo debe estar insertado o conectado por medio de la operación de Universal Restore.

Puede agregar controladores a un dispositivo de arranque cuando crea un dispositivo extraíble o su ISO o medio extraíble, como una unidad de memoria flash. Los controladores no se pueden cargar en WDS/RIS.

Se pueden agregar los controladores a la lista sólo en grupos, al agregar los archivos INF o carpetas que contienen dichos archivos. La selección de controladores individuales desde los archivos INF no es posible, pero el generador de dispositivos muestra el contenido del archivo para su información.

Para agregar unidades:

1. Haga clic en **Agregar** y navegue hasta el archivo INF o la carpeta que contiene los archivos INF.
2. Seleccione el archivo INF o la carpeta.
3. Haga clic en **Aceptar**.

Se pueden eliminar los controladores de la lista sólo en grupos, al eliminar los archivos INF.

Para eliminar los controladores:

1. Seleccione el archivo INF.
2. Haga clic en **Quitar**.

Dispositivos de arranque basados en WinPE y WinRE

Bootable Media Builder ofrece dos formas de integrar Acronis Cyber Protect con WinPE:

- Creación del PE ISO con el complemento desde cero.
- Añadir el complemento Acronis a un archivo WIM. Por ejemplo, para construir la imagen ISO manualmente o añadir otras herramientas a la imagen.

Puede crear imágenes basadas en WinRE sin ninguna preparación adicional, o crear imágenes basadas en WinPE después de instalar Windows Automated Installation Kit (AIK) o Windows Assessment and Deployment Kit (ADK).

Imágenes basadas en WinRE

La creación de imágenes basadas en WinRE es compatible con los siguientes sistemas operativos:

- Windows 7 (64 bits)
- Windows 8 (32 bits y 64 bits)
- Windows 8.1 (32 bits y 64 bits)
- Windows 10 (32 bits y 64 bits)
- Windows 11 (64 bits)
- Windows Server 2012 (64 bits)
- Windows Server 2016 (64 bits)
- Windows Server 2019 (64 bits)
- Windows Server 2022 (64 bits)

Imágenes basadas en WinPE

Después de instalar Windows Automated Installation Kit (AIK) o Windows Assessment and Deployment Kit (ADK), Bootable Media Builder es compatible con las distribuciones de WinPE que están basadas en cualquiera de los siguientes kernels:

- Windows Vista (PE 2.0)
- Windows Vista SP1 y Windows Server 2008 (PE 2.1)
- Windows 7 (PE 3.0) con o sin el complemento para Windows 7 SP1 (PE 3.1)
- Windows 8 (PE 4.0)
- Windows 8.1 (PE 5.0)
- Windows 10 (PE 10.0.1xxx)
- Windows 11 (PE 10.0.2xxx)

Bootable Media Builder es compatible con las distribuciones de 32 bits y 64 bits de WinPE. Las distribuciones de 32 bits de WinPE también funcionan en hardware de 64 bits. Sin embargo, necesita una distribución de 64 bits para arrancar un equipo que utiliza Unified Extensible Firmware Interface (UEFI).

Las imágenes PE basadas en WinPE 4 y versiones posteriores necesitan aproximadamente 1 GB de RAM para funcionar.

Nota
La funcionalidad de gestión del disco no está disponible para dispositivos de arranque basados en Windows PE 4.0 o posterior. Por lo tanto, la gestión del disco es compatible con Windows 7 y sistemas operativos anteriores. Para ejecutar operaciones de gestión del disco en Windows 8 y sistemas posteriores, debe instalar Acronis Disk Director. Para obtener más información, consulte este artículo de la Base de conocimientos: https://kb.acronis.com/content/47031.

Preparación: WinPE 2.x y 3.x

Para poder crear o modificar imágenes PE 2.x o 3.x, instale Bootable Media Builder y Windows Automated Installation Kit (AIK) en el equipo.

Pasos para preparar un equipo

1. Descargue el archivo de imagen AIK desde el sitio web de Microsoft de la siguiente manera:
   - Para Windows Vista (PE 2.0): https://www.microsoft.com/es-es/download/details.aspx?id=10333
   - Para Windows Vista SP1 y Windows Server 2008 (PE 2.1): https://www.microsoft.com/es-es/download/details.aspx?id=9085
   - Para Windows 7 (PE 3.0): https://www.microsoft.com/es-es/download/details.aspx?id=5753
     Para Windows 7 SP1 (PE 3.1), también necesita el suplemento AIK disponible en https://www.microsoft.com/es-es/download/details.aspx?id=5188

2. Grabe el archivo de imagen en un disco DVD o en una memoria USB.
3. Desde el archivo de imagen, instale lo siguiente:
   - Microsoft .NET Framework (NETFXx86 o NETFXx64, dependiendo de su hardware)
   - MSXML (Analizador XML de Microsoft)
   - Windows AIK
4. Instale Bootable Media Builder en el mismo equipo.

Preparación: WinPE 4.0 y posterior

Para poder crear o modificar imágenes PE 4 o posteriores, instale Bootable Media Builder y Windows Assessment and Deployment Kit (ADK) en el mismo equipo.

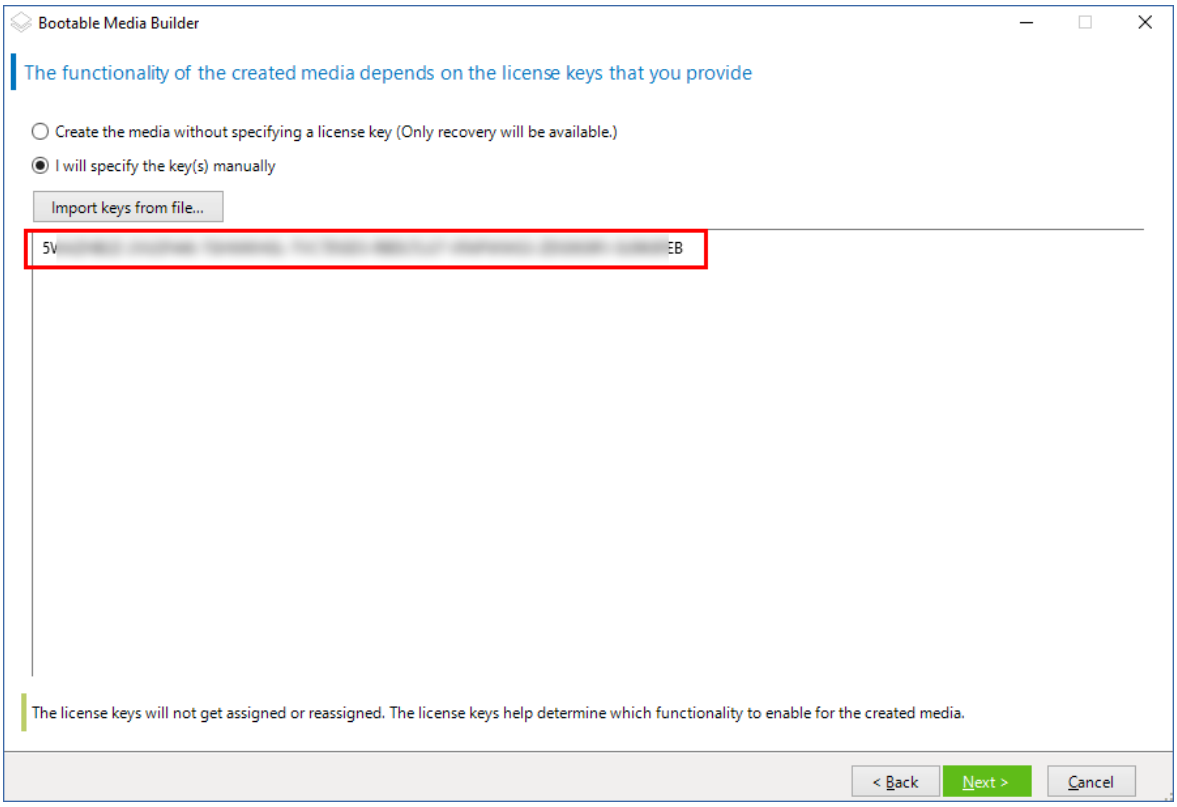
Pasos para preparar un equipo

1. Descargue el programa de configuración de ADK desde la página web de Microsoft.
   Las siguientes versiones de Windows son compatibles:
   - Windows 11 (PE 10.0.2xxx)
   - Windows 10 (PE 10.0.1xxx)
   - Windows 8.1 (PE 5.0)
   - Windows 8 (PE 4.0)
2. Instale Assessment and Deployment Kit.
3. Instale Bootable Media Builder.

Añadir el complemento Acronis a WinPE

Para añadir el complemento Acronis a WinPE:

1. Inicie Bootable Media Builder.
2. Para crear un dispositivo de arranque con todas las funciones, especifique una clave de licencia de Acronis Cyber Protect. Esta clave se utiliza para determinar las funciones que se incluirán en el dispositivo de arranque. No se revocarán las licencias de ningún equipo.
   Si no especifica una clave de licencia, el dispositivo de arranque resultante solo se usará para operaciones de recuperación.



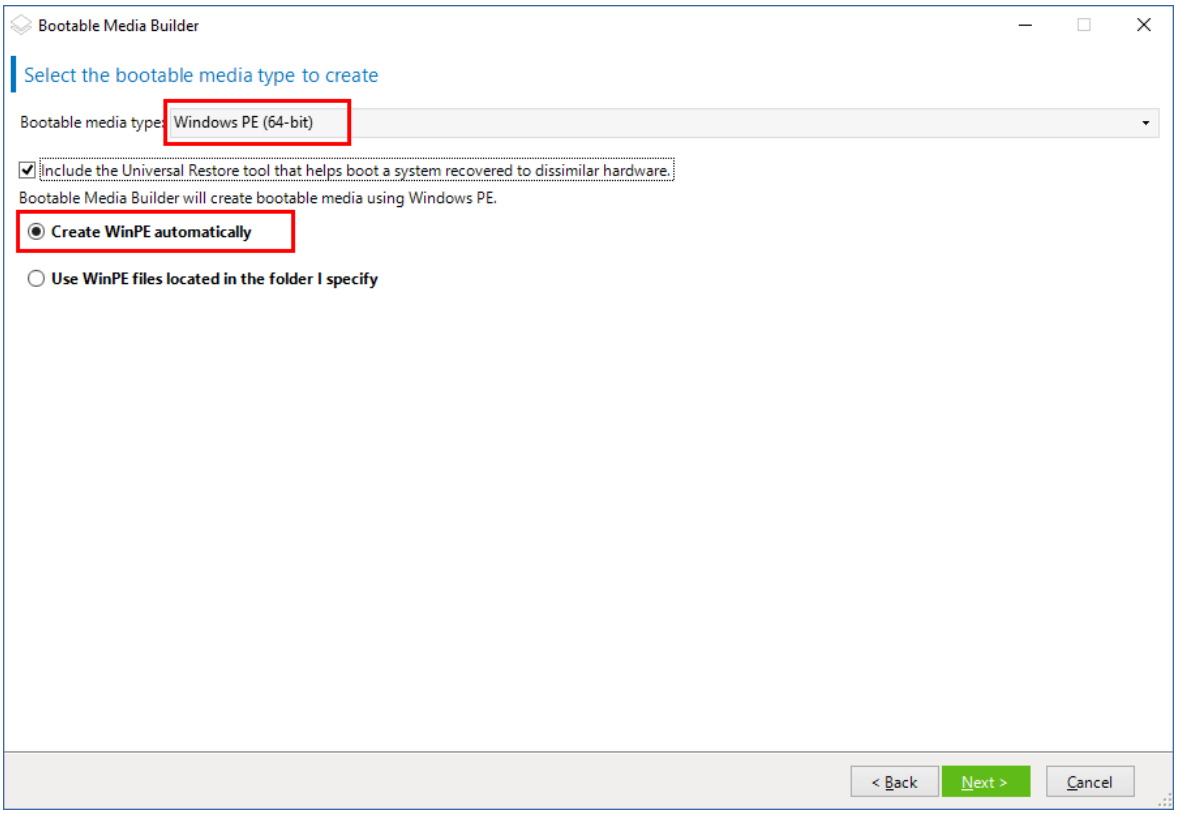
3. Seleccione **Tipo de dispositivo de arranque: Windows PE** o **Tipo de dispositivo de arranque: Windows PE (64 bits)**. Se necesita un dispositivo de 64 bits para arrancar un equipo que utiliza Unified Extensible Firmware Interface (UEFI).

   Si ha seleccionado **Tipo de dispositivo de arranque: Windows PE**, primero realice lo siguiente:

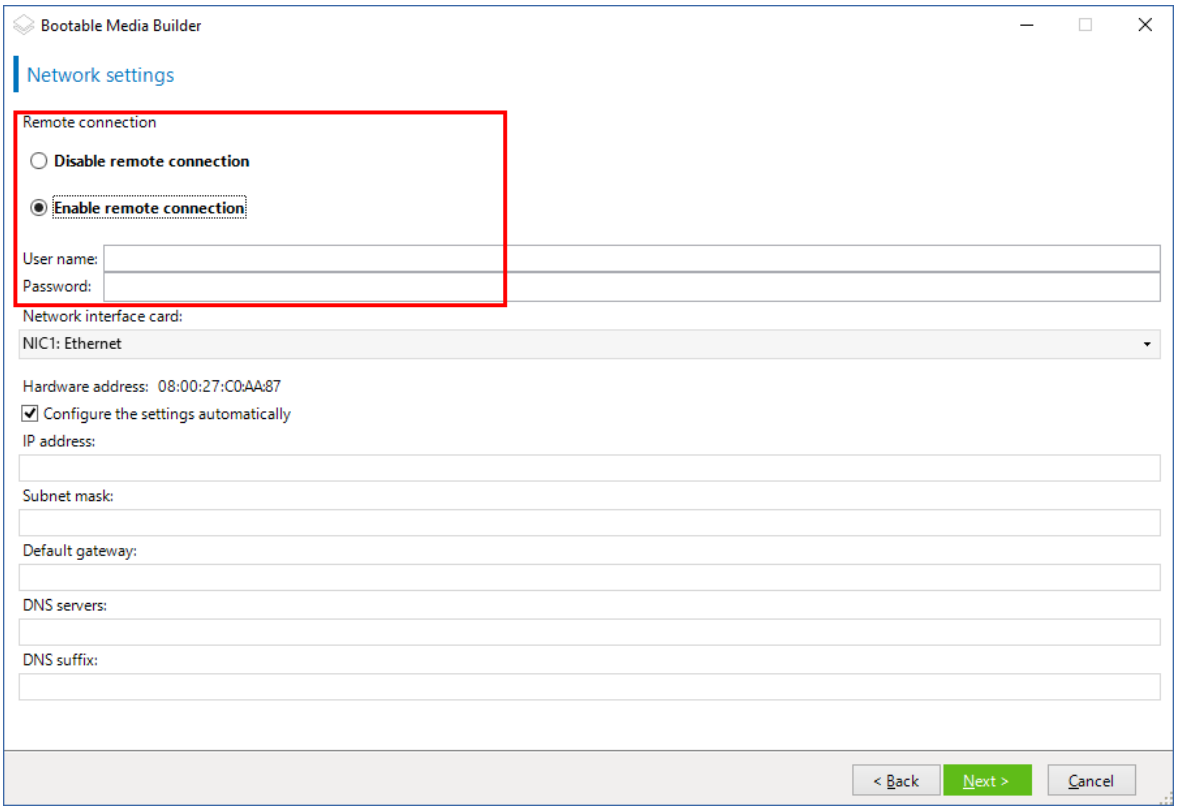
   - Haga clic en **Descargar complemento para WinPE (32 bits)**.
   - Guarde el complemento en **%PROGRAM_FILES%\Acronis\BootableComponents\WinPE32**.

   Si tiene previsto recuperar un sistema operativo en un hardware diferente o en un equipo virtual y desea asegurar la capacidad de arranque del sistema, seleccione la casilla de verificación **Incluir la herramienta Universal Restore...**
4. Seleccione **Crear WinPE automáticamente**.

   El software ejecuta la secuencia de comandos apropiada y continúa a la siguiente ventana.



5. Seleccione el idioma que se utilizará en el dispositivo de arranque.
6. Seleccione si desea habilitar o deshabilitar la conexión remota a un equipo que se arranca desde el medio. Si se habilita, introduzca un nombre de usuario y una contraseña para que se puedan especificar en la línea de comando si la utilidad `acrocmd` se ejecuta en un equipo distinto.
   También puede dejar estas casillas vacías, por lo que podrá conectarse de forma remota a través de la interfaz de la línea de comando sin credenciales.
   Estas credenciales también son necesarias al registrar el dispositivo en el servidor de gestión desde la consola web de Cyber Protect.



7. Especifique las configuraciones de red de los adaptadores de red del equipo o elija la configuración automática DHCP.

Nota
La configuración de la red solo está disponible con licencias de Acronis Cyber Protect 15 Advanced y Acronis Cyber Protect 15 Backup Advanced. Para obtener una comparación detallada de la función, consulte este artículo de la base de conocimientos.

8. [Opcional] Seleccione cómo deben registrarse los dispositivos en el servidor de gestión al arrancar. Para obtener más información sobre la configuración de registro, consulte la sección Servidor de gestión.
9. [Opcional] Especifique los controladores de Windows que se deben añadir a Windows PE.

   Cuando haya iniciado su equipo en Windows PE, los controladores le ayudarán a acceder al dispositivo donde está ubicada la copia de seguridad. Añada los controladores de 32 bits si utiliza una distribución de 32 bits de WinPE o controladores de 64 bits si utiliza una distribución de 64 bits de WinPE.

   Además, podrá apuntar a los controladores añadidos al configurar Universal Restore para Windows. En Universal Restore, añada los controladores de 32 bits o 64 bits según esté planificando recuperar un sistema operativo de Windows de 32 bits o 64 bits.

   Para añadir los controladores:

   - Haga clic en **Añadir** y especifique la ruta al archivo .inf necesario para el correspondiente controlador SCSI, RAID o SATA, adaptador de red, unidad de cinta u otro dispositivo.

- Repita este procedimiento para cada controlador que desee incluir en el medio WinPE resultante.

10. Escoja si desea crear una imagen ISO o WIM o cargar el medio en un servidor (WDS o RIS).
11. Especifique la ruta completa al archivo de imagen que se obtendrá incluyendo el nombre del archivo o especifique el servidor y proporcione el nombre de usuario y la contraseña para acceder a él.
12. Compruebe su configuración en la pantalla de resumen y haga clic en **Continuar**.
13. Grabe el .ISO en un CD o DVD con una herramienta de otra empresa o prepárelo en una unidad de memoria flash de arranque.

Una vez que el equipo se inicia en WinPE, el agente se inicia automáticamente.

Para crear una imagen PE (archivo ISO) del archivo WIM resultante:

- Reemplace el archivo boot.wim predeterminado en su carpeta de Windows PE junto al archivo WIM creado recientemente. Para el ejemplo anterior, escriba:

```
copy c:\AcronisMedia.wim c:\winpe_x86\ISO\sources\boot.wim
```

- Use la herramienta **Oscdimg**. Para el ejemplo anterior, escriba:

```
oscdimg -n -bc:\winpe_x86\etfsboot.com c:\winpe_x86\ISO c:\winpe_x86\winpe_x86.iso
```

Advertencia.
No copie y pegue este ejemplo. Introduzca el comando manualmente o de lo contrario fallará.

Para obtener más información sobre cómo personalizar Windows PE 2.x y 3.x, consulte el manual de usuario de Entorno de preinstalación de Windows (Winpe.chm). La información acerca de la personalización de Windows PE 4.0 y posterior está disponible en la biblioteca Microsoft TechNet.

Conexión a un equipo que se inició desde un medio

Una vez que un equipo inicia desde un dispositivo de arranque, la terminal del equipo muestra una ventana de inicio con la dirección IP que el servidor DHCP proporcionó o la establecida de acuerdo a los valores preconfigurados.

Configurar los ajustes de red

Para cambiar los ajustes red de la sesión actual, haga clic en **Configurar red** en la ventana de inicio. La ventana **Configuraciones de red** que aparece le permitirá configurar los ajustes de red de cada tarjeta de interfaz de red (NIC) del equipo.

Los cambios realizados durante una sesión se perderán cuando se reinicie el equipo.

Añadir VLAN

En la ventana **Configuraciones de red** puede añadir redes de área local virtual (VLAN). Utilice esta función si precisa acceder a la ubicación de una copia de seguridad incluida en una VLAN específica.

Las VLAN se utilizan principalmente para dividir una red de área local en segmentos. Las NIC conectadas a un puerto de *acceso* del conmutador pueden acceder a la VLAN especificada en la configuración del puerto. Las NIC conectadas a un puerto *troncal* del conmutador pueden acceder a las VLAN incluidas en la configuración del puerto únicamente si especifica la VLAN en las configuraciones de red.

Para habilitar el acceso a una VLAN mediante un puerto troncal

1. Haga clic en **Añadir VLAN**.
2. Seleccione la NIC que proporciona el acceso a la red de área local en la que se incluye la VLAN necesaria.
3. Especifique el identificador de la VLAN.

Después de hacer clic en **Aceptar**, aparecerá una entrada nueva en la lista de adaptadores de red.

Si desea eliminar una VLAN, seleccione la entrada de la VLAN correspondiente y, a continuación, en **Eliminar la VLAN**.

Conexión local

Para realizar la operación directamente en el equipo iniciado desde el dispositivo de arranque, haga clic en **Gestionar este equipo localmente** en la ventana de inicio.

Conexión remota

Para conectarse al dispositivo de forma remota, regístrelo en el servidor de gestión, como se indica en "Registro de dispositivos en el servidor de gestión".

Registro de dispositivos en el servidor de gestión

El registro de dispositivos de arranque le permite gestionar los dispositivos a través de la consola web de Cyber Protect como si se tratase de un equipo registrado. Este se aplica a todos los dispositivo de arranque independientemente del método de arranque (dispositivos físicos, Startup Recovery Manager, Acronis PXE Server, WDS o RIS). Sin embargo, no es posible registrar dispositivo de arranque creados en el sistema operativo Mac.

El registro de dispositivos únicamente es posible si se añade al menos una licencia avanzada de Acronis Cyber Protect al servidor de gestión.

Puede registrar el dispositivo desde la IU del mismo.

Se pueden configurar con antelación los parámetros de registro en la opción servidor de gestión de Bootable Media Builder. Si se configuran con anterioridad todos los parámetros de registro, los

dispositivos aparecerán en la consola web de Cyber Protect de manera automática. Si solo se configuran con anterioridad parte de los parámetros, puede que algunos pasos de los procedimientos siguientes no estén disponibles.

Registro de los dispositivos desde la IU del dispositivo

Se puede crear o descargar el dispositivo con Bootable Media Builder.

Para registrar dispositivos desde la IU del dispositivo

1. Inicie el equipo desde el disco o la unidad USB.
2. Realice uno de los siguientes procedimientos:
   - En la ventana de inicio, en **Servidor de gestión**, haga clic en **Editar**.
   - En la interfaz del dispositivo de arranque, haga clic en **Herramientas** > **Registrar dispositivo en el servidor de gestión**.
3. En **Registrado en**, especifique el nombre del servidor o la dirección IP del equipo donde está instalado el servidor de gestión. Podrá utilizar uno de los siguientes formatos:
   - `http://<server>`. Por ejemplo, `http://10.250.10.10` o `http://server`
   - `<IP address>`. Por ejemplo, `10.250.10.10`
   - `<host name>`. Por ejemplo, `server` o `server.example.com`
4. En **Nombre de usuario** y **Contraseña**, proporcione las credenciales de una cuenta que está en la lista de administradores del servidor de gestión (**Configuración** > **Cuentas**). En la consola web de Cyber Protect, los dispositivos estarán disponibles bajo la organización o bajo una unidad específica, en función de los permisos otorgados a esa cuenta especificada.
5. En **Mostrar nombre**, especifique el nombre que deberá mostrarse para este equipo en la consola web de Cyber Protect. Si usted deja este campo vacío, el nombre para mostrar se configurará en uno de los siguientes:
   - Si el equipo se ha registrado previamente en el servidor de gestión, tendrá el mismo nombre.
   - De lo contrario, se utilizarán el nombre de dominio completamente cualificado (FQDN) o la dirección IP del equipo
6. Haga clic en **Aceptar**.

Operaciones locales con dispositivos de arranque

Las operaciones con el dispositivo de arranque son similares a las operaciones de recuperación y de copia de seguridad que se llevan a cabo en un sistema operativo actualmente en ejecución. Las diferencias son las siguientes:

1. En un dispositivo de arranque con un volumen de representación de tipo Windows, un volumen tiene la misma letra de unidad que en Windows. A los volúmenes que no tienen letras de unidad en Windows (como el volumen Reservado del sistema) se les asignan letras según el orden de su secuencia en el disco.

Si el dispositivo de arranque no puede detectar Windows en el equipo o detecta más de uno, se asigna una letra a todos los volúmenes, incluidos aquellos que no tienen letra de unidad de disco, según el orden de su secuencia en el disco. Por eso, es posible que las letras de los volúmenes no coincidan con las de Windows. Por ejemplo, la unidad D: del dispositivo de arranque podría corresponder a la unidad E: de Windows.

Nota
Le recomendamos que asigne nombres únicos a los volúmenes.

2. Los dispositivos de arranque con la representación del volumen de estilo Linux muestran los discos y volúmenes locales como desmontados (sda1, sda2...).
3. Las copias de seguridad creadas con un dispositivo de arranque tienen nombres de archivo simplificados. Los nombres estándares se asignan a las copias de seguridad solo si se añaden a un archivo comprimido existente con una asignación de nombres estándar o si el destino no admite los nombres de archivo simplificados.
4. El dispositivo de arranque con la representación del volumen de estilo Linux no puede realizar copias de seguridad en un volumen formateado con NTFS. Si es necesario, cambie a un medio con un volumen de representación de estilo Windows. Para cambiar las representaciones del volumen del dispositivo de arranque, haga clic en **Herramientas** > **Cambiar representación del volumen**.
5. No se pueden planificar las tareas. Si necesita repetir una operación, configúrela desde cero.
6. La vida útil del registro se limita a la sesión actual. Puede guardar todo el registro o las entradas del registro filtradas a en un archivo.
7. Las bóvedas centralizadas no se muestran en el árbol de carpetas de la ventana de **Archivos**.
   Para acceder a una bóveda gestionada, escriba la siguiente cadena en el campo de **Ruta**:
   bsp://dirección_nodo/nombre_bóveda/
   Para acceder a una bóveda centralizada sin gestionar, escriba la ruta completa de la carpeta de la bóveda.
   Después de introducir las credenciales de acceso, verá una lista de los archivos comprimidos que se encuentran en la bóveda.

Configuración del modo de visualización

Cuando inicia un equipo desde un dispositivo de arranque basado en Linux, se detecta automáticamente un modo de vídeo de visualización basado en la configuración del hardware (especificaciones de la tarjeta del monitor y de los gráficos). Si el modo vídeo se detecta de manera incorrecta, realice lo siguiente:

1. Pulse F11 en el menú de inicio.
2. En la línea de comando, introduzca lo siguiente: **Vga=ask** y prosiga con el arranque.
3. En la lista de modos de vídeo compatibles, escoja el correcto al escribir su número (por ejemplo, **318**) y pulse **Intro**.

Si no desea seguir este procedimiento cada vez que inicie una configuración de hardware en concreto, cree de nuevo el dispositivo de arranque con el número de modo apropiado (en el ejemplo anterior, **vga=0x318**) escrito en la ventana **Parámetros del kernel**.

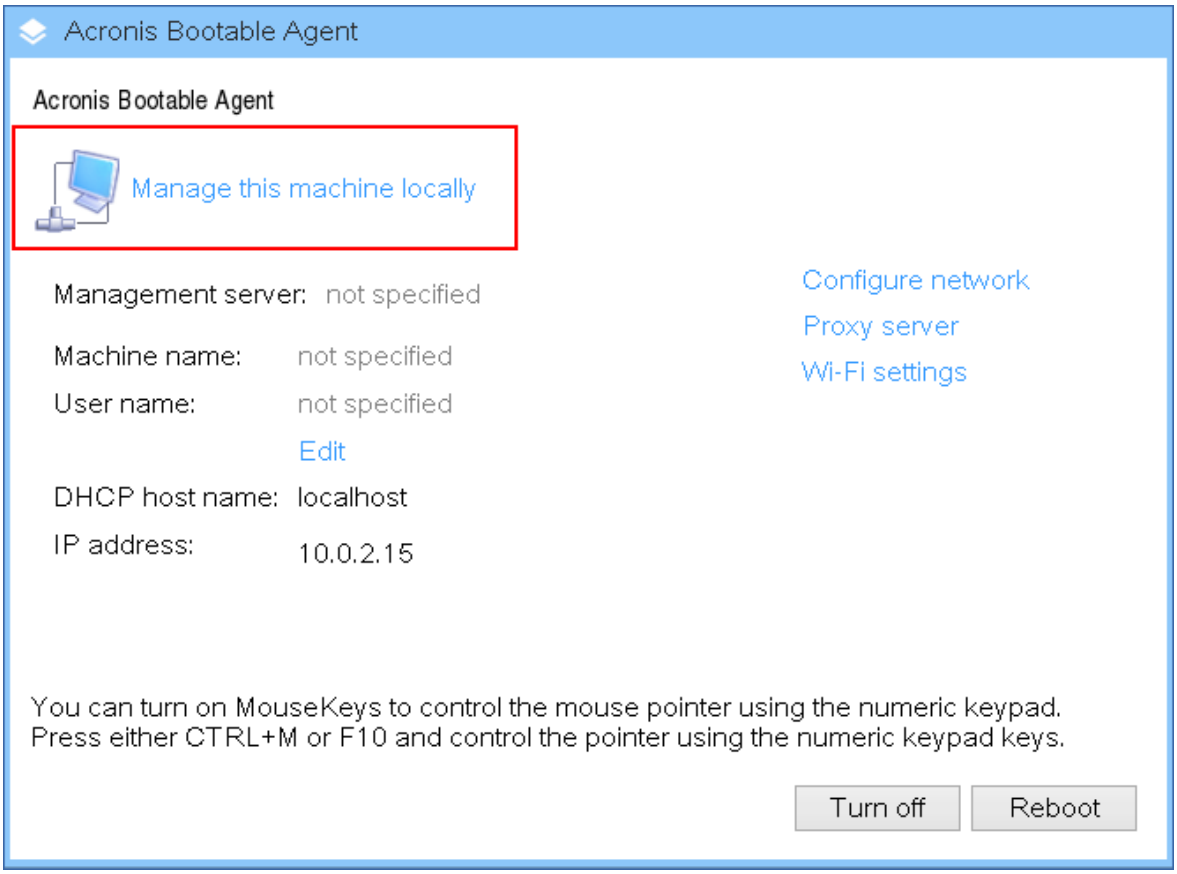
Copia de seguridad con soporte de arranque in situ

Puede crear una copia de seguridad de datos solo con un dispositivo de arranque que haya creado con Bootable Media Builder y su clave de licencia de Acronis Cyber Protect. Para obtener más información sobre cómo crear dispositivos de arranque, consulte Dispositivos de arranque basados en Linux o Dispositivos de arranque basados en Windows-PE respectivamente.

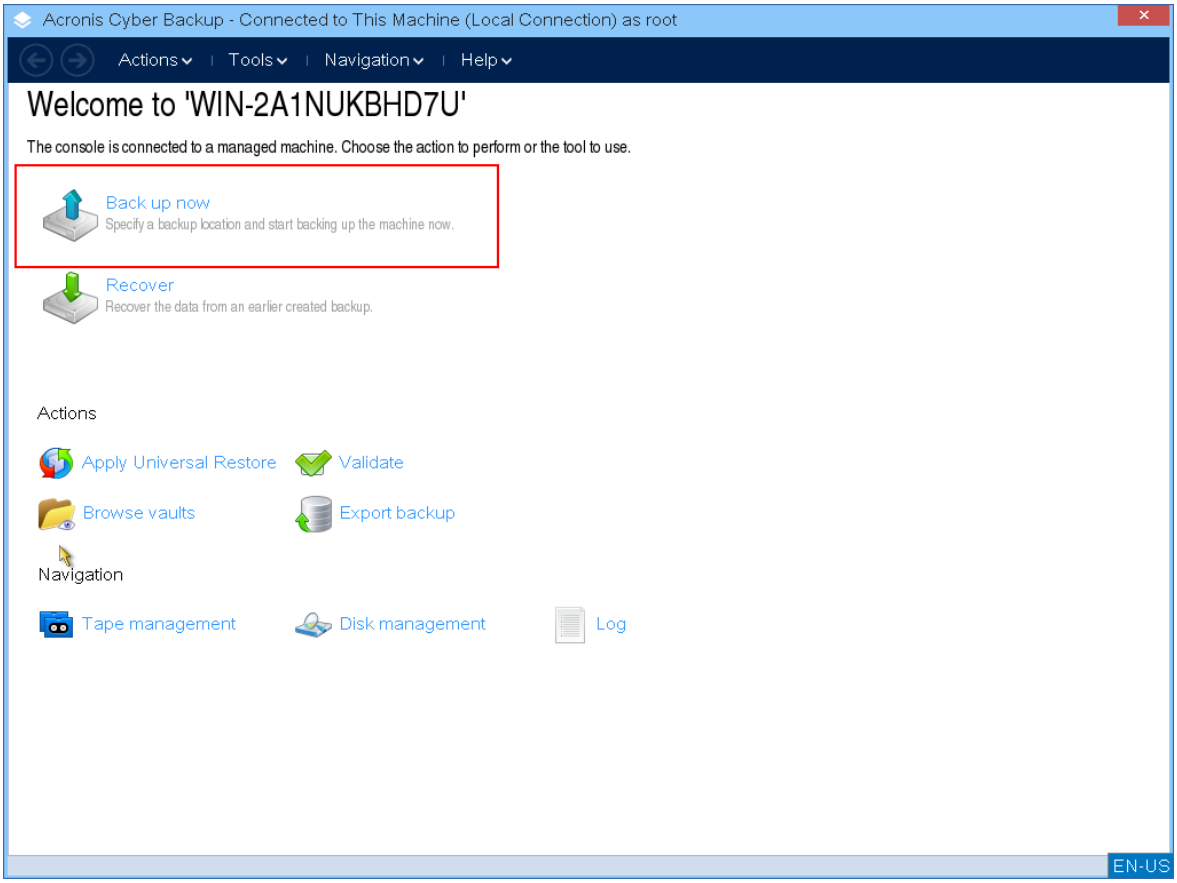
Pasos para crear copia de seguridad de datos mediante un dispositivo de arranque

1. Inicie desde el dispositivo de rescate de arranque de Acronis.

2. Para hacer una copia de seguridad del equipo local, haga clic en **Gestionar este equipo localmente**. Para conexiones remotas, consulte Registro de dispositivos en el servidor de gestión.



3. Haga clic en **Crear copia de seguridad ahora**.

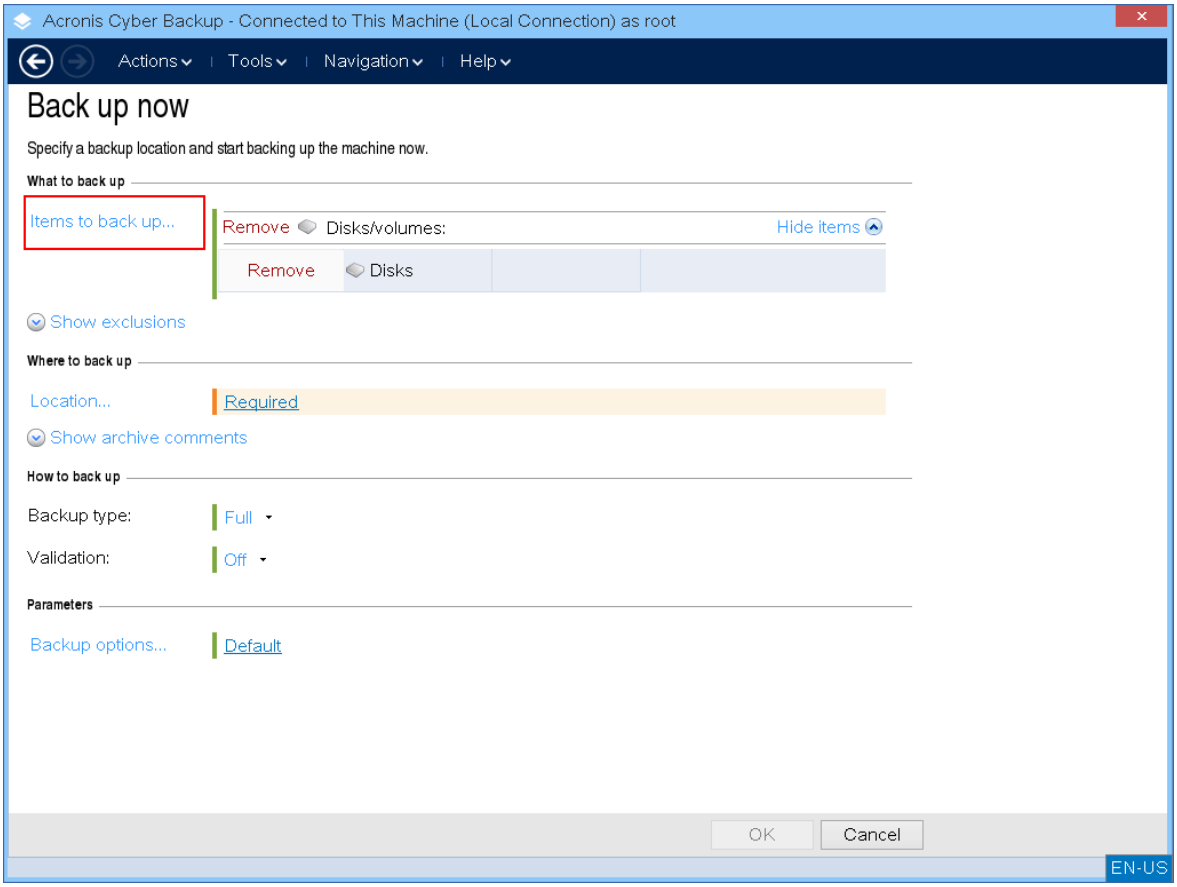


4. Todos los discos no extraíbles del equipo se seleccionan automáticamente para la copia de seguridad. Para cambiar los datos que se incluirán en la copia de seguridad, haga clic en **Elementos para incluir en la copia de seguridad** y seleccione los discos o volúmenes deseados.

   Al seleccionar los datos que se incluirán en la copia de seguridad, aparecerá el siguiente mensaje: "*Este equipo no puede seleccionarse directamente. Una versión previa del agente está instalada en el equipo. Utilice las reglas de las directivas para seleccionar este equipo para la copia de seguridad.*" Esta interfaz de usuario puede ignorarse. Seleccione los discos o volúmenes individuales de los que desea realizar una copia de seguridad.

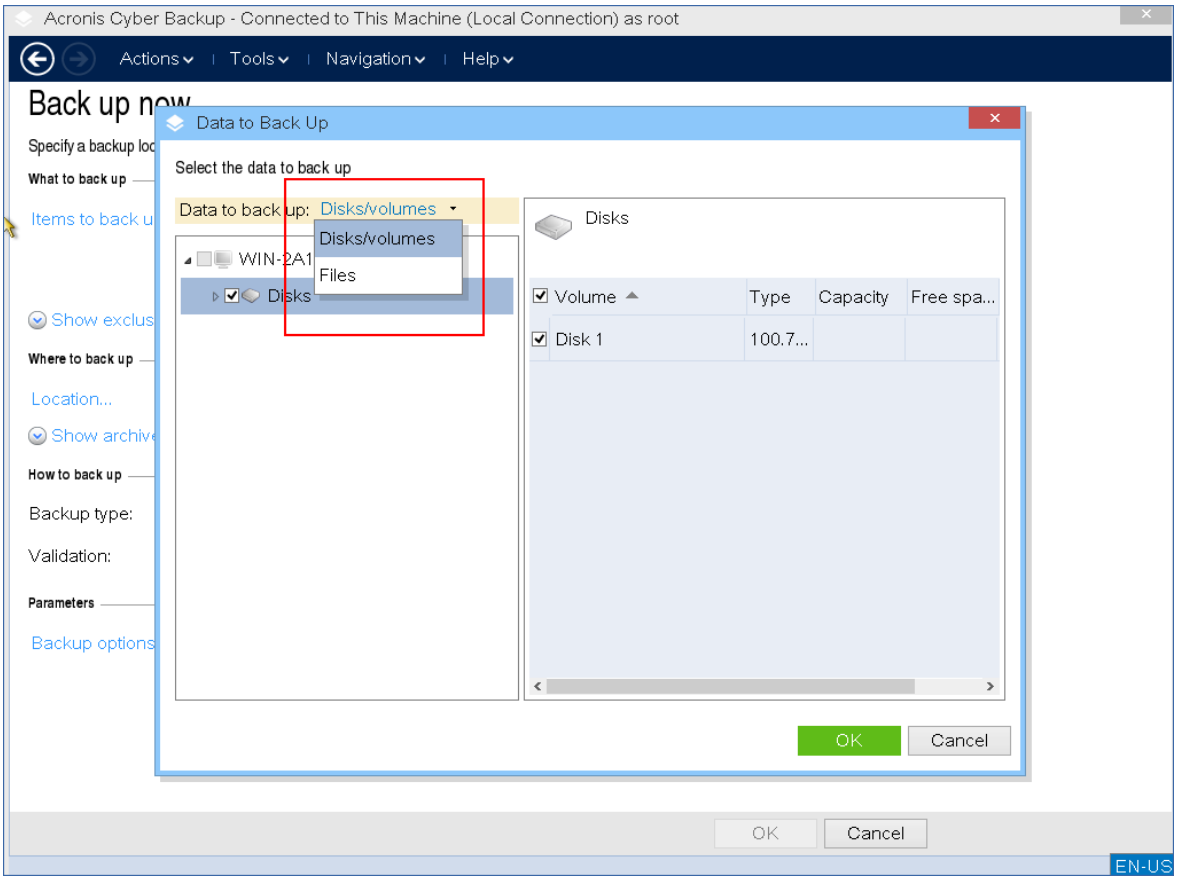
   Nota

   Puede que vea que las letras de unidad son distintas de las de Windows con el dispositivo de arranque basado en Linux. Intente identificar el dispositivo o la partición que necesita por su tamaño o etiqueta.

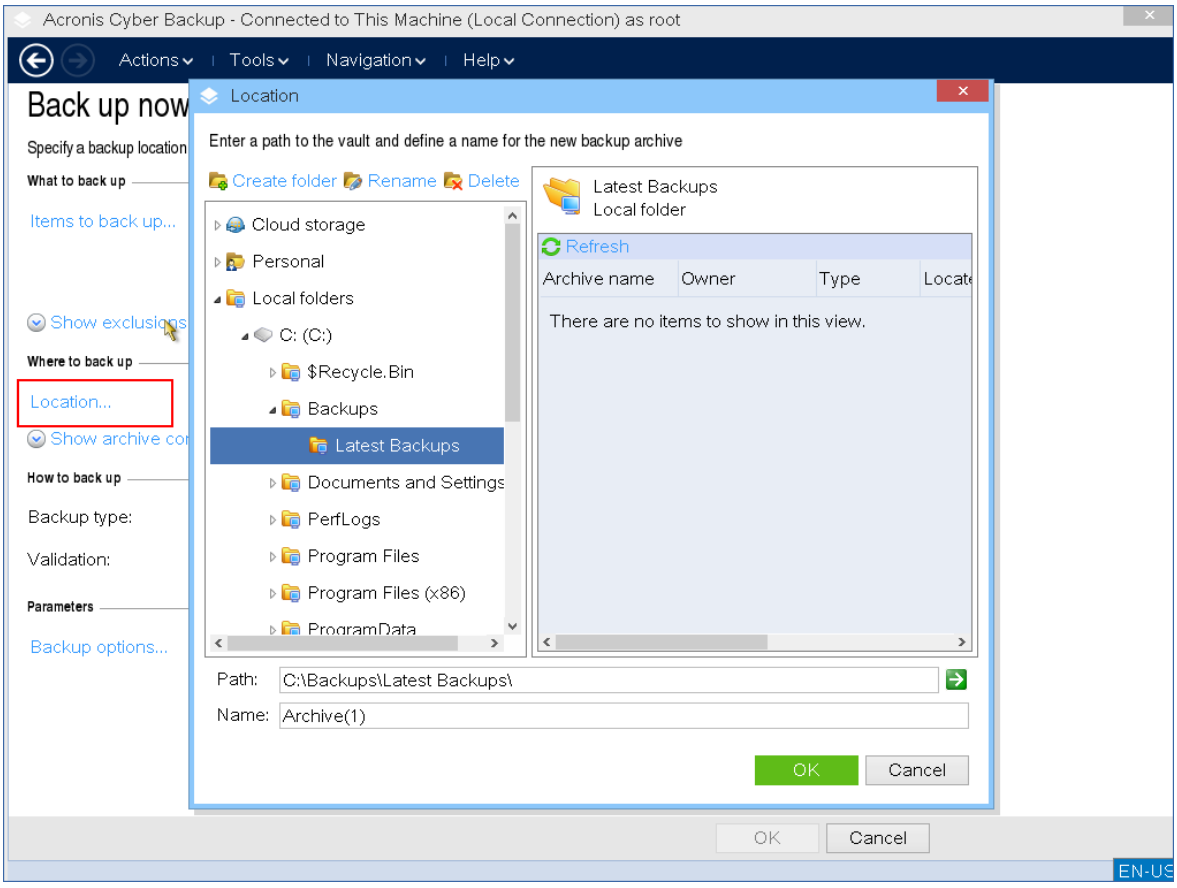


5. Si desea hacer una copia de seguridad de archivos o carpetas en lugar de discos, cambie a **Archivos** en **Datos para incluir en la copia de seguridad**.

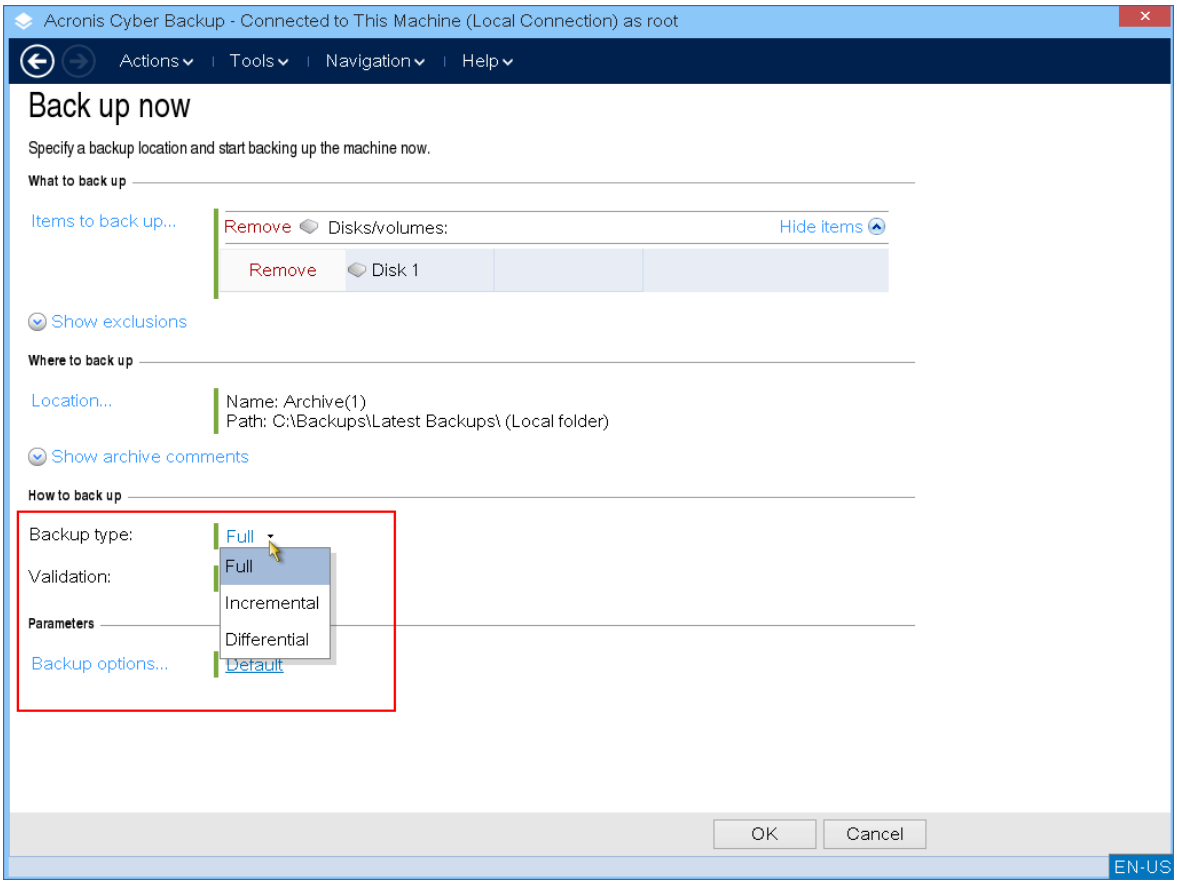
   Solo el disco/la partición y el archivo/la carpeta de copia de seguridad están disponibles mediante el dispositivo de arranque. Otros tipos de copia de seguridad, como las de bases de datos, solo están disponibles en el sistema operativo en ejecución.



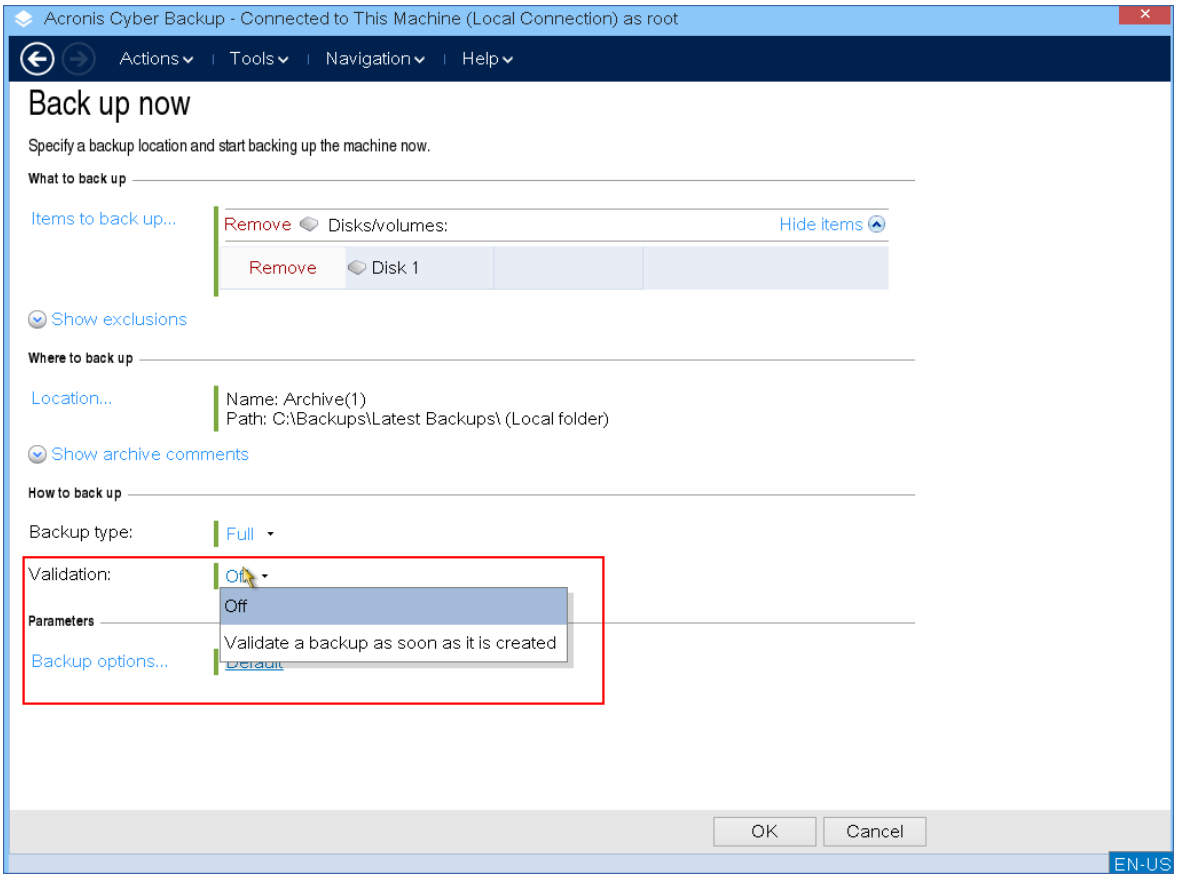
6. Haga clic en **Ubicación** y seleccione dónde se guardará la copia de seguridad.



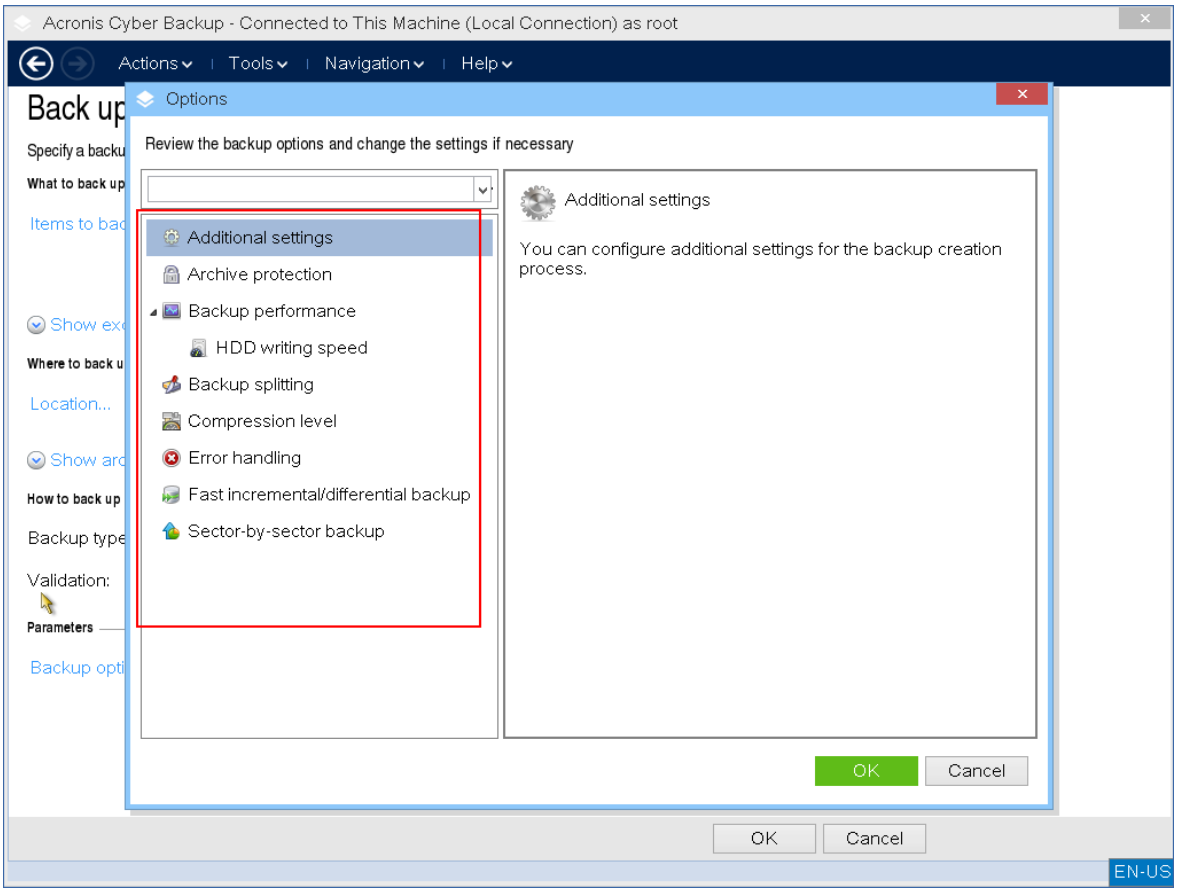
7. Indique la ubicación y el nombre de su copia de seguridad.
8. Indique el tipo de copia de seguridad. Si es la primera vez que se crea una copia de seguridad en esta ubicación, se hará una completa. Si sigue una cadena de copias de seguridad, puede seleccionar **Incremental** o **Diferencial** para ahorrar espacio. Para obtener más información sobre los tipos de copia de seguridad, consulte https://kb.acronis.com/content/1536.



9. [Opcional] Si quiere validar el archivo de la copia de seguridad, seleccione **Validar una copia de seguridad cuando se cree**.

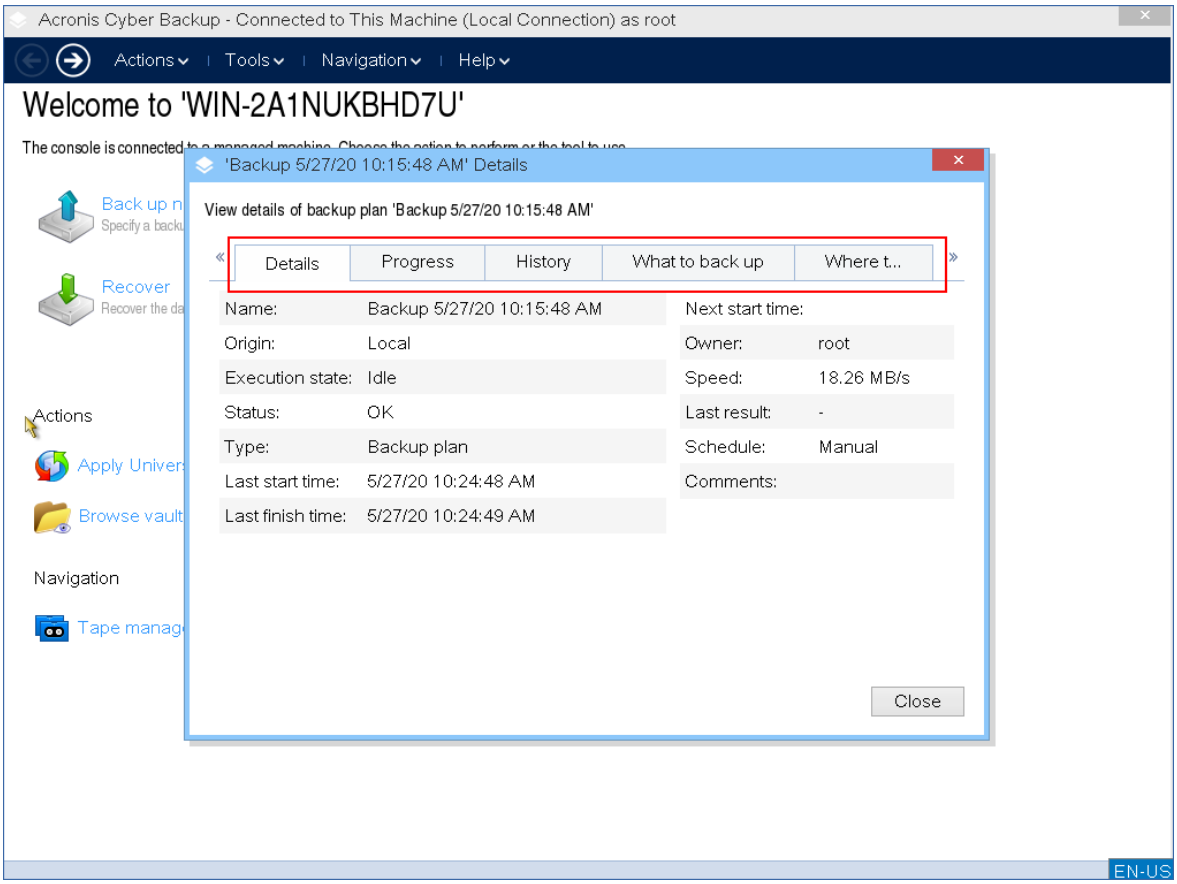


10. [Opcional] Especifique las opciones de copia de seguridad que necesite, como la contraseña del archivo de la copia de seguridad, la división de copias de seguridad o la gestión de errores.



11. Haga clic en **Aceptar** para iniciar la copia de seguridad.

    El dispositivo de arranque lee los datos del disco, los comprime en un archivo .tib y escribe el archivo en la ubicación seleccionada. No crea una instantánea del disco porque no hay aplicaciones en ejecución.
12. Puede comprobar el estado de la tarea de copia de seguridad y la información adicional sobre la copia de seguridad en la ventana que aparece.

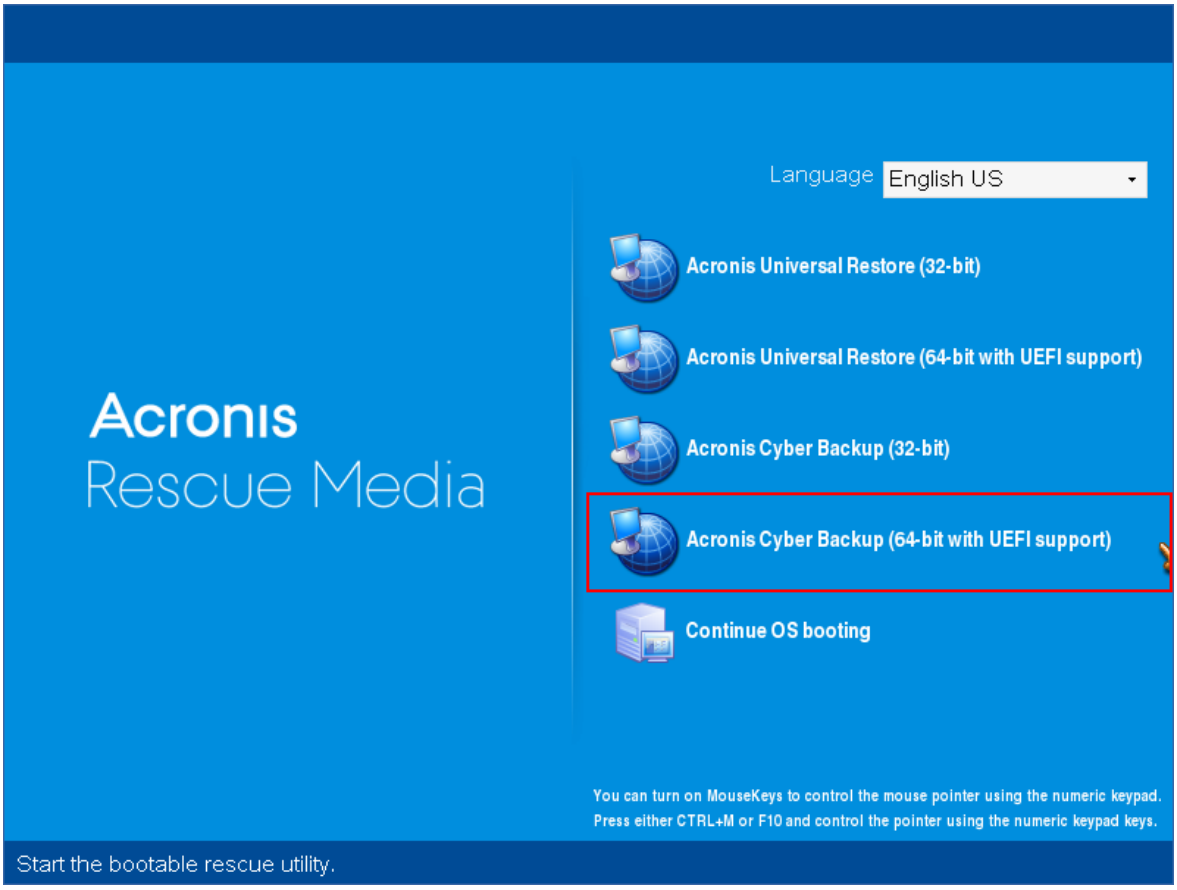


Recuperación con soporte de arranque in situ

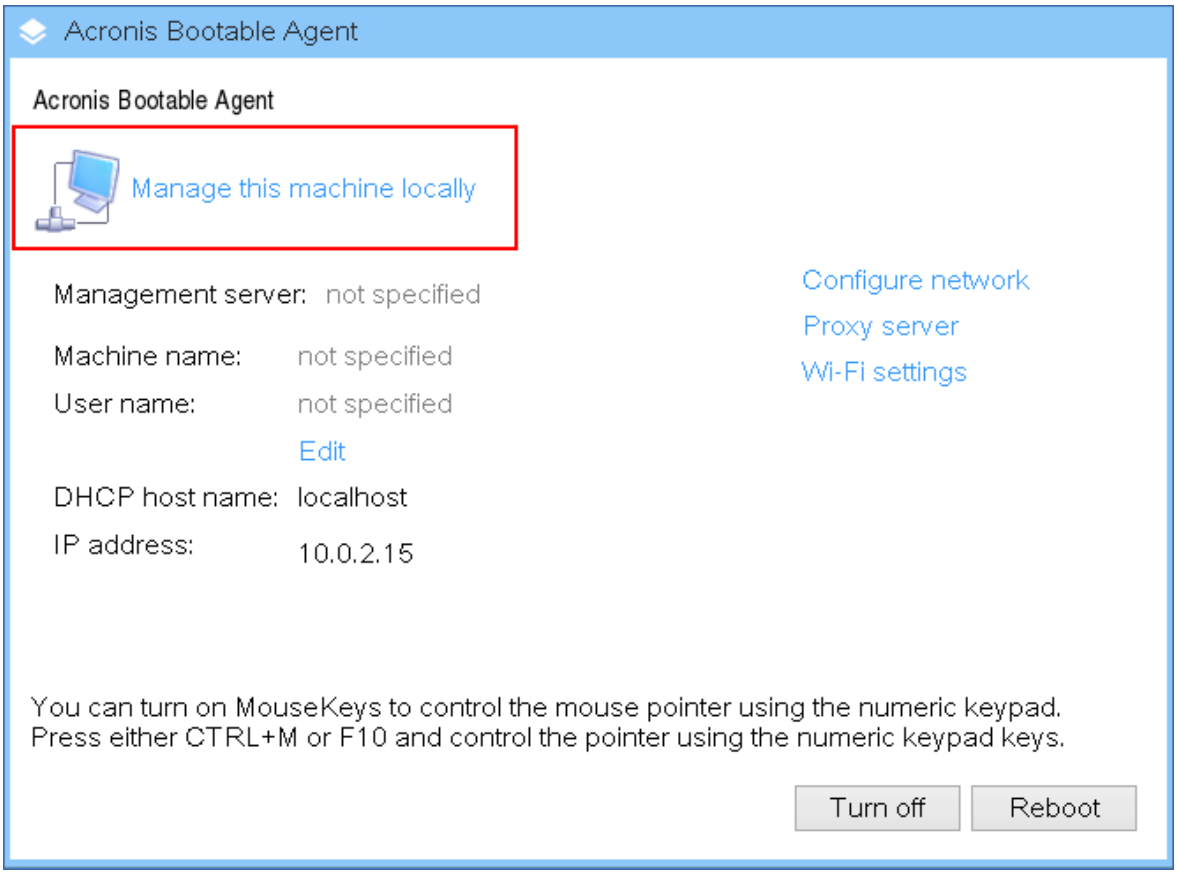
La operación de recuperación está disponible tanto en los dispositivos de arranque creados con Bootable Media Builder como en los dispositivos de arranque disponibles que se hayan descargado.

Pasos para recuperar datos mediante un dispositivo de arranque

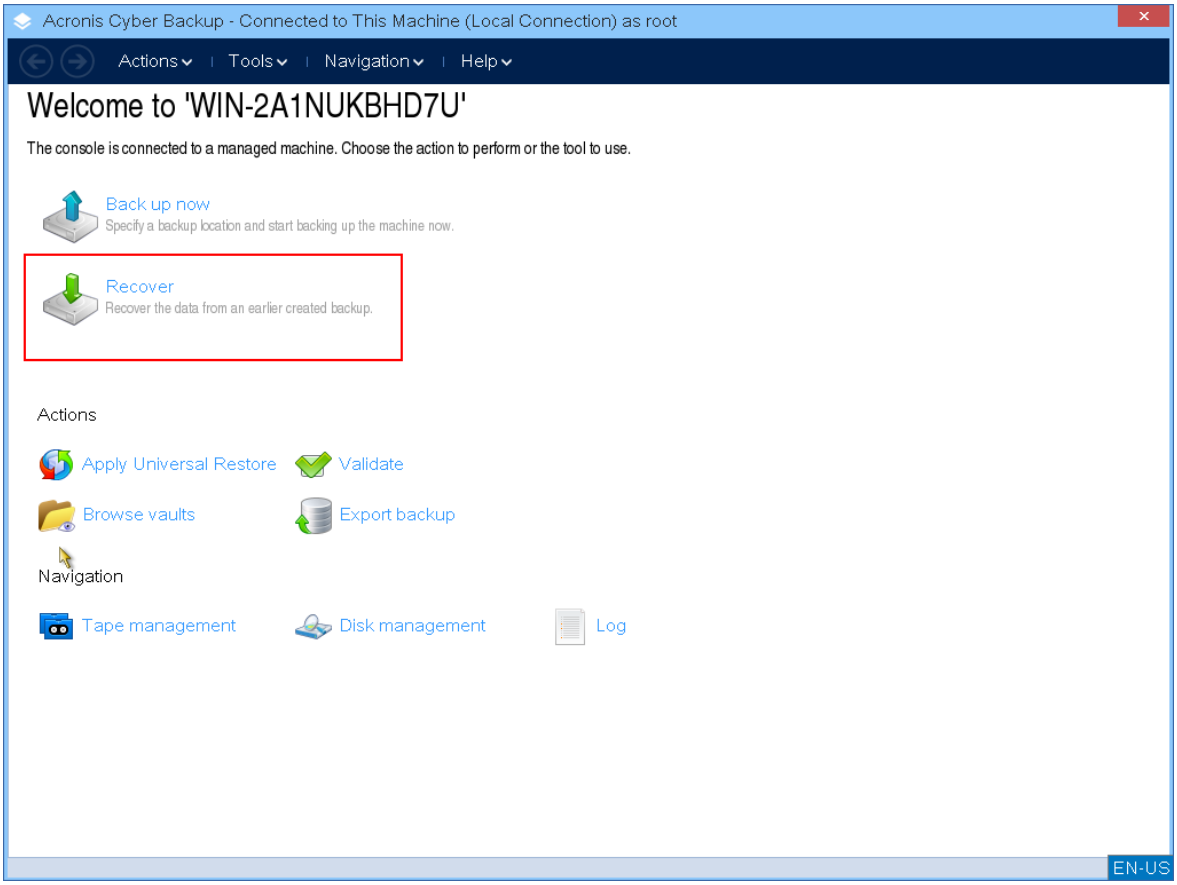
1. Inicie desde el dispositivo de rescate de arranque de Acronis.



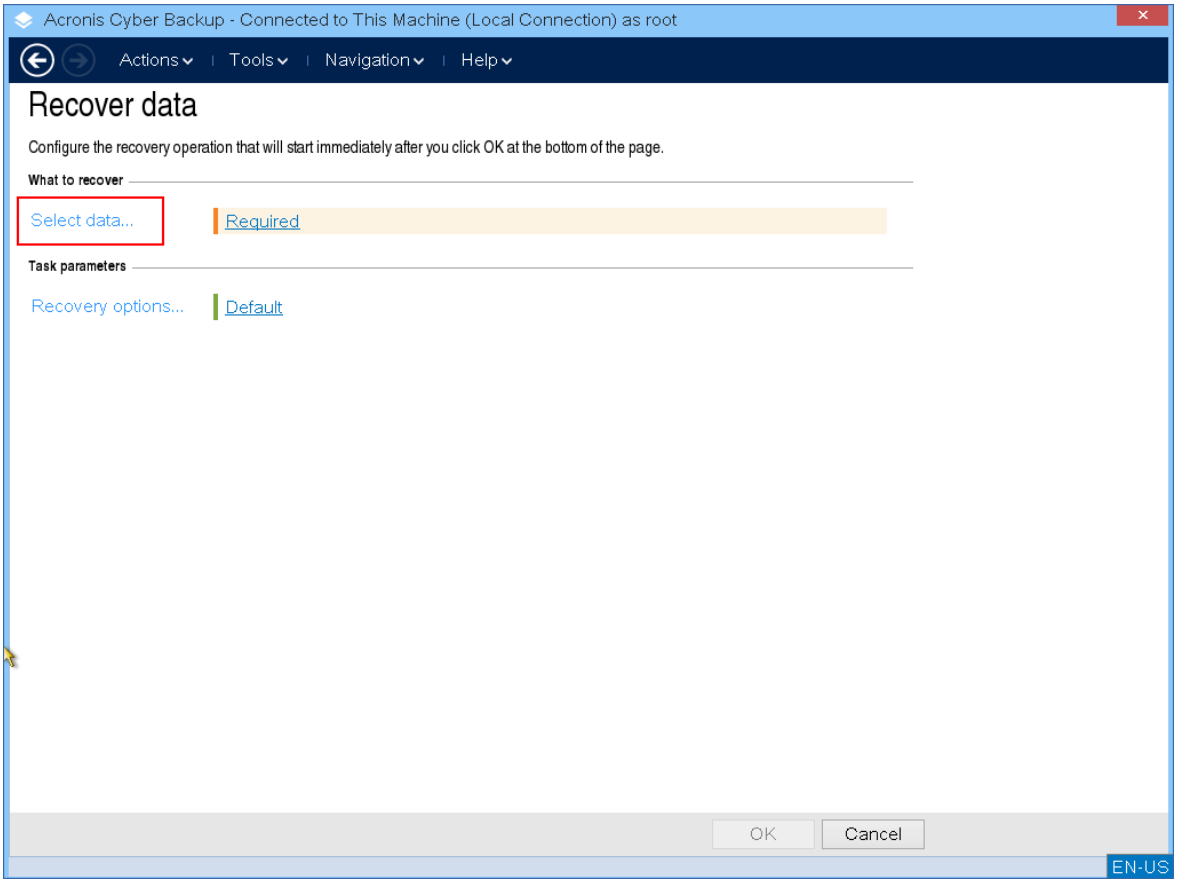
2. Para recuperar datos del equipo local, haga clic en **Gestionar este equipo localmente**. Para conexiones remotas, consulte Registro de dispositivos en el servidor de gestión.



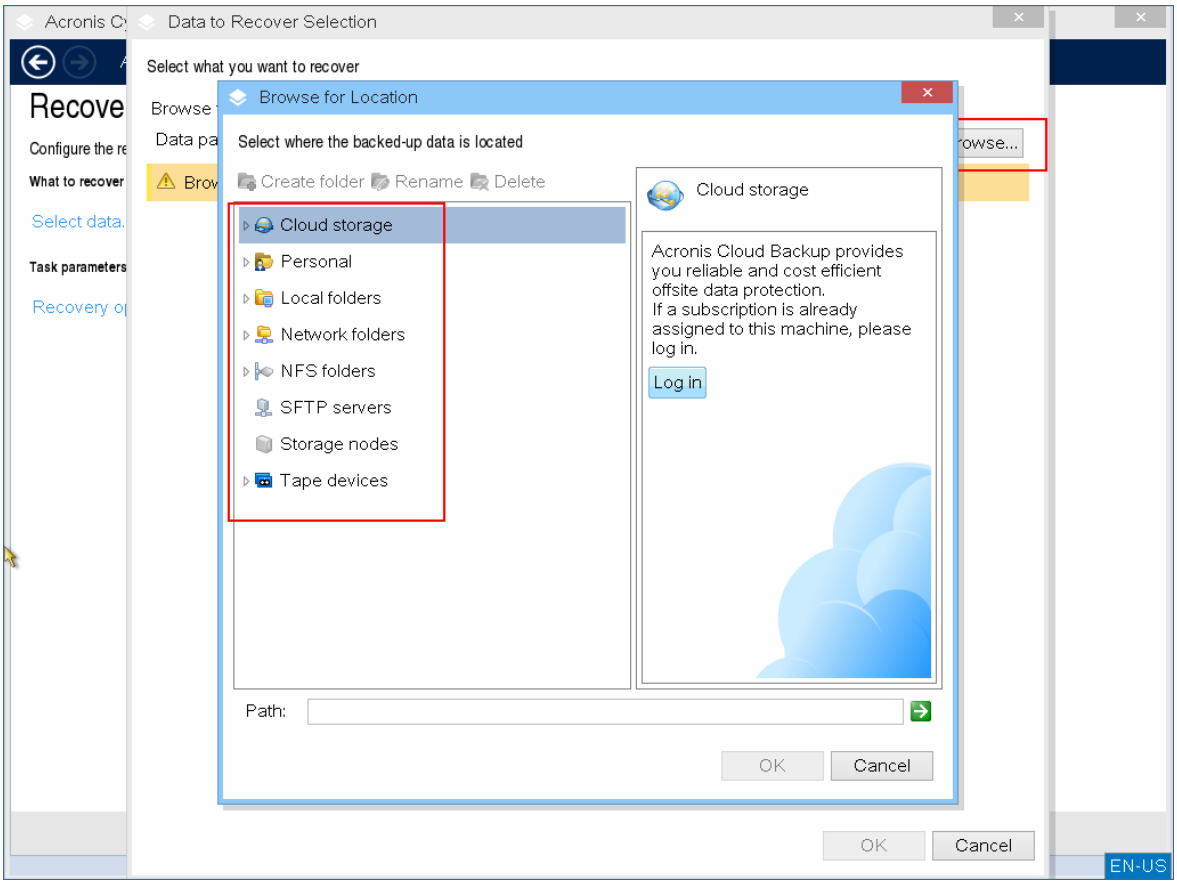
3. Haga clic en **Recuperar**.



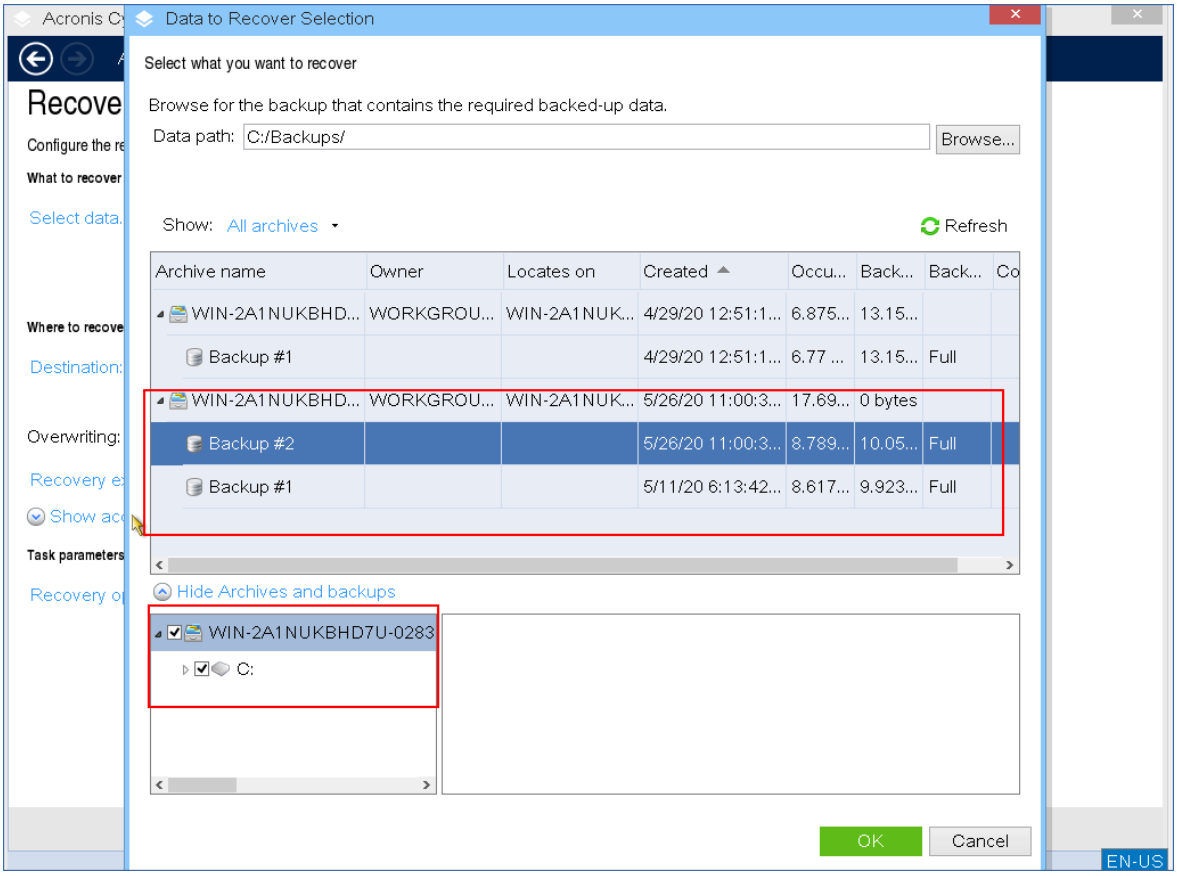
4. En **Qué recuperar**, haga clic en **Seleccionar datos**.



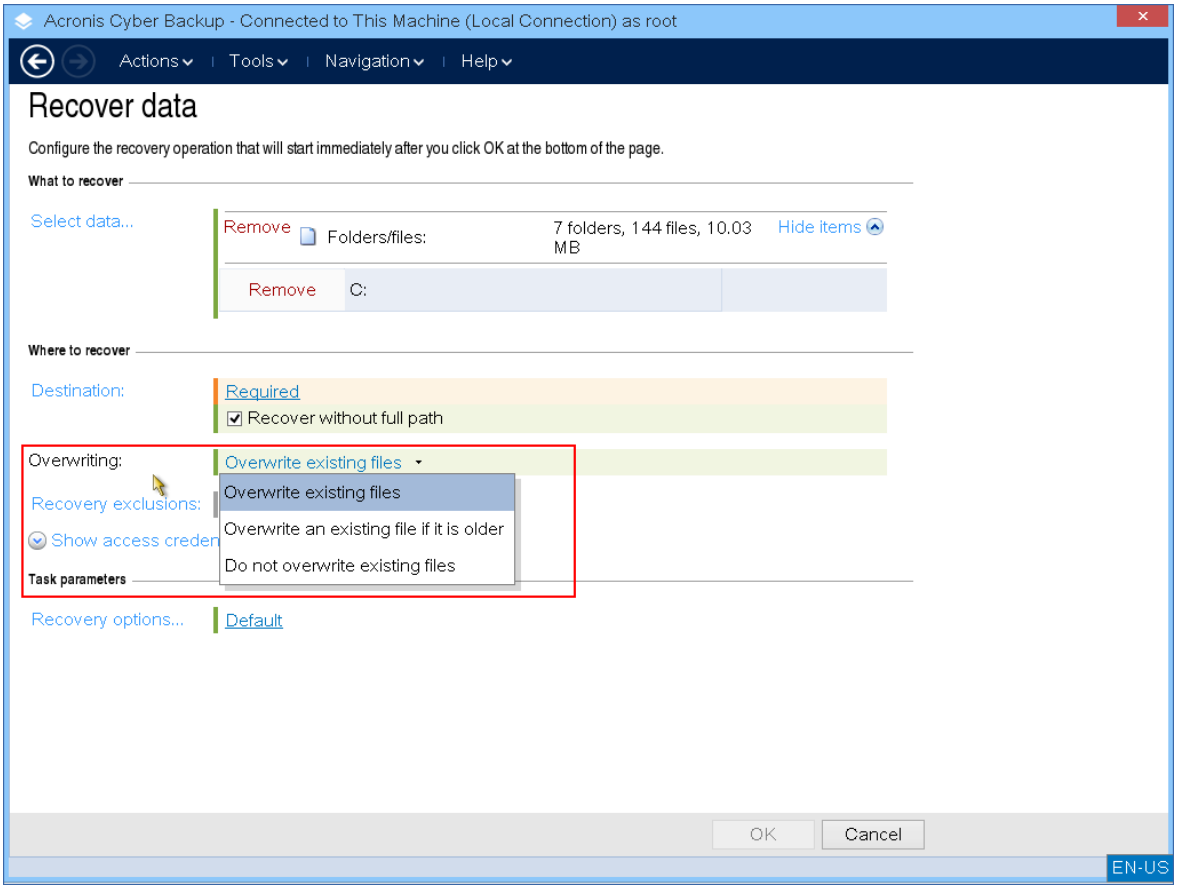
5. Haga clic en **Examinar** y seleccione la ubicación de la copia de seguridad.



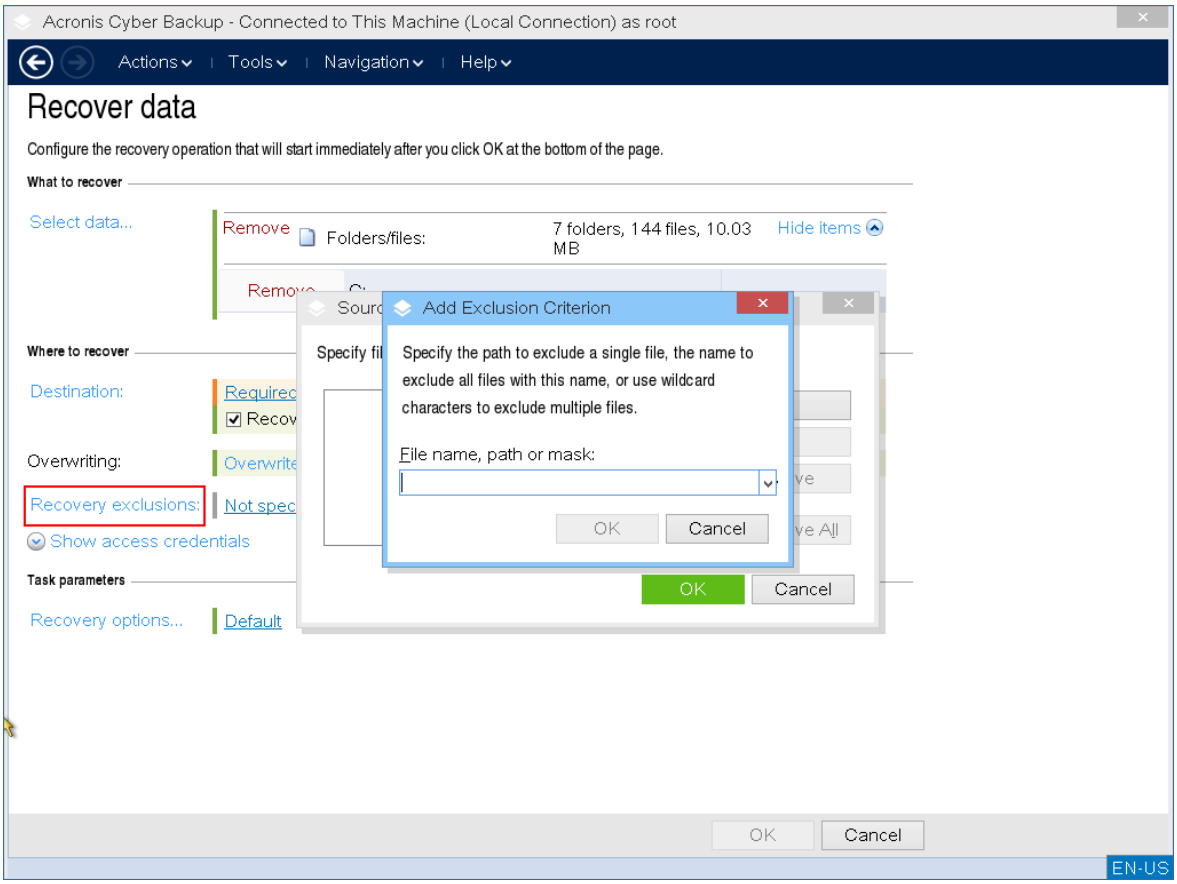
6. Seleccione el archivo de la copia de seguridad que desea recuperar.



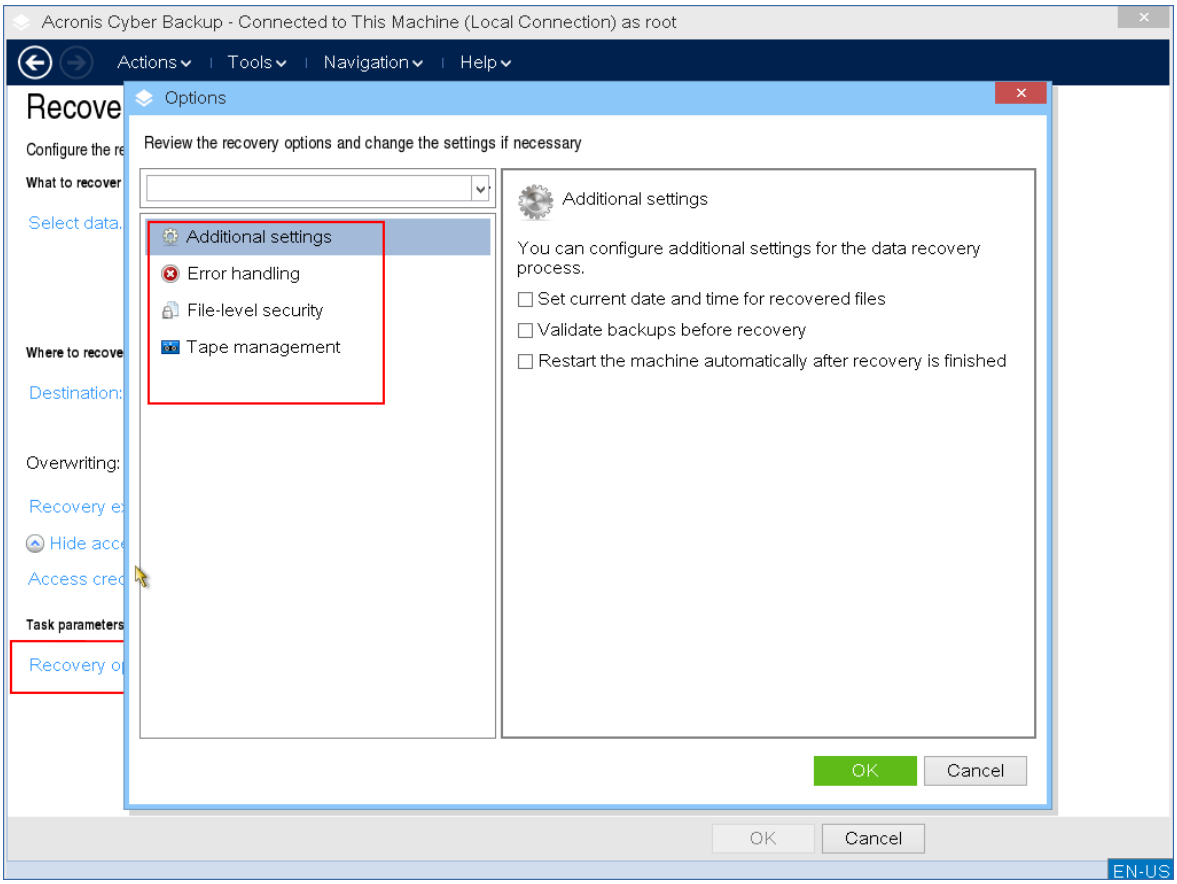
7. En el panel inferior izquierdo, seleccione las unidades o volúmenes (o archivos y carpetas) que desee recuperar y haga clic en **Aceptar**.
8. [Opcional] Configurar las reglas de sobreescritura.



9. [Opcional] Configurar las exclusiones de recuperación.



10. [Opcional] Configurar las opciones de recuperación.



11. Compruebe que su configuración sea correcta y haga clic en **Aceptar**.

Nota

Para recuperar datos de hardware diferente, utilice Acronis Universal Restore.

Acronis Universal Restore no está disponible cuando la copia de seguridad está ubicada en Acronis Secure Zone.

Administración de discos con soportes de arranque

Con el dispositivo de arranque de Acronis puede preparar una configuración de disco/volumen para recuperar las imágenes del volumen incluidas en la copia de seguridad con Acronis Cyber Protect.

A veces, después de realizar la copia de seguridad de un volumen y guardar la imagen en un lugar seguro, puede cambiar la configuración del disco del equipo a causa de unl reemplazo de un HDD o pérdida de hardware. En dicho caso, puede recrear la configuración necesaria de disco para que se pueda recuperar con exactitud la imagen del disco "como estaba" o con cualquier alteración de la estructura del disco o del volumen que pueda considerar necesario.

Tome todas las precauciones necesarias para evitar cualquier posible pérdida de datos.

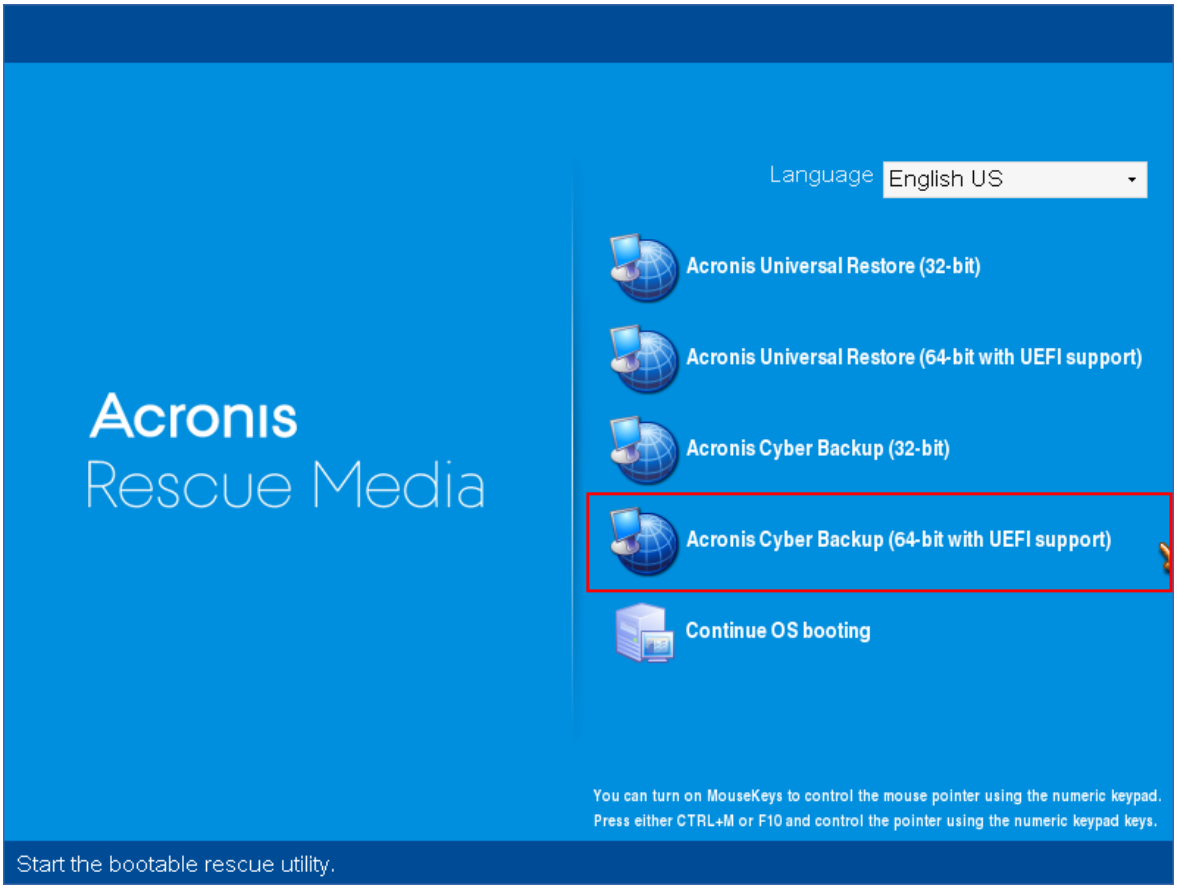
Importante
Todas las operaciones con discos y volúmenes involucran cierto riesgo de daños de los datos. Las operaciones en el sistema, los volúmenes de arranque o datos, deben realizarse con mucho cuidado para evitar cualquier problema potencial con el proceso de arranque o el almacenamiento de los datos en el disco duro.
Las operaciones con disco duros y volúmenes llevan cierto tiempo, y cualquier pérdida de potencia, apagado involuntario del equipo o pulsación accidental del botón Reiniciar durante el proceso podría causar daños y pérdida de datos.

Puede ejecutar operaciones de gestión del disco en una restauración completa, en un equipo que no se pueda iniciar o en uno que no tenga Windows. Necesitará un dispositivo de arranque que haya creado con Bootable Media Builder y su clave de licencia de Acronis Cyber Protect. Para obtener más información sobre cómo crear dispositivos de arranque, consulte Dispositivos de arranque basados en Linux o Dispositivos de arranque basados en Windows-PE respectivamente.

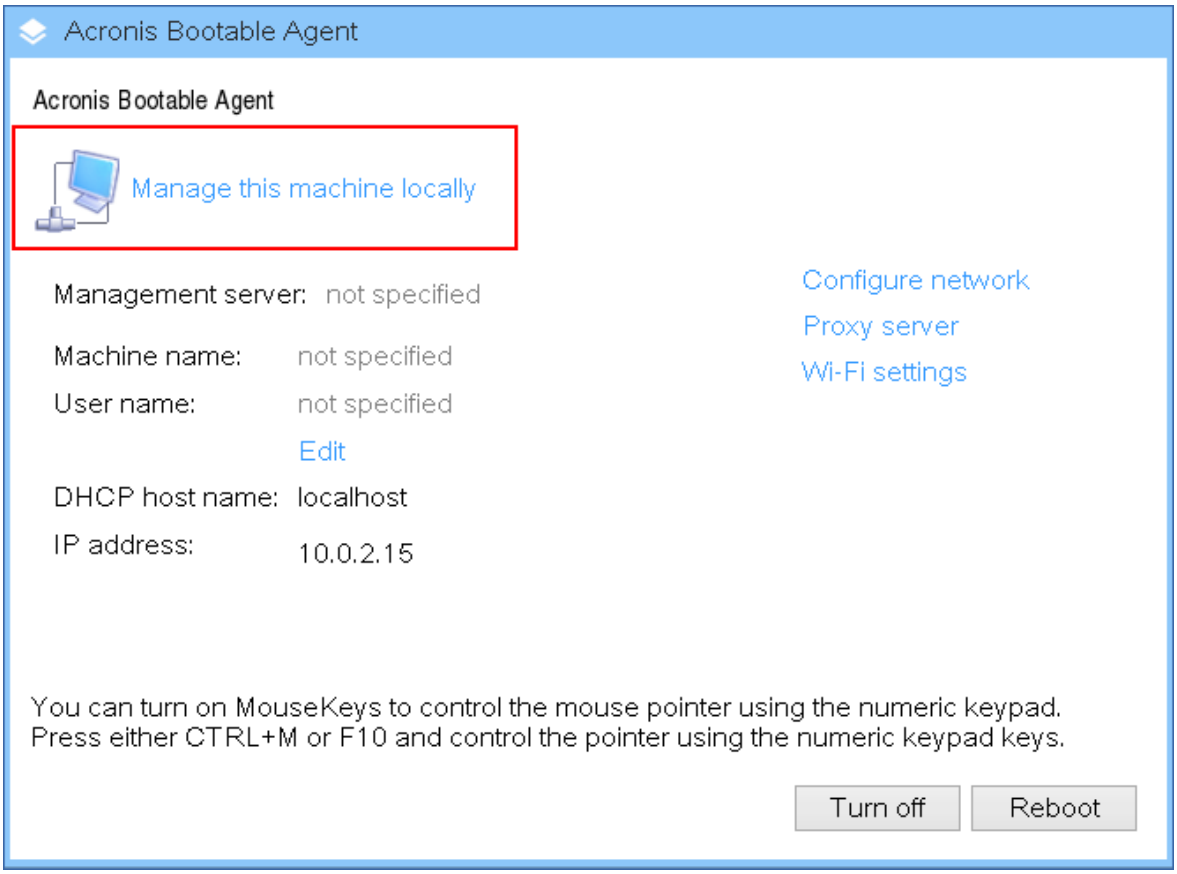
Nota
La funcionalidad de gestión del disco no está disponible para dispositivos de arranque basados en Windows PE 4.0 o posterior. Por lo tanto, la gestión del disco es compatible con Windows 7 y sistemas operativos anteriores. Para ejecutar operaciones de gestión del disco en Windows 8 y sistemas posteriores, debe instalar Acronis Disk Director. Para obtener más información, consulte este artículo de la Base de conocimientos: https://kb.acronis.com/content/47031.

Pasos para ejecutar operaciones de gestión del disco

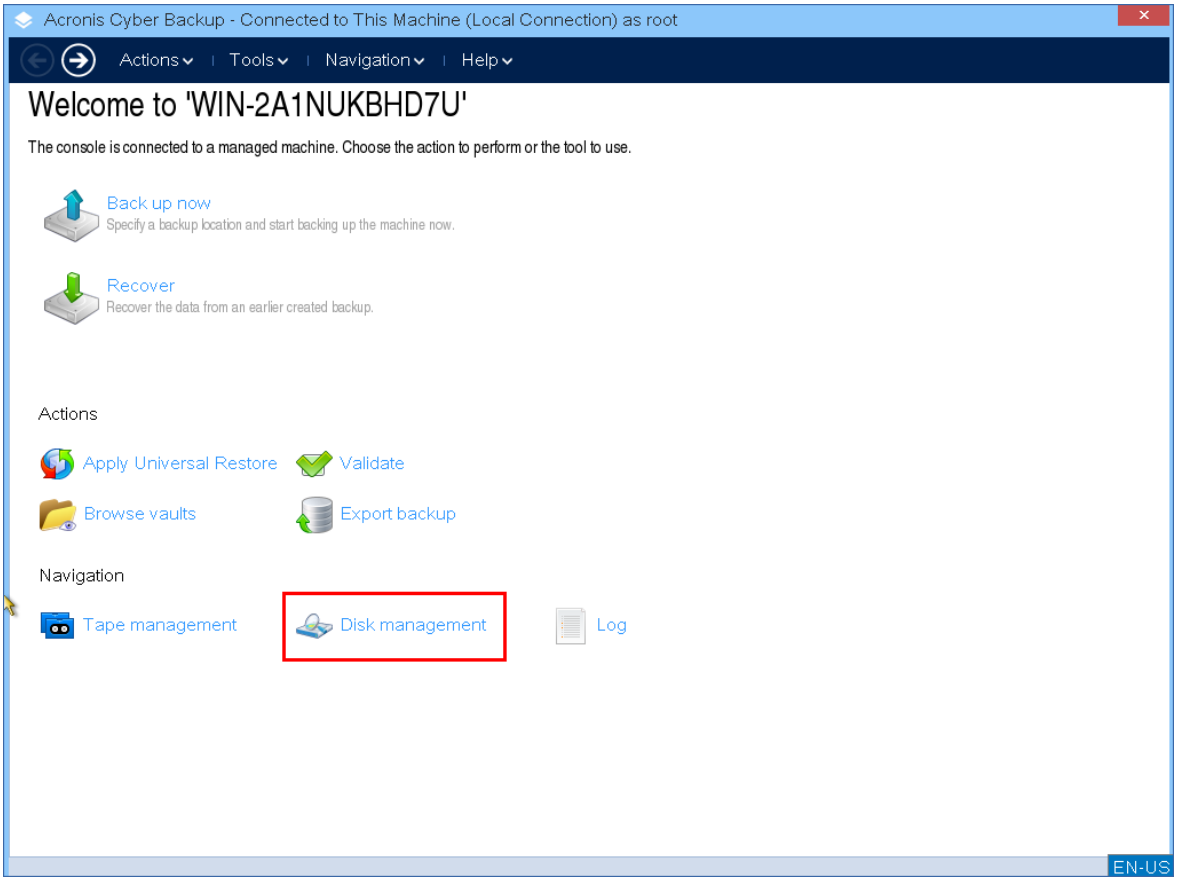
1. Inicie desde el dispositivo de rescate de arranque de Acronis.



2. Para trabajar en el equipo local, haga clic en **Gestionar este equipo localmente**. Para conexiones remotas, consulte Registro de dispositivos en el servidor de gestión.



3. Haga clic en **Gestión del disco**.



Nota
Puede que las operaciones de gestión del disco desde el dispositivo de arranque no funcionen correctamente si hay espacios de almacenamiento configurados en el equipo.

Sistemas de archivos compatibles

El dispositivo de arranque admite la gestión del disco con los siguientes sistemas de archivos:

- FAT 16/32
- NTFS

Si necesita ejecutar operaciones en un volumen con un sistema de archivos diferente, utilice Acronis Disk Director. Ofrece más herramientas y utilidades para gestionar discos y volúmenes con los siguientes sistemas de archivos:

- FAT 16/32
- NTFS
- Ext2
- Ext3
- HFS+
- HFSX
- ReiserFS
- JFS
- Linux SWAP

Precauciones posibles

Para evitar posibles daños al disco y a la estructura del volumen o pérdida de datos, tome todas las precauciones necesarias y siga estas directrices:

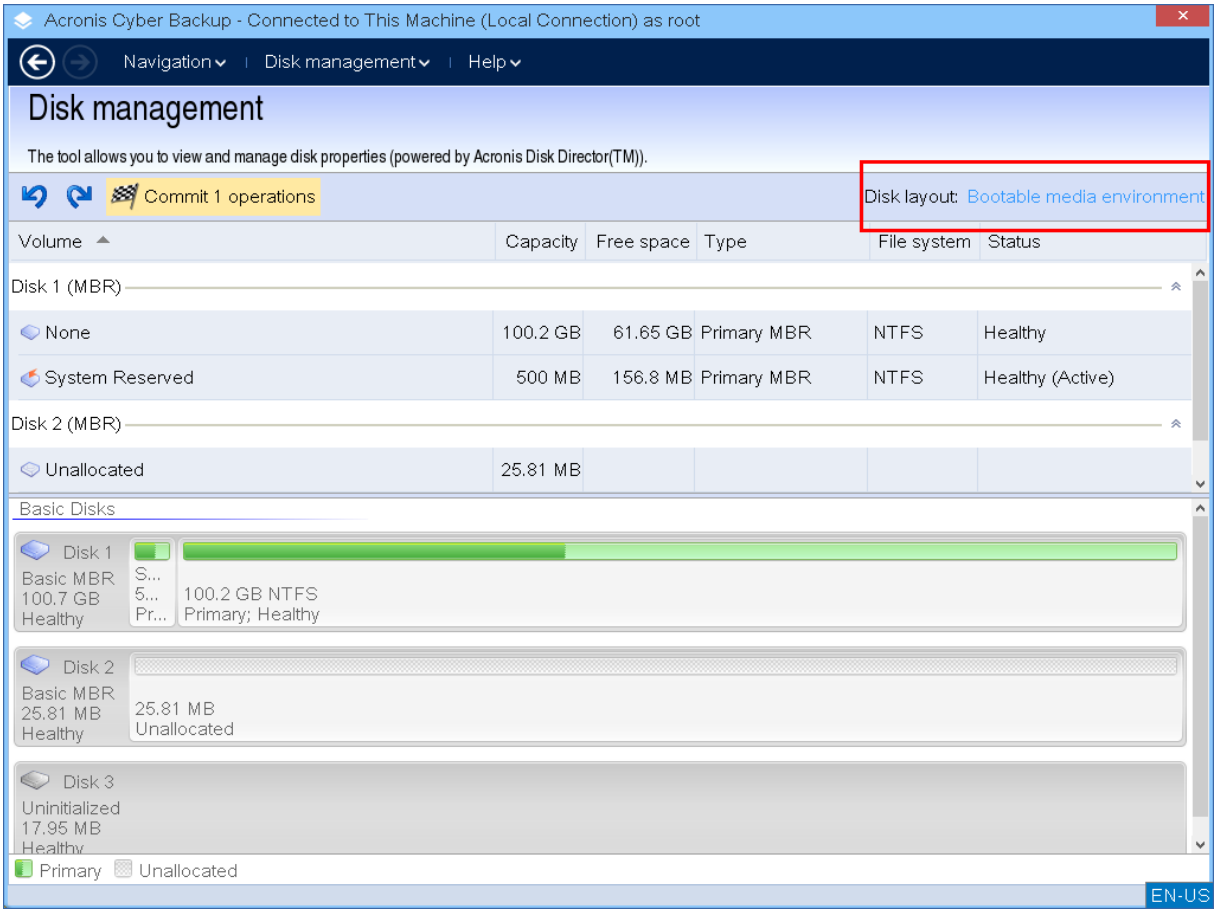
1. Crear la copia de seguridad del disco en los que se crearán o gestionarán los volúmenes Tener la copia de seguridad de sus datos más importantes en otro disco duro, red compartida o dispositivo extraíble le permitirá trabajar en los volúmenes de discos sabiendo que sus datos están seguros.
2. Pruebe su disco para asegurarse de que es completamente funcional y no contiene sectores defectuosos o errores del sistema de archivos.
3. No realice ninguna operación de disco/volumen mientras ejecuta otro software que tenga acceso bajo a nivel de disco.

Elección del sistema operativo para la gestión de discos

En un equipo con dos o más sistemas operativos, la representación de los discos y volúmenes depende de qué sistema operativo esté ejecutándose actualmente. El mismo volumen podría tener

diferentes letras en distintos sistemas operativos.

Cuando realice una operación de gestión de discos, debe especificar para qué sistema operativo se mostrará la distribución del disco. Para ello, haga clic en el nombre del sistema operativo al lado de la etiqueta **Distribución del disco** y seleccione el sistema operativo que desee en la ventana que se abra.



Operaciones del disco

Con el dispositivo de arranque, puede realizar las siguientes operaciones de gestión del disco:

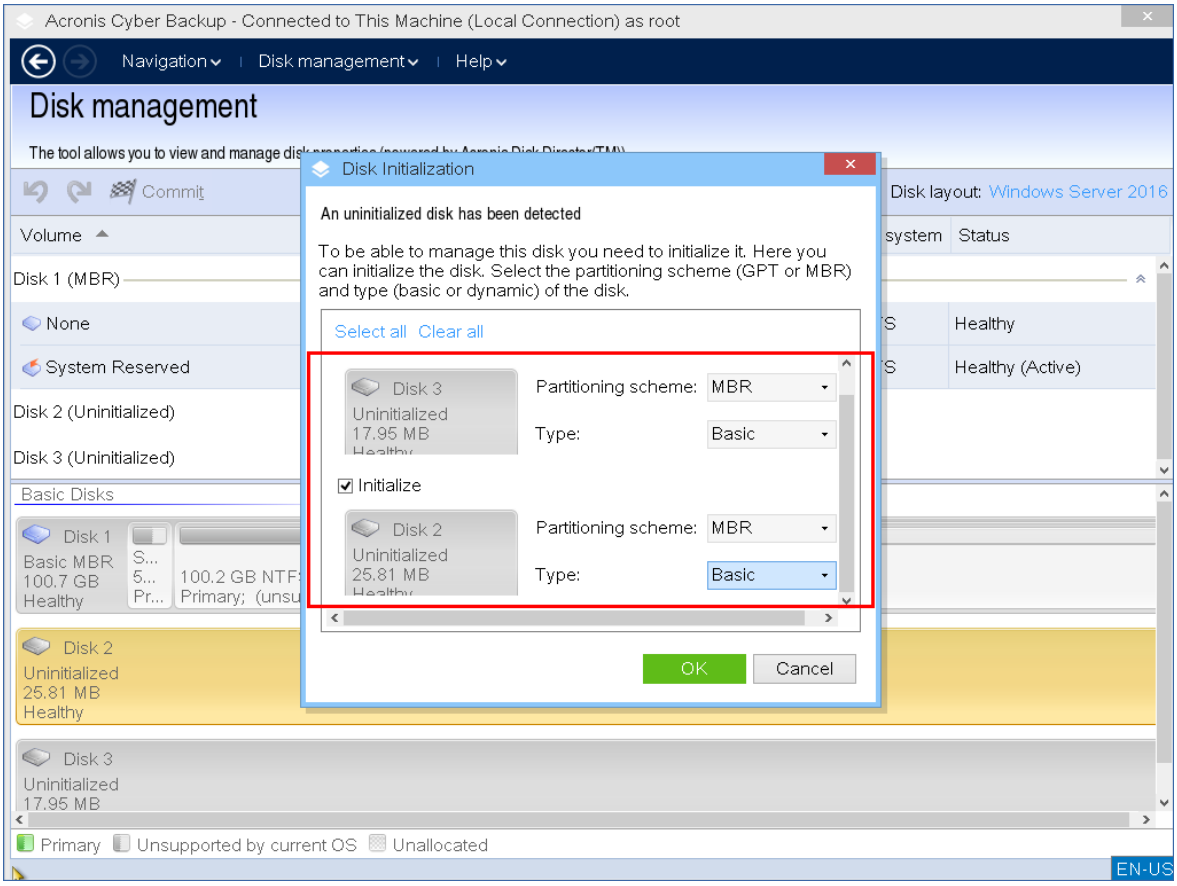
- Inicialización del disco: inicializa un nuevo hardware que se haya añadido al sistema
- Clonación de disco básico: transfiere todos los datos de un disco básico MBR de origen a un disco de destino
- Conversión del disco: de MBR a GPT: convierte una tabla de partición MBR en GPT
- Conversión del disco: de GPT a MBR: convierte una tabla de partición GPT en MBR
- Conversión del disco: de básico a dinámico: convierte un disco básico en dinámico
- Conversión del disco: de dinámico a básico: convierte un disco dinámico en básico

Inicialización del disco

El dispositivo de arranque mostrará el disco no inicializado como un bloque gris con un icono deshabilitado para su selección, que indica que el sistema no puede utilizar el disco.

Pasos para inicializar un disco

1. Haga clic con el botón derecho en el disco que desee y después haga clic en **Inicializar**.
2. En la ventana **Inicialización del disco**, configure el esquema de partición de disco (MBR o GPT) y el tipo de disco (básico o dinámico).
3. Al hacer clic en **Aceptar**, añadirá una operación pendiente de inicialización del disco.
4. Para completar la operación que ha añadido, ejecútela. Si sale del programa sin ejecutar la operación, se cancelará de manera efectiva.
5. Después de la inicialización, el espacio de disco permanece no asignado. Para poder usarlo, debe crear un volumen.



Clonación de disco básico

Puede clonar discos MBR básicos con un dispositivo de arranque con todas las funciones basado en Linux. La clonación de discos no está disponible en los dispositivos de arranque que puede descargar ni en los que cree sin una clave de licencia.

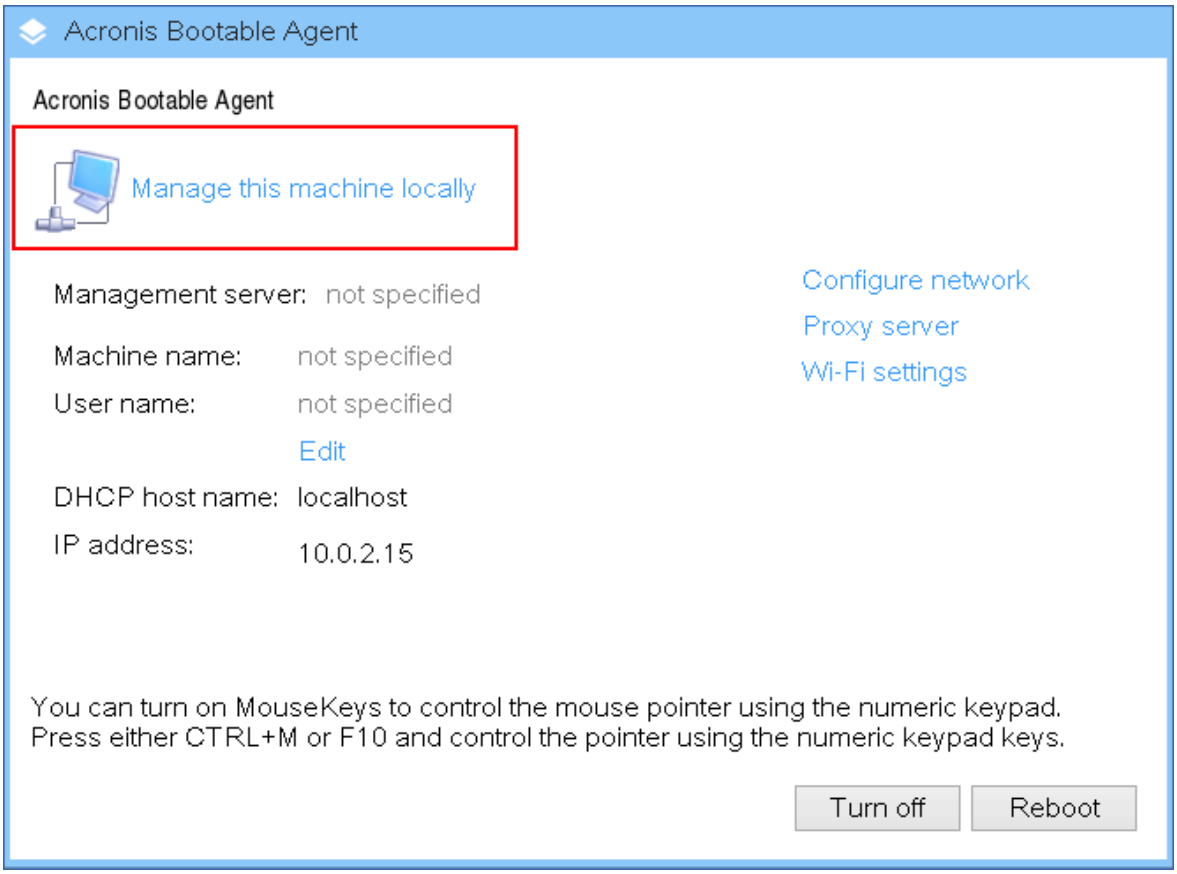
Nota

También puede clonar discos con la utilidad Acronis Cyber Protect Command-Line.

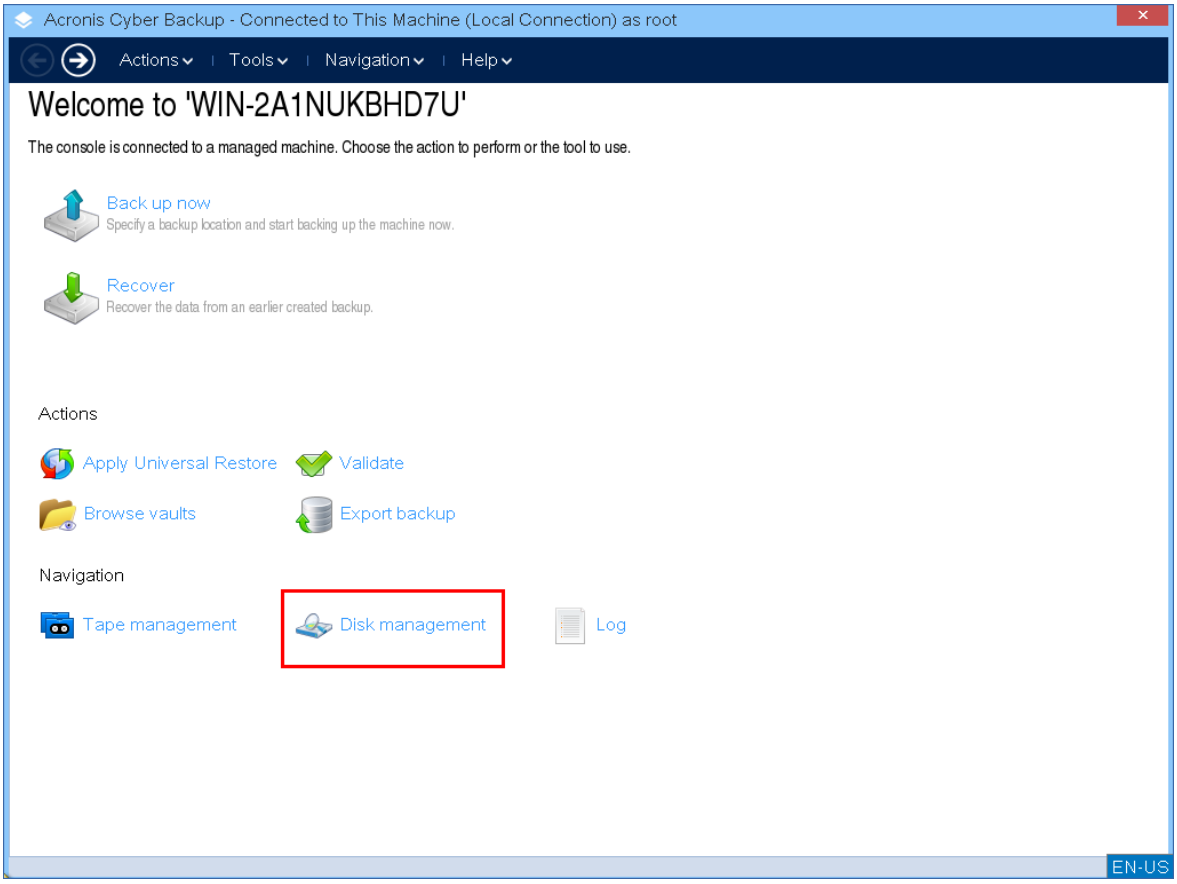
Pasos para clonar discos básicos mediante un dispositivo de arranque

1. Inicie desde el dispositivo de rescate de arranque de Acronis.

2. Para clonar un disco del equipo local, haga clic en **Gestionar este equipo localmente**. Para conexiones remotas, consulte Registro de dispositivos en el servidor de gestión.

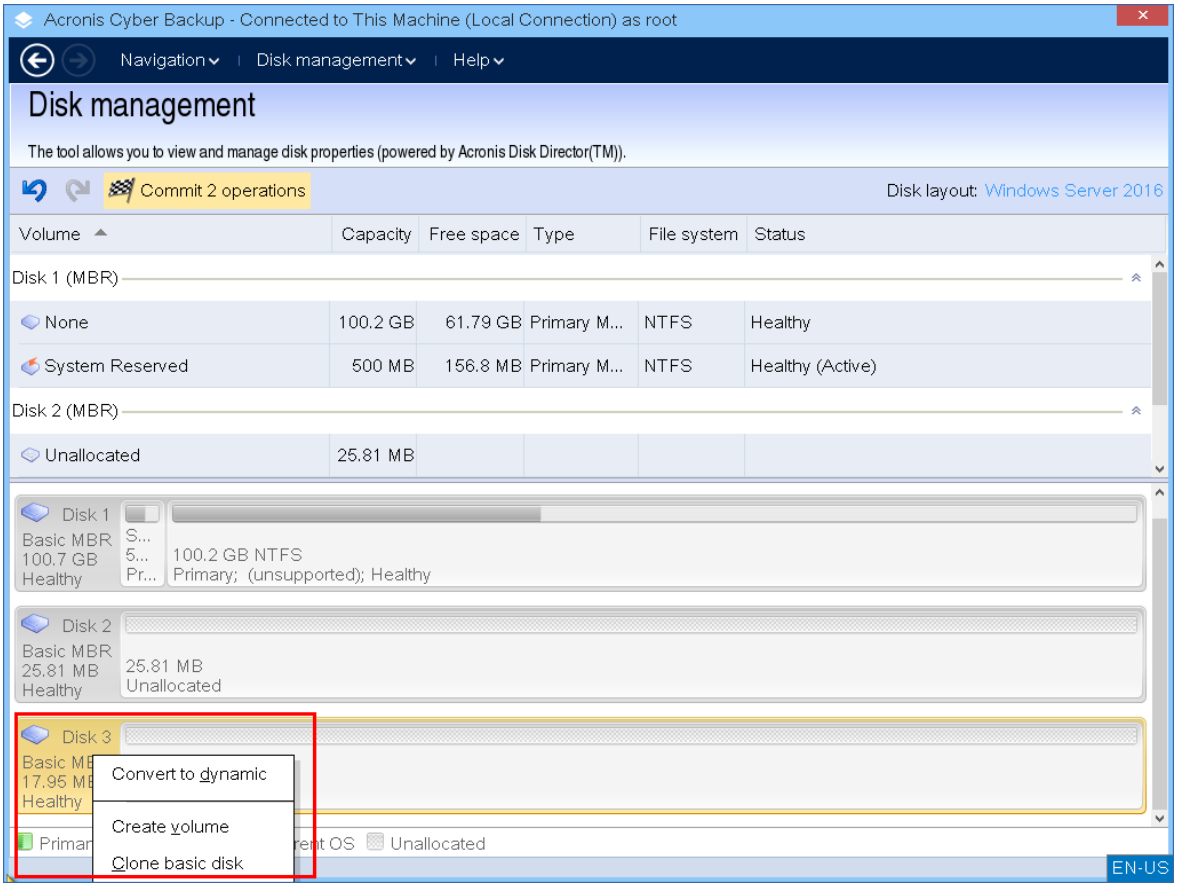


3. Haga clic en **Gestión del disco**.

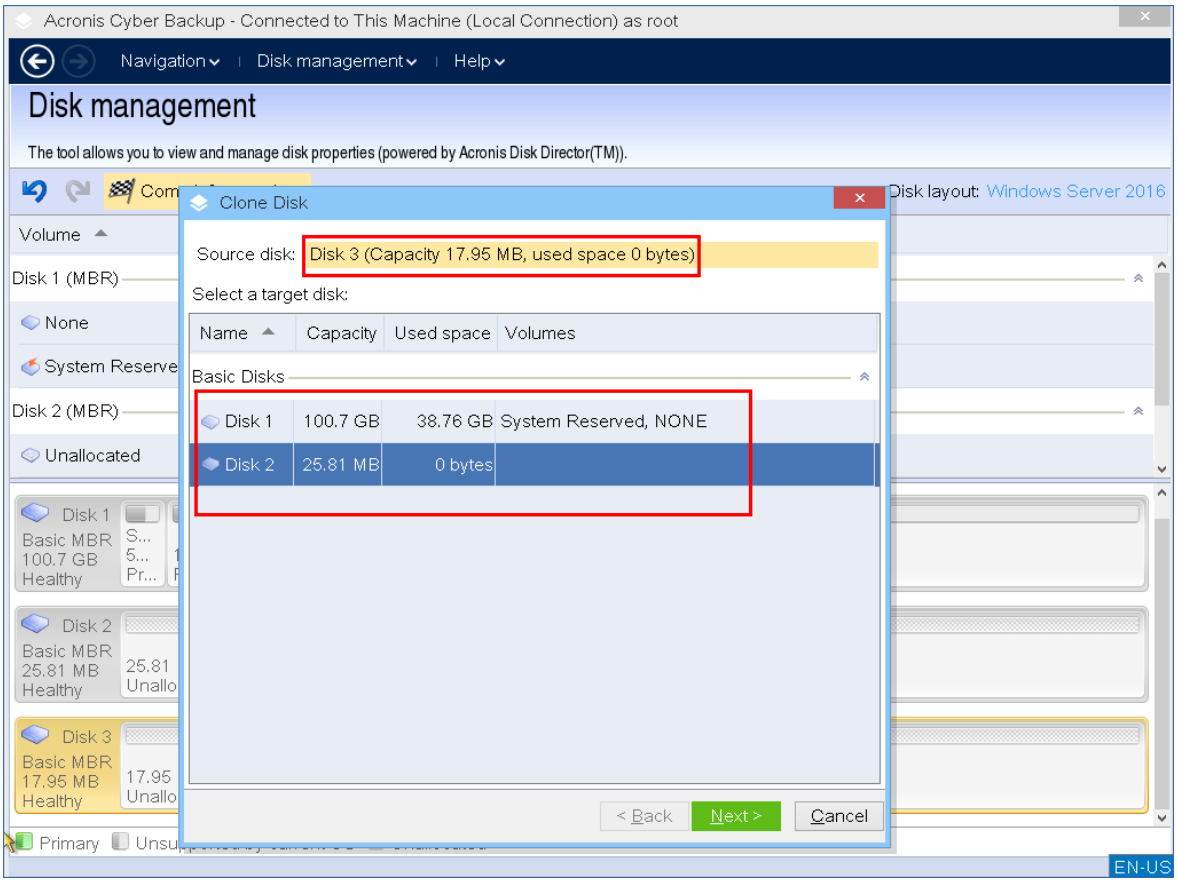


4. Se mostrarán los discos disponibles. Haga clic con el botón derecho en el disco que desee clonar y después haga clic en **Clonar disco básico**.

Nota
Solo puede clonar discos completos. La clonación de particiones no está disponible.



5. Se mostrará una lista de los posibles discos de destino. El programa le permite seleccionar un disco de destino si es lo suficientemente grande para recibir todos los datos del disco de origen sin ninguna pérdida. Seleccione un disco de destino y haga clic en **Siguiente**.

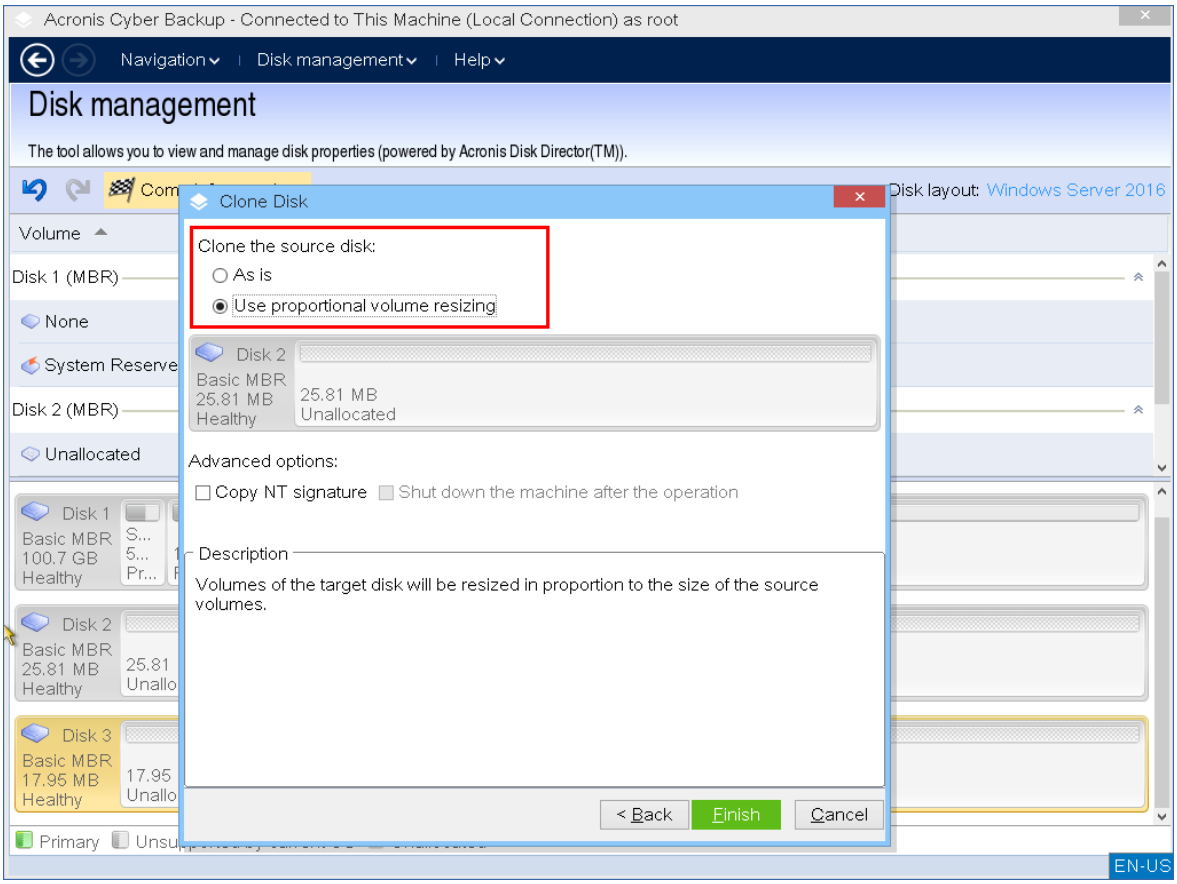


Si el disco de destino es más grande, puede clonarlo como está o redimensionar los volúmenes del disco de origen de manera proporcional (opción predeterminada) para evitar dejar espacio sin asignar en el disco de destino.

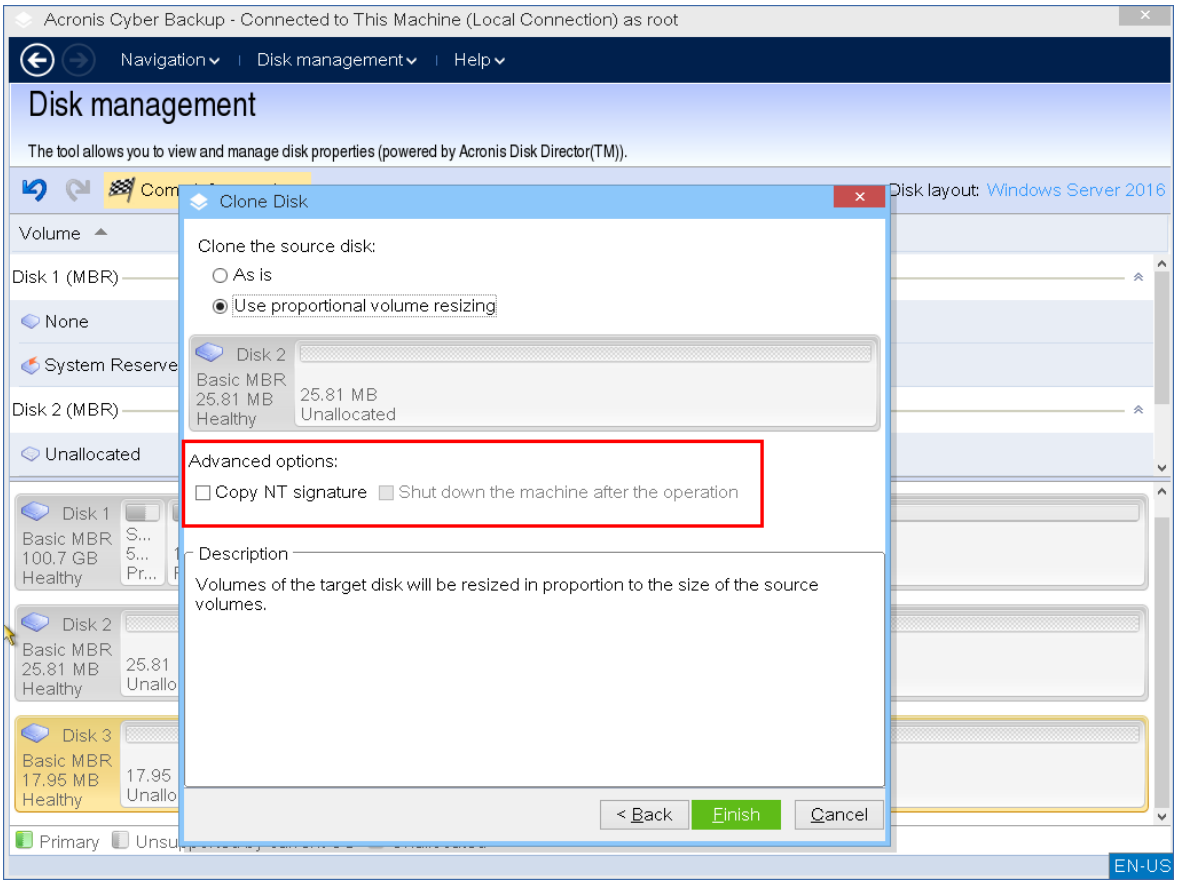
Si el disco de destino es más pequeño, solo estará disponible la redimensión proporcional. Si no es posible clonarlo de forma segura incluso con la redimensión proporcional, no podrá continuar la operación.

Importante

Si hay datos en el disco de destino, aparecerá la siguiente advertencia: "*El disco de destino seleccionado no está vacío. Se sobrescribirán los datos en sus volúmenes.*" Si continúa, todos los datos del disco de destino se perderán irrevocablemente.



6. Seleccione si necesita copiar la firma NT o no.



Si clona un disco que incluye un volumen del sistema, necesita retener la capacidad de arranque operativa en el volumen del disco de destino. Esto significa que el sistema operativo debe tener la información de volumen del sistema (por ejemplo, la letra del volumen) coincidente con la firma NT del disco que se mantiene en el registro de MBR del disco. Sin embargo, dos discos con la misma firma NT no pueden funcionar de manera correcta en un sistema operativo.

Si hay dos discos con la misma firma NT e incluyen un volumen del sistema en un equipo, al inicio el sistema operativo se ejecuta desde el primer disco, descubre la misma firma en el segundo, genera de manera automática una nueva firma NT única y se la asigna al segundo disco. Como resultado, todos los volúmenes del segundo disco perderán sus letras, todas las rutas ya no serán válidas y los programas no encontrarán sus archivos. El sistema operativo de ese disco no se iniciará.

Para retener la capacidad de inicio del sistema en el volumen del disco de destino, puede:

a. **Copiar la firma NT**: le da al disco de destino la firma NT del disco de origen coincidente con las claves de registro también copiadas en el disco de destino.

   Para ello, seleccione la casilla de verificación **Copiar firma NT**.

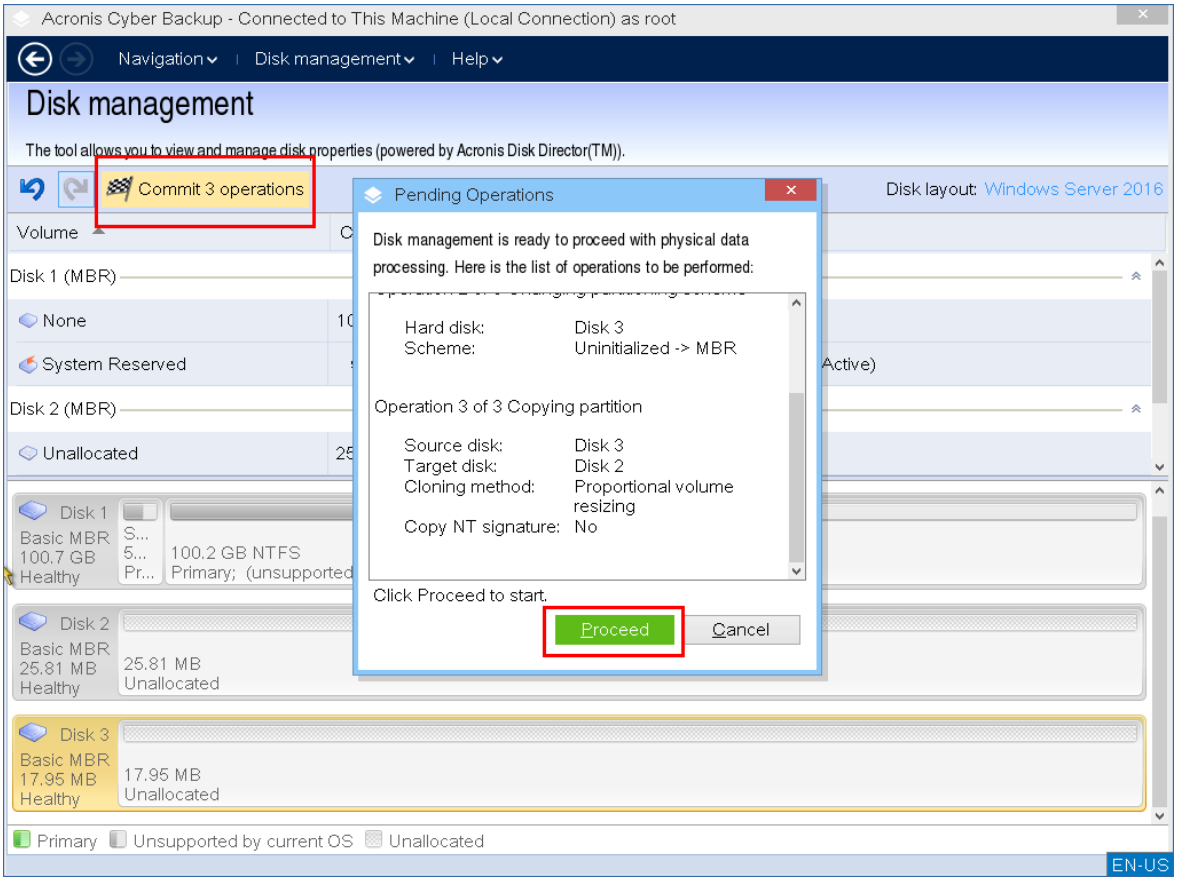
   Recibirá la siguiente advertencia: *"Si hay un sistema operativo en el disco duro, desinstale la unidad de disco duro de origen o de destino de su equipo antes de reiniciarlo.De otro modo, el SO se iniciará desde el primero de los dos discos y el SO en el segundo no se podrá iniciar.*

   Se selecciona y deshabilita automáticamente la casilla de verificación **Apagar el equipo después de la operación**.

b. **Dejar la firma NT**: mantiene la antigua firma del disco de destino y actualiza el sistema operativo de acuerdo con esa firma.

   Para ello, haga clic para borrar la casilla de verificación **Copiar firma NT**, si es necesario. Se deshabilita automáticamente la casilla de verificación **Apagar el equipo después de la operación**.

7. Haga clic en **Finalizar** para agregar la operación pendiente de clonación de discos.
8. Haga clic en **Ejecutar** y después en **Continuar** en la ventana de **Operaciones pendientes**. Si sale del programa sin ejecutar la operación, se cancelará de manera efectiva.



9. Si elige copiar la firma NT, espere hasta que se complete la operación y se apague el equipo y desconecte del equipo la unidad de disco duro de origen o de destino.

Conversión del disco: de MBR a GPT

Puede convertir un disco básico MBR a uno básico GPT si necesita:

- Más de 4 volúmenes primarios en un disco.
- Confiabilidad adicional de un disco, ante cualquier posibilidad de daño de los datos.

Importante
El disco básico MBR que contiene el volumen de arranque con el sistema operativo en ejecución no se puede convertir a GPT.

Pasos para convertir un disco básico MBR a uno básico GPT

1. Haga clic con el botón derecho en el disco que desee clonar y después haga clic en **Convertir a GPT**.
2. Al hacer clic en **Aceptar**, agregará una operación pendiente de conversión de disco MBR a GPT.
3. Para completar la operación que ha añadido, ejecútela. Si sale del programa sin ejecutar la operación, se cancelará de manera efectiva.

Nota
un disco particionado con GPT reserva el espacio necesario para el área de copia de seguridad al final del área particionada, la cual almacena copias del encabezado GPT y la tabla de partición. Si el disco está lleno y el tamaño del volumen no se puede reducir automáticamente, la operación de conversión del disco MBR a GPT fallará.
La operación es irreversible. Si tiene un volumen primario que pertenece a un disco MBR, y convierte el disco primero a GPT y después de regreso a MBR, el volumen será lógico y no se podrá utilizar como volumen del sistema.

Conversión de disco dinámico: de MBR a GPT

El dispositivo de arranque no admite la conversión directa de MBR a GPT para discos dinámicos. Sin embargo, puede efectuar las siguientes conversiones para lograr este objetivo:

1. Conversión de disco MBR: de dinámico a básico mediante la operación **Convertir a básico**.
2. Conversión de disco básico: De MBR a GPT mediante la operación **Convertir a GPT**.
3. Conversión de disco GPT: de básico a dinámico mediante la operación **Convertir a dinámico**.

Conversión del disco: de GPT a MBR

Si planea instalar un SO que no admite discos GPT, la conversión del disco GPT a MBR es posible.

Importante
El disco básico GPT que contiene el volumen de arranque con el sistema operativo en ejecución no se puede convertir a MBR.

Pasos para convertir un disco GPT a MBR

1. Haga clic con el botón derecho en el disco que desee clonar y después haga clic en **Convertir a MBR**.
2. Al hacer clic en **Aceptar**, agregará una operación pendiente de conversión de disco GPT a MBR.
3. Para completar la operación que ha añadido, ejecútela. Si sale del programa sin ejecutar la operación, se cancelará de manera efectiva.

Nota
Después de la operación, los volúmenes de este disco serán lógicos. Este cambio es irreversible.

Conversión de disco: de básico a dinámico

Puede convertir un disco básico a dinámico si:

- Planea usar el disco como parte de un grupo de discos dinámicos
- Desea lograr confiabilidad adicional del disco para el almacenamiento de datos

Pasos para convertir un disco básico a dinámico

1. Haga clic con el botón derecho en el disco que desee convertir y después haga clic en **Convertir a dinámico**.
2. Haga clic en **Aceptar**.

La conversión se efectuará de inmediato y, si es necesario, su equipo se reiniciará.

Nota
un disco dinámico ocupa el último megabyte del disco físico para almacenar la base de datos, incluso la descripción de cuatro niveles (volumen, componente, partición, disco) para cada volumen dinámico. Si durante la conversión del disco a dinámico, el disco básico está completo y el tamaño de los volúmenes no se puede reducir automáticamente, la operación no se realizará.
La conversión de discos que incluye volúmenes de sistema lleva cierto tiempo y cualquier pérdida de energía, apagado involuntario del equipo o presión accidental del botón de Restablecimiento durante el procedimiento podrían generar una pérdida en la capacidad de arranque.

En contraste con el Administrador de discos de Windows, el programa asegura la capacidad de arranque de un **sistema operativo fuera de línea** en el disco, después de la operación.

Conversión de disco: de dinámico a básico

Puede elegir convertir discos dinámicos de nuevo a básicos, por ejemplo, si desea usar un sistema operativo que no admita discos dinámicos.

Pasos para convertir un disco dinámico a básico:

1. Haga clic con el botón derecho en el disco que desee convertir y después haga clic en **Convertir a básico**.
2. Haga clic en **Aceptar**.

La conversión se efectuará de inmediato y, si es necesario, su equipo se reiniciará.

Nota
Esta operación no está disponible para discos dinámicos que contengan volúmenes extendidos, segmentados o RAID-5.

Después de la conversión, los últimos 8 Mb de espacio de disco se reservan para una conversión futura del disco de básico a dinámico. En algunos casos, es posible que difieran el espacio no asignado posible y el tamaño máximo de volumen propuesto (por ejemplo, cuando el tamaño de un espejo establece el del otro o cuando los últimos 8 Mb de espacio de disco están reservados para la conversión futura del disco de básico a dinámico).

Nota
La conversión de discos que incluyen volúmenes del sistema lleva cierto tiempo y cualquier pérdida de energía, apagado involuntario del equipo o presión accidental del botón de Restablecimiento durante el procedimiento podrían generar una pérdida en la capacidad de arranque.

En contraste con el Administrador de discos de Windows, el programa asegura:

- Una conversión segura de un disco dinámico a básico cuando contiene volúmenes **con datos** para volúmenes simples y duplicados
- En los sistemas de inicio múltiples, la capacidad de arranque del sistema que estuvo **fuera de línea** durante la operación

Operaciones del volumen

Con el dispositivo de arranque, puede realizar las siguientes operaciones en los volúmenes:

- Crear volumen: crea un volumen nuevo
- Eliminar volumen: elimina el volumen seleccionado
- Configurar activo: configura el volumen activo seleccionado para que el equipo pueda iniciarse con el SO instalado en el mismo
- Cambiar letra: cambia la letra del volumen seleccionada
- Cambiar etiqueta: cambia la etiqueta de volumen seleccionada
- Formatear volumen: formatea un volumen con un sistema de archivos

Tipos de volúmenes dinámicos

Volumen simple

Un volumen creado desde espacio libre de un único disco físico. Puede constar de una o varias regiones en el disco, unidas virtualmente por el Administrador de discos lógicos (LDM). No brinda confiabilidad adicional, ni mejora de velocidad, ni tamaño extra.

Volumen extendido

Un volumen creado desde espacio de disco libre unido virtualmente por el LDM, a partir de varios discos físicos. Se pueden incluir hasta 32 discos en un solo volumen, de manera tal que se superan las limitaciones de tamaño del hardware. Sin embargo, si tan solo un disco falla, se perderán todos los datos. Además, no se podrá eliminar ninguna parte del volumen extendido sin destruirlo en su totalidad. Por lo tanto, un volumen extendido no brinda confiabilidad adicional ni una mejor tasa de E/S.

Volumen segmentado

Un volumen, también denominado RAID 0, que consta de segmentos de datos de igual tamaño escritos a través de cada disco en el volumen. Es decir, para crear un volumen segmentado, necesita dos o más discos dinámicos. No es necesario que los discos de un volumen segmentado sean idénticos, pero debe haber espacio no utilizado disponible en cada disco que desee incluir en el volumen. El tamaño del volumen dependerá del tamaño del espacio más pequeño. El acceso a los datos de un volumen segmentado por lo general es más rápido que el acceso a los mismos datos en un disco físico único, porque la E/S está distribuida entre más de un disco.

Los volúmenes segmentados se crean para mejorar el rendimiento, no por su confiabilidad superior, ya que no contienen información redundante.

Volumen duplicado

Un volumen resistente a fallos, también denominado RAID 1, cuyos datos se duplican en dos discos físicos idénticos. Todos los datos de un disco se copian a otro, para brindar redundancia de datos. Casi todos los volúmenes se pueden duplicar, incluso los de sistema e inicio, si uno de los discos falla, es posible acceder a los datos desde los discos restantes. Desafortunadamente, las limitaciones del hardware en cuanto a tamaño y rendimiento son aún más graves con el uso de volúmenes duplicados.

Volumen duplicado-segmentado

Un volumen tolerante a errores, también denominado RAID 1+0, que combina la ventaja de la alta velocidad de E/S del diseño segmentado y la redundancia del tipo duplicado. La desventaja sigue siendo inherente a la arquitectura de duplicado: una baja proporción de tamaño de disco a volumen.

RAID-5

Un volumen resistente a fallos cuyos datos se segmentan a través de un conjunto de tres o más discos. No es necesario que los discos sean idénticos, pero debe haber bloques de igual tamaño de espacio no asignado disponible en cada disco del volumen. La paridad (un valor calculado que se puede utilizar para recuperar datos después de un fallo) también se segmenta en el conjunto de discos y siempre se almacena en un disco diferente al que contiene los datos. Si un disco físico falla, la porción del volumen RAID-5 que estaba en el disco donde se produjo el fallo se puede volver a crear a partir de los datos y la paridad restantes. Un volumen RAID-5 brinda confiabilidad y puede superar las limitaciones físicas del tamaño de discos con una proporción superior de tamaño disco a volumen, comparada con la del tipo duplicado.

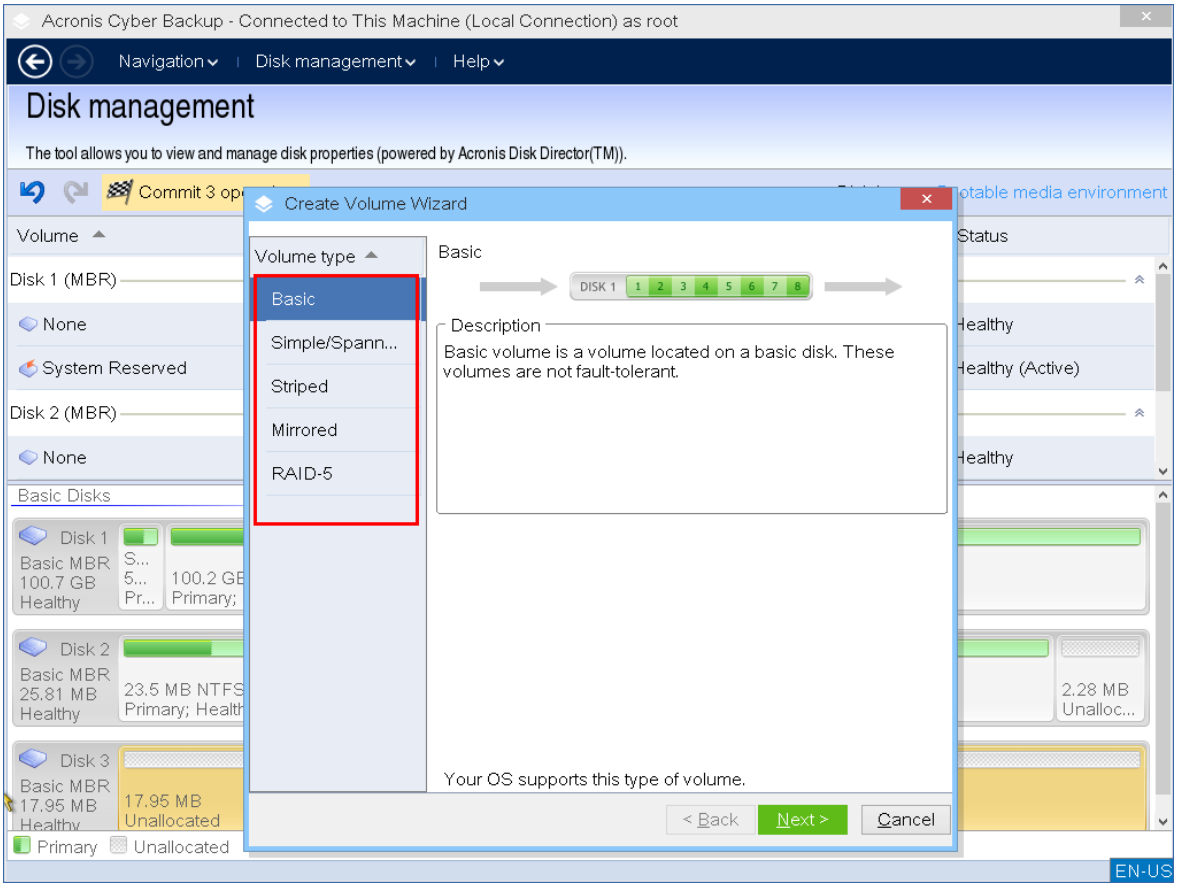
Crear un volumen

Es posible que necesite un volumen nuevo para:

- Recuperar una copia de seguridad guardada previamente en la configuración “tal como estaba”
- Almacenar colecciones de archivos similares por separado, por ejemplo, una colección de archivos MP3 o de video en un volumen separado
- Almacenar copias de seguridad (imágenes) de otros volúmenes/discos en un volumen especial
- Instalar un sistema operativo nuevo (o archivo de intercambio) en un volumen nuevo
- Agregar hardware nuevo a un equipo

Pasos para crear un volumen

1. Haga clic con el botón derecho en un espacio no asignado de un disco y después haga clic en **Crear volumen**. Se abrirá el asistente **Crear volumen**.



2. Seleccione el tipo de volumen. Las siguientes opciones están disponibles:
   - Básico
   - Simple/Extendido
   - Segmentado
   - Duplicado
   - RAID-5

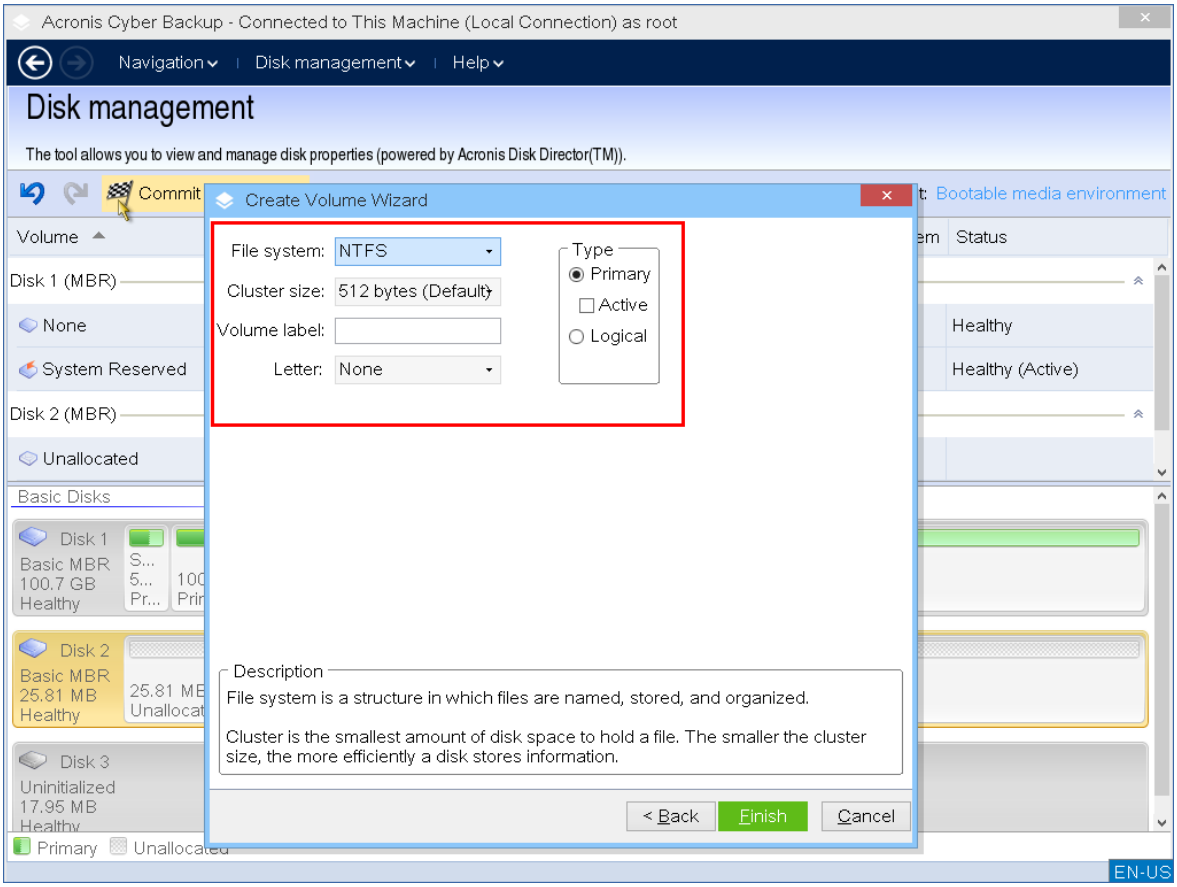
   Si el sistema operativo actual no admite el tipo de volumen seleccionado, recibirá una advertencia y se deshabilitará el botón **Siguiente**. Deberá seleccionar otro tipo de volumen para continuar.

3. Especifique el espacio sin asignar o seleccione los discos de destino.
   - En un volumen básico, especifique el espacio sin asignar en el disco seleccionado.
   - Seleccione uno o más discos de destino en un volumen simple/extendido.
   - Seleccione dos discos de destino en un volumen duplicado.
   - Seleccione dos o más discos de destino en un volumen segmentado.
   - Seleccione tres discos de destino en un volumen RAID-5

   Si está creando un volumen **dinámico** y selecciona uno o varios discos **básicos** como destino, recibirá una advertencia que indica que el disco seleccionado se convertirá a dinámico automáticamente.
4. Configurar el tamaño del volumen.

   Por lo general, el valor máximo incluye el mayor espacio no asignado posible. En algunos casos, el tamaño máximo de volumen propuesto puede variar (por ejemplo, cuando el tamaño de un espejo establece el del otro o cuando los últimos 8 Mb de espacio de disco están reservados para la conversión futura del disco de básico a dinámico).

   Puede escoger la posición de un nuevo volumen básico en un disco si el espacio no asignado de dicho disco es mayor que el volumen.
5. Configurar las opciones de volumen.



Puede asignar la **Letra** de volumen (por defecto, la primera letra del abecedario) y, como opción, una **Etiqueta** (por defecto, ninguna). Aquí también puede especificar el **Sistema de archivos** y el **Tamaño del clúster**.

Las posibles opciones del sistema de archivos son:

- FAT16 (deshabilitado, si el tamaño del volumen se configuró en más de 2 GB)
- FAT32 (deshabilitado, si el tamaño del volumen se configuró en más de 2 TB)
- NTFS
- Dejar el volumen sin formatear.

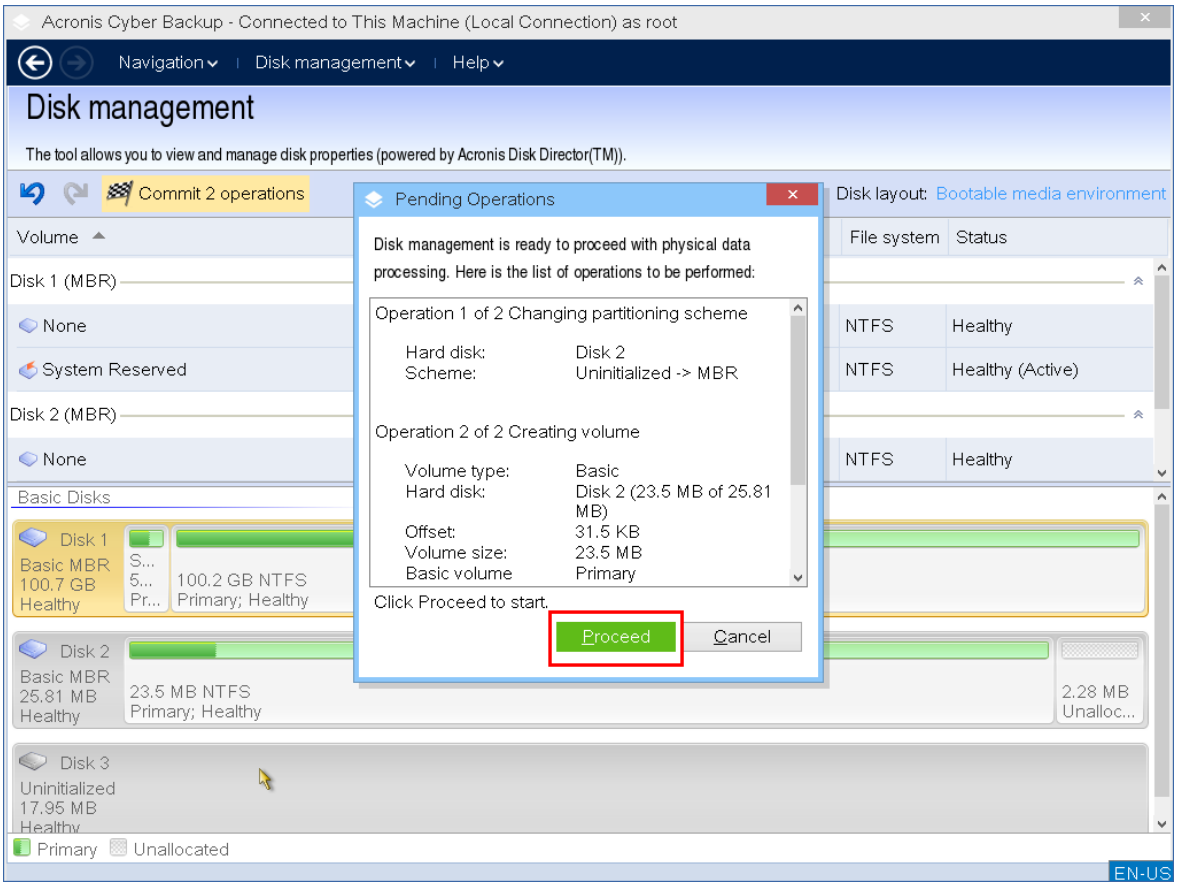
Al configurar el tamaño del clúster, puede elegir entre cualquier número en la cantidad preconfigurada para cada sistema de archivos. El mejor tamaño del clúster para el volumen, con el sistema de archivos elegido, es el que se sugiere de forma predeterminada. Si configura un tamaño del clúster de 64K para FAT16/FAT32, o bien un tamaño del clúster de 8KB-64KB para NTFS, Windows puede montar el volumen, pero algunos programas (por ejemplo, los programas de configuración) podrían calcular su espacio de disco de manera incorrecta.

Si está creando un volumen básico, el cual se puede convertir en un volumen del sistema, también puede seleccionar el tipo de volumen: **primario** (**activo primario**) o **lógico**. Por lo general, se selecciona **Primario** cuando quiere instalar un sistema operativo en un volumen. Seleccione el valor predeterminado **Activo** si quiere instalar un sistema operativo en este volumen que arranque al iniciar el equipo. Si el botón **Primario** no está seleccionado, la opción **Activo** estará inactiva. Si utilizará el volumen para almacenamiento de datos, seleccione **Lógico**.

Nota

Un disco básico puede contener hasta cuatro volúmenes primarios. Si ya existen, se deberá convertir el disco a dinámico, de otro modo las opciones **Activo** y **Primario** se deshabilitarán y sólo podrá seleccionar el tipo de volumen **Lógico** .

6. Haga clic en **Ejecutar** y después en **Continuar** en la ventana de **Operaciones pendientes**. Si sale del programa sin ejecutar la operación, se cancelará de manera efectiva.



Eliminar un volumen

Pasos para eliminar un volumen

1. Haga clic con el botón derecho en el volumen que desee eliminar.
2. Haga clic en **Eliminar volumen**.

> **Nota**
> Toda la información de ese volumen se perderá de forma irreversible.

3. Al hacer clic en **Aceptar**, añadirá una operación pendiente de eliminación de volumen.
4. Para completar la operación que ha añadido, ejecútela. Si sale del programa sin ejecutar la operación, se cancelará de manera efectiva.

Después de eliminar un volumen, se agrega su espacio al espacio de disco no asignado. Puede utilizarlo para crear un volumen nuevo o para cambiar el tipo de otro volumen.

Configurar volumen activo

Si tiene varios volúmenes primarios, debe especificar uno para que sea el volumen de inicio. Para esto, puede configurar un volumen para que sea el activo. Un disco puede tener solo un volumen activo.

Pasos para configurar un volumen activo:

1. Haga clic con el botón derecho en el volumen primario que desee, en un disco MBR básico, y haga clic en **Marcar como activo**.

   Si no hay otro volumen activo en el sistema, se agregará la operación pendiente de configuración de volumen activo. Si hay otro volumen activo presente en el sistema, recibirá una advertencia de que el volumen activo anterior se deberá configurar como pasivo en primer lugar.

   Nota
   Debido a la configuración del volumen activo nuevo, la letra del anterior se podría cambiar y algunos de los programas instalados podrían dejar de ejecutarse.

2. Al hacer clic en **Aceptar**, añadirá una operación pendiente de configuración de volumen activo.

   Nota
   Incluso si tiene el sistema operativo en el nuevo volumen activo, en algunos casos el equipo no podrá iniciarse desde allí. Deberá confirmar su decisión para configurar el volumen nuevo como activo.

3. Para completar la operación que ha añadido, ejecútela. Si sale del programa sin ejecutar la operación, se cancelará de manera efectiva.

Cambiar la letra del volumen

Los sistemas operativos Windows les asignan letras (C:, D:, etc.) a los volúmenes de los discos duros en el inicio. Las aplicaciones y los sistemas operativos usan estas letras para ubicar archivos y carpetas en los volúmenes. Al conectar un disco adicional y al crear o eliminar un volumen en los discos existentes, se podría cambiar la configuración del sistema. Como resultado, algunas aplicaciones dejan de funcionar correctamente o es posible que no se puedan encontrar ni abrir de manera automática los archivos del usuario. Para evitar esto, puede cambiar manualmente las letras que el sistema operativo asigna de manera automática a los volúmenes.

Cambiar una letra que asignó el sistema operativo a un volumen

1. Haga clic con el botón derecho en el volumen que desee y después haga clic en **Cambiar letra**.
2. Seleccione una letra nueva en la ventana **Cambiar letra**.
3. Al hacer clic en **Aceptar**, añadirá una operación pendiente de asignación de letra de volumen.
4. Para completar la operación que ha añadido, ejecútela. Si sale del programa sin ejecutar la operación, se cancelará de manera efectiva.

Cambiar la etiqueta de volumen

La etiqueta de volumen es un atributo opcional. Es un nombre asignado a un volumen para reconocerlo con mayor facilidad.

Pasos para cambiar una etiqueta de volumen

1. Haga clic con el botón derecho en el volumen que desee y después haga clic en **Cambiar etiqueta**.
2. Ingrese una etiqueta nueva en el campo de texto de la ventana **Cambiar etiqueta** .
3. Al hacer clic en **Aceptar**, añadirá una operación pendiente de cambio de etiqueta de volumen.
4. Para completar la operación que ha añadido, ejecútela. Si sale del programa sin ejecutar la operación, se cancelará de manera efectiva.

Formatear volumen

Se recomienda formatear un volumen si quiere cambiar su sistema de archivos:

- Guardar espacio adicional que se está perdiendo debido al tamaño del clúster en los sistemas de archivos FAT16 o FAT32
- Como una manera más rápida y más o menos confiable de destruir datos que se encuentran en este volumen

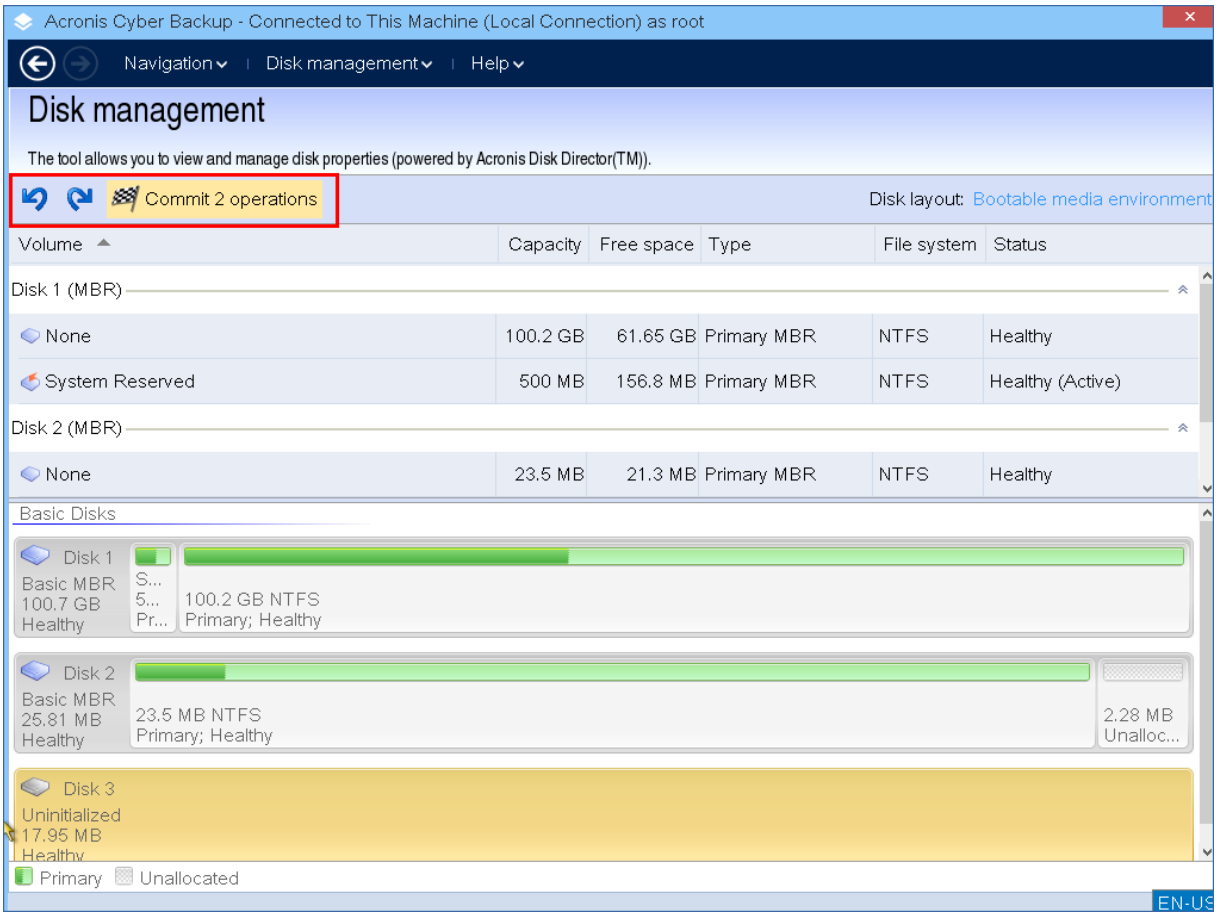
Para formatear un volumen:

1. Haga clic con el botón derecho en el volumen que desee y después haga clic en **Formatear**.
2. Seleccione el tamaño del clúster y el sistema de archivos. Las posibles opciones del sistema de archivos son:
   - FAT16 (deshabilitado, si el tamaño del volumen se configuró en más de 2 GB)
   - FAT32 (deshabilitado, si el tamaño del volumen se configuró en más de 2 TB)
   - NTFS
3. Al hacer clic en **Aceptar**, añadirá una operación pendiente de formateo de volumen.
4. Para completar la operación que ha añadido, ejecútela. Si sale del programa sin ejecutar la operación, se cancelará de manera efectiva.

Operaciones pendientes

Todas las operaciones se consideran pendientes hasta que emita y confirme el comando **Ejecutar**. Esto le permite controlar todas las operaciones planeadas, verificar dos veces los cambios pensados y, si es necesario, cancelar operaciones antes de que se ejecuten.

La vista **Administración del disco** contiene la barra de herramientas con iconos para iniciar las acciones de **Deshacer**, **Rehacer** y **Ejecutar** para las operaciones pendientes. Estas acciones también se podrían iniciar desde el menú **Administración del disco**.



Todas las operaciones planeadas se agregan a la lista de operaciones pendientes.

La acción **Deshacer** le permite deshacer la última operación de la lista. En tanto que la lista no esté vacía, esta acción está disponible.

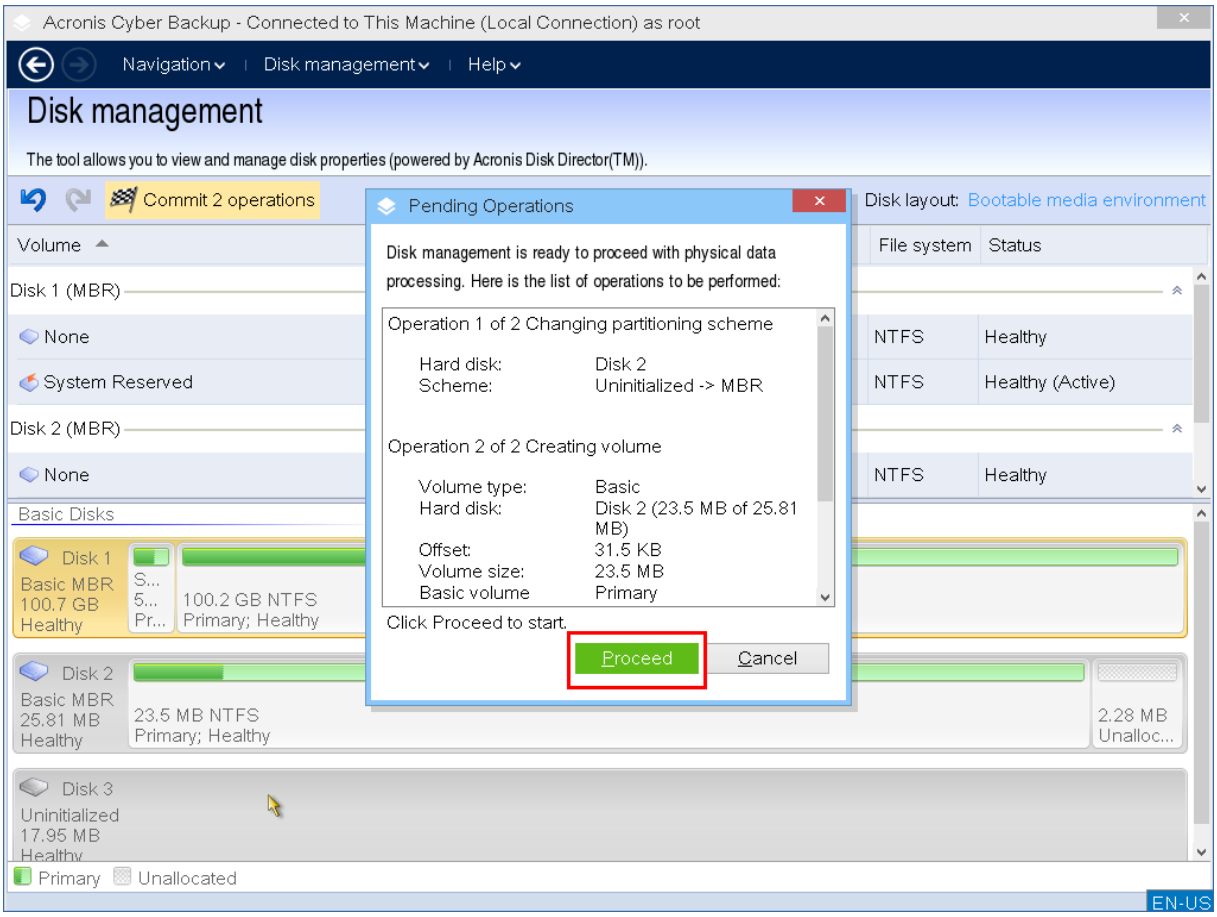
La acción **Rehacer** le permite rehacer la última operación pendiente que se deshizo.

La acción **Ejecutar** lo envía a la ventana de **Operaciones pendientes**, donde podrá visualizar la lista de operaciones pendientes.

Para iniciar su ejecución, haga clic en **Continuar**.

Nota
No podrá deshacer ninguna acción ni operación después de elegir la operación **Continuar**.

Si no desea continuar con la ejecución, haga clic en **Cancelar**. De este modo no se harán cambios en la lista de operaciones pendientes. Si sale del programa sin ejecutar las operaciones pendientes también las cancelará de manera efectiva.



Operaciones remotas con soportes de arranque

Para ver el soporte de arranque en la consola de Cyber Protect, primero debe registrarlo como se describe en "Registro de dispositivos en el servidor de gestión" (p. 441).

Después de registrar el medio en la consola de Cyber Protect, aparece en **Dispositivos** > **Soporte de arranque**.

Al utilizar la interfaz web, puede administrar los medios de forma remota. Por ejemplo, puede recuperar datos, reiniciar o apagar el equipo arrancado con el medio o ver información, actividades y alertas sobre el medio.

Pasos para recuperar archivos o carpetas con el soporte de arranque de forma remota

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Soporte de arranque**.
1. Seleccione el medio que desee utilizar para la recuperación de datos.
2. Haga clic en **Recuperación**.
3. Seleccione la ubicación y, a continuación, seleccione la copia de seguridad que necesite. Tenga en cuenta que las copias de seguridad se filtran por ubicación.
4. Seleccione el punto de recuperación y haga clic en **Recuperar archivos o carpetas**.

5. Vaya hasta la carpeta requerida o utilice la barra de búsqueda para obtener la lista de los archivos y carpetas deseados.

   Puede utilizar uno o más caracteres comodín (* y ?). Para obtener más información sobre el uso de los caracteres comodín, consulte la sección "Filtros de archivo" (p. 325).
6. Haga clic para seleccionar los archivos que desea recuperar y, a continuación, haga clic en **Recuperar**.
7. En **Ruta**, seleccione el destino de la recuperación.
8. [Opcional] Para la configuración de recuperación avanzada, haga clic en **Opciones de recuperación**. Para obtener más información, consulte "Opciones de recuperación" (p. 384).
9. Haga clic en **Iniciar recuperación**.
10. Seleccione una de las opciones de sobreescritura de archivos:
    - **Sobrescribir archivos existentes**
    - **Sobrescribir un archivo existente si es más antiguo**
    - **No sobrescribir archivos existentes**

    Elija si desea reiniciar el equipo automáticamente.
11. Haga clic en **Continuar** para iniciar la recuperación. El proceso de recuperación se muestra en la pestaña **Actividades**.

Pasos para recuperar discos, volúmenes o equipos completos con el soporte de arranque de forma remota

1. En la pestaña, **Dispositivos**, vaya al grupo **Soporte de arranque** y seleccione el medio que desee utilizar para la recuperación de datos.
2. Haga clic en **Recuperación**.
3. Seleccione la ubicación y, a continuación, seleccione la copia de seguridad que necesite. Tenga en cuenta que las copias de seguridad se filtran por ubicación.
4. Seleccione el punto de recuperación y haga clic en **Recuperar** > **Todo el equipo**.

   Si fuese necesario, configure el equipo de destino y la asignación de volúmenes como se describe en "Recuperación en un equipo físico" (p. 364).
5. Para la configuración de recuperación avanzada, haga clic en **Opciones de recuperación**. Para obtener más información, consulte "Opciones de recuperación" (p. 384).
6. Haga clic en **Iniciar recuperación**.
7. Confirme si desea sobrescribir los discos con sus respectivas copias de seguridad. Elija si desea reiniciar el equipo automáticamente.
8. El proceso de recuperación se muestra en la pestaña **Actividades**.

Pasos para reiniciar el equipo arrancado de forma remota

1. En la pestaña, **Dispositivos**, vaya al grupo **Soporte de arranque** y seleccione el medio que desee utilizar para la recuperación de datos.
2. Haga clic en **Reiniciar**.
3. Confirme que quiere reiniciar el equipo arrancado con el medio.

Pasos para apagar el equipo arrancado de forma remota

1. En la pestaña, **Dispositivos**, vaya al grupo **Soporte de arranque** y seleccione el medio que desee utilizar para la recuperación de datos.
2. Haga clic en **Apagar**.
3. Confirme que quiere apagar el equipo arrancado con el medio.

Pasos para ver información sobre el soporte de arranque

1. En la pestaña, **Dispositivos**, vaya al grupo **Soporte de arranque** y seleccione el medio que desee utilizar para la recuperación de datos.
2. Haga clic en **Detalles**, **Actividades** o **Alertas** para ver la información correspondiente.

Pasos para eliminar el soporte de arranque de forma remota

1. En la pestaña, **Dispositivos**, vaya al grupo **Soporte de arranque** y seleccione el medio que desee utilizar para la recuperación de datos.
2. Haga clic en **Eliminar** para eliminar el soporte de arranque de la consola de Cyber Protect.
3. Confirme que desea eliminar el soporte de arranque.

Configuración de los dispositivos iSCSI

Esta sección describe cómo configurar los dispositivos de la Internet Small Computer System Interface (iSCSI) mientras trabaja desde un dispositivo de arranque. Cuando haya realizado los pasos siguientes, podrá utilizar estos servicios como si estuvieran conectados localmente al equipo iniciado desde un dispositivo de arranque.

Un **servidor de destino iSCSI** (o **portal de destino**) es un servidor que aloja un dispositivo iSCSI. Un **objetivo de iSCSI** es un componente del servidor de destino; este componente comparte el dispositivo y especifica los iniciadores iSCSI que tienen permiso para acceder al dispositivo. Un **iniciador iSCSI** es un componente del equipo; este componente proporciona interacción entre el equipo y un objetivo de iSCSI. Al configurar el acceso a un dispositivo iSCSI en un equipo iniciado desde un dispositivo de arranque, debe especificar el portal de destino iSCSI del dispositivo y uno de los iniciadores iSCSI especificados en el objetivo. Si el destino comparte varios dispositivos, tendrá acceso a todos ellos.

Para añadir un dispositivo iSCSI a un dispositivo de arranque basado en Linux:

1. Haga clic en **Herramientas** > **Configurar dispositivos iSCSI/NDAS**.
2. Haga clic en **Añadir servidor**.
3. Especifique la dirección IP y el puerto del portal de destino iSCSI, y el nombre de cualquier iniciador iSCSI al que se permita acceder al dispositivo.
4. Si el servidor requiere autenticación, especifique el nombre de usuario y contraseña para el mismo.
5. Haga clic en **Aceptar**.

6. Seleccione el objetivo de iSCSI en la lista y haga clic en **Conectar**.
7. Si la autenticación CHAP está habilitada en la configuración del objetivo de iSCSI, se le pedirán las credenciales para acceder al objetivo de iSCSI. Especifique el mismo nombre de usuario y secreto de destino que en la configuración del objetivo de iSCSI. Haga clic en **Aceptar**.
8. Haga clic en **Cerrar** para cerrar la ventana.

Para añadir un dispositivo iSCSI a un dispositivo de arranque basado en PE:

1. Haga clic en **Herramientas** > **Ejecutar la instalación de iSCSI**.
2. Haga clic en la pestaña **Detección**.
3. En **Portales de destino**, haga clic en **Añadir** y especifique la dirección IP y el puerto del portal de destino iSCSI. Haga clic en **Aceptar**.
4. Haga clic en la pestaña **General**, haga clic en **Cambiar** y especifique el nombre de cualquier iniciador iSCSI al que se permita acceder al dispositivo.
5. Haga clic en la pestaña **Objetivos**, haga clic en **Actualizar**, seleccione el objetivo de iSCSI de la lista y haga clic en **Conectar**. Haga clic en **Aceptar** para conectarse al objetivo de iSCSI.
6. Si la autenticación CHAP está habilitada en la configuración del objetivo de iSCSI, verá un error de **Autentificación**. En este caso, haga clic en **Conectar**, haga clic en **Avanzado**, active la casilla de verificación **Habilitar inicio de sesión CHAP**, y especifique el mismo nombre de usuario y secreto de destino que en la configuración del objetivo de iSCSI. Haga clic en **Aceptar** para cerrar la ventana y en **Aceptar** de nuevo para conectarse al objetivo de iSCSI.
7. Haga clic en **Aceptar** para cerrar la ventana.

Startup Recovery Manager

Startup Recovery Manager es un componente de arranque que reside en su disco duro. Con Startup Recovery Manager, podrá iniciar la utilidad de rescate de arranque sin utilizar un soporte de arranque independiente.

Startup Recovery Manager es especialmente útil para los usuarios que viajan. Si se produce un fallo, reinicie el equipo, espere a que se muestre el mensaje **Pulse F11 para que aparezca Acronis Startup Recovery Manager...** y, a continuación, pulse F11. El programa se iniciará y podrá realizar la recuperación. En equipos con el cargador de arranque GRUB instalado, seleccione Startup Recovery Manager en el menú de arranque en lugar de pulsar F11 durante el reinicio.

También puede realizar copias de seguridad con Startup Recovery Manager mientras está en movimiento.

Para utilizar Startup Recovery Manager, debe activarlo. Así activará el mensaje de tiempo de arranque **Pulse F11 para Acronis Startup Recovery Manager** (o añada el elemento **Startup Recovery Manager** al menú de GRUB si utiliza el cargador de arranque GRUB).

Nota
Para activar Startup Recovery Manager en un equipo con un volumen del sistema no cifrado, el equipo debe tener por lo menos 100 MB de espacio libre. Las operaciones de recuperación que requieren reiniciar el equipo necesitan 100 MB más.

Puede activar Startup Recovery Manager en un equipo que tenga un volumen cifrado con BitLocker si este tiene al menos otro volumen no cifrado. El volumen no cifrado debe tener por lo menos 500 MB de espacio libre. Para las operaciones de recuperación que requieren reiniciar el equipo, este debe tener otros 500 MB de espacio libre.

Importante
Si no se puede activar Startup Recovery Manager, fallarán las operaciones de copia de seguridad que crean las copias de seguridad de recuperación con un clic.

A menos que use el cargador de arranque GRUB y este esté instalado en el registro de arranque maestro (MBR), la activación de Startup Recovery Manager sobrescribirá el registro de inicio maestro con su propio código de arranque. Por lo tanto, necesitará activar nuevamente cargadores de inicio de terceros, si están instalados.

En Linux, cuando se utiliza un cargador de arranque que no sea GRUB (como LILO, por ejemplo), considere instalarlo en un registro de inicio de partición de raíz (o inicio) de Linux en lugar de MBR antes de activar Startup Recovery Manager. De lo contrario, vuelva a configurar este cargador de inicio manualmente después de la activación.

Activación de Startup Recovery Manager

En un equipo que ejecute el Agente para Windows o el Agente para Linux, puede activar Startup Recovery Manager mediante la consola web de Cyber Protect.

Pasos para activar Startup Recovery Manager en la consola web de Cyber Protect

1. Seleccione el equipo en el que desea activar Startup Recovery Manager.
2. Haga clic en **Detalles**.
3. Habilite el conmutador de **Startup Recovery Manager**.
4. Espere mientras el software activa Startup Recovery Manager.

Pasos para activar Startup Recovery Manager en un equipo sin un agente

1. Inicie el equipo desde un dispositivo de arranque.
2. Haga clic en **Herramientas** > **Activar Startup Recovery Manager**.
3. Espere mientras el software activa Startup Recovery Manager.

Desactivación de Startup Recovery Manager

Para desactivar Startup Recovery Manager, repita el procedimiento de activación y seleccione las acciones opuestas correspondientes. La desactivación deshabilita el mensaje de tiempo de inicio **Pulse F11 para Acronis Startup Recovery Manager** (o el elemento del menú en GRUB).

Si Startup Recovery Manager no está activado, necesitará realizar algunas de las siguientes acciones para recuperar el sistema cuando el arranque falle:

- inicie el equipo desde un dispositivo de arranque diferente;
- realice el inicio de red desde PXE Server o Microsoft Remote Installation Services (RIS).

Servidor PXE Acronis

El servido PXE de Acronis permite el inicio del equipo de los componentes de arranque de Acronis a través de la red.

Inicio en red:

- Elimina la necesidad de contar con un técnico en el lugar para instalar el dispositivo de arranque en el sistema que debe iniciarse.
- Durante las operaciones de los grupos, reduce el tiempo requerido para el inicio de múltiples equipos en comparación al uso de dispositivos de arranque.

Los componentes se cargan a Acronis PXE Server utilizando Acronis Bootable Media Builder. Para cargar los componentes de inicio, inicie Bootable Media Builder y siga las instrucciones paso a paso descritas en la sección "Dispositivos de arranque basados en Linux".

El inicio de varios equipos desde Acronis PXE Server tiene sentido si hay un servidor de Protocolo de configuración dinámica de servidores (DHCP) en su red. Entonces, las interfaces de red de los equipos iniciados obtendrán sus direcciones IP automáticamente.

Limitación:

Acronis PXE Server no es compatible con el cargador de arranque UEFI.

Instalación de Acronis PXE Server

Para instalar Acronis PXE Server

1. Inicie sesión como administrador e inicie el programa de instalación de Acronis Cyber Protect.
2. [Opcional] Para cambiar el idioma del programa de instalación, haga clic en **Idioma de instalación**.
3. Acepte los términos del acuerdo de licencia y la declaración de privacidad y, a continuación, haga clic en **Siguiente**.

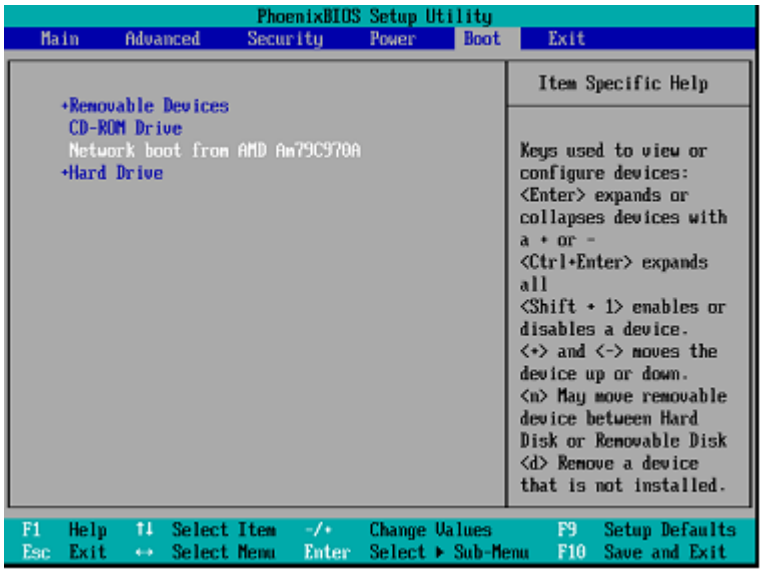
4. Haga clic en **Personalizar configuración de la instalación**.
5. Junto a **Qué instalar**, haga clic en **Cambiar**.
6. Marque la casilla de verificación **PXE Server**. Si no desea instalar otros componentes en este equipo, desmarque las casillas de verificación que corresponda. Haga clic en **Realizado** para continuar.
7. [Opcional] Cambiar otras configuraciones de la instalación.
8. Haga clic en **Instalar** para proceder con la instalación.
9. Cuando haya terminado la instalación, haga clic en **Cerrar**.

Acronis PXE Server se ejecuta como un servicio inmediatamente después de la instalación. Más adelante, se iniciará automáticamente en cada reinicio del sistema. Puede detener e iniciar Acronis PXE Server del mismo modo que otros servicios de Windows.

Configuración de un equipo para que inicie desde PXE.

Para que sea completa, es suficiente que el BIOS del equipo admita el arranque desde red.

En un equipo que tiene un sistema operativo en el disco duro, se debe configurar el BIOS para que la interfaz de red sea el primer dispositivo de arranque o, al menos, tenga prioridad ante la unidad de disco duro. El ejemplo que se muestra a continuación indica una de las configuraciones de BIOS razonables. Si no inserta el dispositivo de arranque, el equipo se iniciará desde la red.



En algunas versiones de BIOS, debe guardar los cambios de la BIOS después de activar la tarjeta de interfaz de red para que ésta aparezca en la lista de dispositivos de arranque.

Si el hardware cuenta con múltiples tarjetas de interfaz de red, asegúrese de que la tarjeta compatible con la BIOS tenga el cable de red conectado.

Trabajo en todas las subredes

Para permitir que el Acronis PXE Server trabaje en otra subred (mediante el conmutador), configure el conmutador para que retransmita el tráfico de PXE. Las direcciones IP del servidor PXE se configuran por interfaz mediante la función auxiliar IP, de la misma manera que las direcciones del servidor DHCP. Para obtener más información, consulte la página https://docs.microsoft.com/es-es/troubleshoot/mem/configmgr/boot-from-pxe-server.

Protección de dispositivos móviles

La aplicación de copia de seguridad le permite realizar una copia de seguridad de los datos de un dispositivo móvil en el almacenamiento en la nube para que pueda recuperarlos en caso de pérdida o daños. Tenga en cuenta que el uso del almacenamiento en la nube requiere una cuenta y una suscripción a la nube.

Dispositivos móviles compatibles

Puede instalar la aplicación de copia de seguridad en cualquier dispositivo móvil que ejecute uno de los siguientes sistemas operativos:

- iOS 15 a iOS 17 (iPhone, iPod, iPad)
- De Android 9 a Android 13

De qué puede realizar una copia de seguridad

- Contactos
- Fotografías
- Vídeos
- Calendarios
- Recordatorios (solo en dispositivos iOS)

Qué necesita saber

- Puede realizar una copia de seguridad de los datos solo en el almacenamiento en la cloud.
- Cuando abra la aplicación, verá el resumen de los cambios en los datos y podrá iniciar manualmente una copia de seguridad.
- La funcionalidad **Copia de seguridad continua** se encuentra habilitada de forma predeterminada. Al activar esta configuración:
  - En Android 7.0 o versiones posteriores, la aplicación de copia de seguridad detectará automáticamente los datos nuevos sobre la marcha y los subirá a la nube.
  - En Android 5 y 6, buscará cambios cada tres horas. Puede desactivar la copia de seguridad continua en la configuración de la aplicación.
- La opción **Usar Wi-Fi solamente** está habilitada de forma predeterminada en la configuración de la aplicación. Si se activa esta configuración, la aplicación de copia de seguridad realizará una copia de seguridad de los datos solo cuando se disponga de una conexión Wi-Fi. En el caso de perder la conexión, no se iniciará el proceso de copia de seguridad. Si quiere que la aplicación también pueda usar los datos móviles, desactive esta opción.
- Existen dos métodos para ahorrar batería:

- La función **Realizar cop. de seg. durante la carga**, que está deshabilitada de forma predeterminada. Si se activa esta configuración, la aplicación de copia de seguridad realizará una copia de seguridad de los datos solo cuando el dispositivo esté conectado a la corriente. En el caso de que el dispositivo se desconecte de la corriente durante un proceso de copia de seguridad continua, se pausará la copia de seguridad.
- El **modo de ahorro de energía**, que está habilitado de forma predeterminada. Si se activa esta configuración, la aplicación de copia de seguridad realizará una copia de seguridad de los datos solo cuando el dispositivo tenga un nivel de batería adecuado. Cuando el nivel de batería sea bajo, se pausará la copia de seguridad continua. Esta opción está disponible para Android 8 o versiones posteriores.

- Puede acceder a los datos de la copia de seguridad desde cualquier dispositivo móvil registrado en su cuenta. Esto le ayudará a transferir los datos desde un dispositivo móvil antiguo a uno nuevo. Los contactos y fotografías de un dispositivo Android pueden recuperarse en un dispositivo iOS y viceversa. También puede descargar una foto, un vídeo o un contacto en cualquier dispositivo mediante la consola web de Cyber Protect.
- Los datos de los que realizó una copia de seguridad desde un dispositivo móvil registrado en su cuenta solo están disponibles en dicha cuenta. Nadie más puede ver o recuperar sus datos.
- En la aplicación de copia de seguridad solo puede recuperar la versión más reciente de los datos. Si necesita recuperar datos de una versión de copia de seguridad específica, use la consola web de Cyber Protect en una tableta o un ordenador.
- Solo para dispositivos Android: si hay una tarjeta SD presente durante la copia de seguridad, también se realizará una copia de seguridad de los datos almacenados en dicha tarjeta. Los datos se recuperarán en la carpeta **Recuperado por la copia de seguridad** de una tarjeta SD si está presente durante la recuperación. En caso contrario, la aplicación le solicitará que indique otra ubicación en la que recuperar los datos.

Dónde obtener la aplicación de copia de seguridad

1. En un dispositivo móvil, abra un explorador y vaya a https://backup.acronis.com/.
2. Inicie sesión con los datos de su cuenta.
3. Haga clic en **Todos los dispositivos** > **Añadir**.
4. En **Dispositivos móviles**, seleccione el tipo de dispositivo.
   Según el tipo de dispositivo, es posible que sea redirigido a App Store o Google Play.
5. [Solo en dispositivos iOS] Haga clic en **Obtener**.
6. Haga clic en **Instalar** para instalar la aplicación de copias de seguridad.

Cómo empezar a realizar copias de seguridad de los datos

1. Abra la aplicación.
2. Inicie sesión con los datos de su cuenta.

Toque **Configurar** para crear su primera copia de seguridad.

1. Seleccione las categorías de datos de las que desea realizar la copia de seguridad. De manera predeterminada, se seleccionan todas las categorías.
2. Paso opcional: habilite **Cifrar copia de seguridad** para proteger su copia de seguridad con cifrado. En ese caso, también deberá hacer lo siguiente:
   a. Escriba una contraseña de cifrado en dos campos distintos.

      Nota
      Es importante que recuerde la contraseña, puesto que, si se le olvida, no podrá restaurarla ni cambiarla.

   b. Pulse **Cifrar**.
3. Pulse **Crear copia de seguridad**.
4. Permita a la aplicación acceder a sus datos personales. Si deniega el acceso a algunas categorías de datos, estas no se incluirán en la copia de seguridad.

La copia de seguridad comienza.

Cómo recuperar los datos en un dispositivo móvil

1. Abra la aplicación de copias de seguridad.
2. Pulse **Examinar**.
3. Pulse el nombre del dispositivo.
4. Realice uno de los siguientes procedimientos:
   - Para recuperar todos los datos incluidos en la copia de seguridad, pulse **Recuperar todos**. No es necesario realizar más acciones.
   - Para recuperar una o más categorías de datos, pulse **Seleccionar** y después seleccione las casillas de verificación de las categorías elegidas. Pulse **Recuperar**. No es necesario realizar más acciones.
   - Para recuperar uno o más elementos que pertenecen a la misma categoría de datos, pulse la categoría de datos concreta. Continúe a los pasos siguientes.
5. Realice uno de los siguientes procedimientos:

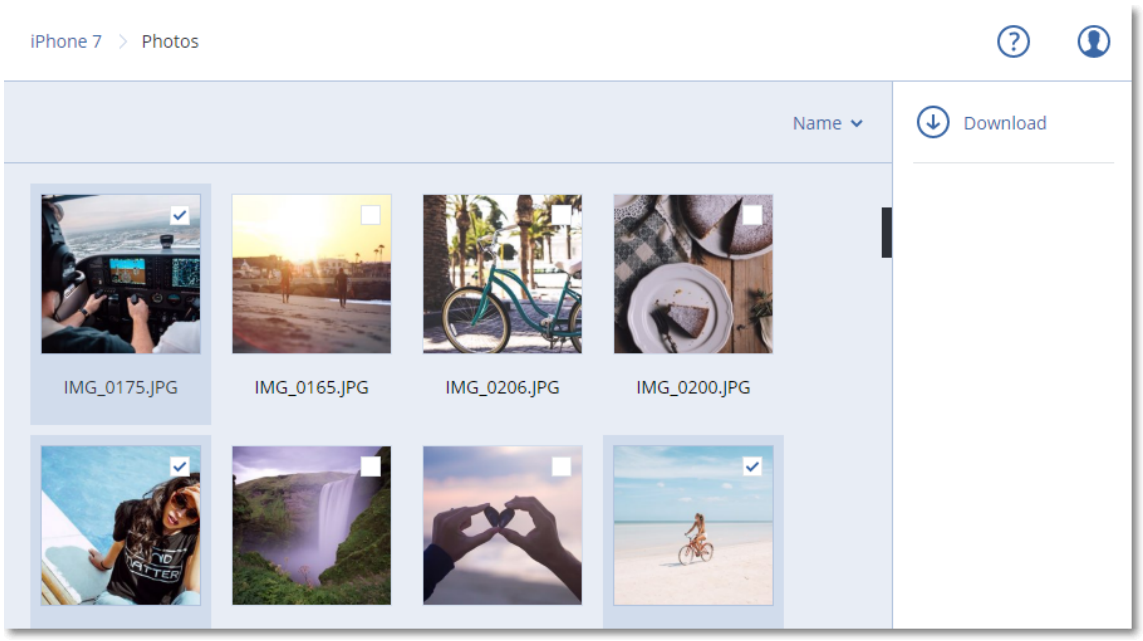
- Para recuperar un único elemento, púlselo.
- Para recuperar varios elementos, pulse **Seleccionar** y después seleccione las casillas de verificación de los elementos elegidos.

6. Pulse **Recuperar**.

Cómo revisar los datos a través de la consola web de Cyber Protect

1. En un equipo, abra un explorador y escriba la URL de la consola web Cyber Protect.
2. Inicie sesión con los datos de su cuenta.
3. En **Todos los dispositivos**, haga clic en la opción **Recupera** bajo el nombre de su dispositivo móvil.
4. Realice una de las siguientes operaciones:
   - Para descargar las fotografías, los vídeos, los contactos, los calendarios o los recordatorios del dispositivo, seleccione las categorías de datos correspondientes. Haga clic en **Descargar**.

   - Para descargar fotografías, vídeos, contactos, calendarios o recordatorios específicos, seleccione el nombre de la categoría de datos correspondiente y, después, marque las casillas de verificación de los elementos en cuestión. Haga clic en **Descargar**.



- Para ver una vista preliminar de una fotografía o un contacto, seleccione el nombre de la categoría de datos correspondiente y, después, haga clic en el elemento elegido.

Protección de aplicaciones de Microsoft

Importante
Algunas de las funciones descritas en esta sección solo están disponibles en implementaciones locales.

Protección de Microsoft SQL Server y Microsoft Exchange Server

Existen dos métodos para proteger estas aplicaciones:

- **Copia de seguridad de la base de datos**
  Se trata de una copia de seguridad a nivel de archivo de las bases de datos y los metadatos asociados. Las bases de datos se pueden recuperar en una aplicación activa o como archivos.
- **Copia de seguridad compatible con la aplicación**
  Se trata de una copia de seguridad a nivel de disco que también recopila los metadatos de las aplicaciones. Estos metadatos permiten la exploración y la recuperación de los datos de las aplicaciones sin que sea necesario recuperar todo el disco o volumen. También se puede recuperar el disco o volumen entero. Esto significa que se puede utilizar una única solución y un solo plan de protección para la recuperación ante desastres y para la protección de datos.

Para Microsoft Exchange Server, puede optar por **Copia de seguridad de buzón de correo**. Esta es una copia de seguridad de buzones de correo individuales que se realiza a través del protocolo de Exchange Web Services. Los buzones de correo o elementos de los buzones de correo pueden recuperarse a un servidor activo de Exchange Server o a Microsoft 365. La copia de seguridad del buzón de correo es compatible con Microsoft Exchange Server 2010 servicio Pack 1 (SP1) o versión posterior.

Protección de Microsoft SharePoint

Una granja de Microsoft SharePoint está compuesta por servidores front-end que ejecutan servicios de SharePoint, servidores de bases de datos que ejecutan Microsoft SQL Server y (opcionalmente) servidores de aplicaciones que excluyen algunos servicios de SharePoint de los servidores front-end. Algunos servidores front-end y de aplicaciones pueden ser idénticos entre sí.

Para proteger toda una granja de SharePoint:

- Haga una copia de seguridad de todos los servidores de bases de datos con una copia de seguridad compatible con la aplicación.
- Haga una copia de seguridad de todos los servidores front-end únicos y los servidores de aplicaciones con una copia de seguridad normal a nivel de disco.

Las copias de seguridad de todos los servidores se deben realizar en la misma fecha.

Para proteger solo el contenido, puede hacer una copia de seguridad de las bases de datos de contenido por separado.

Protección de un controlador de dominio

Un equipo que ejecuta Servicios de dominio de Active Directory se puede proteger con una copia de seguridad compatible con la aplicación. Si un dominio contiene más de un controlador de dominios y desea recuperar alguno de ellos, se realizará una restauración no autorizada y no habrá reversión USN alguna después de la recuperación.

Recuperación de aplicaciones

La siguiente tabla recoge los métodos de recuperación de aplicaciones disponibles.

	A partir de una copia de seguridad de base de datos	**A partir de una copia de seguridad compatible con la aplicación**	**A partir de una copia de seguridad del disco**
Microsoft SQL Server	Bases de datos a una instancia activa de SQL Server Bases de datos como archivos	Todo el equipo Bases de datos a una instancia activa de SQL Server Bases de datos como archivos	Todo el equipo
Microsoft Exchange Server	Bases de datos a un servidor activo de Exchange Bases de datos como archivos Recuperación granular a un servidor activo de Exchange Server o a Microsoft 365*	Todo el equipo Bases de datos a un servidor activo de Exchange Bases de datos como archivos Recuperación granular a un servidor activo de Exchange Server o a Microsoft 365*	Todo el equipo
Servidores de bases de datos de Microsoft SharePoint	Bases de datos a una instancia activa de SQL Server Bases de datos como archivos Recuperación granular mediante SharePoint Explorer	Todo el equipo Bases de datos a una instancia activa de SQL Server Bases de datos como archivos Recuperación granular mediante SharePoint	Todo el equipo

		Explorer	
Servidor web front-end de Microsoft SharePoint	-	-	Todo el equipo
Servicios de dominio de Active Directory	-	Todo el equipo	-

* La recuperación granular también está disponible a partir de la copia de seguridad de un buzón de correo.

Requisitos previos

Antes de configurar la copia de seguridad de la aplicación, asegúrese de que se cumplen los siguientes requisitos.

Para consultar el estado de los escritores de VSS, use el comando `vssadmin list writers`.

Requisitos habituales

En Microsoft SQL Server, asegúrese de que:

- Se haya iniciado al menos una instancia de Microsoft SQL Server.
- El escritor de SQL para VSS esté activado.

En Microsoft Exchange Server, asegúrese de que:

- Se haya iniciado el servicio del almacén de información de Microsoft Exchange.
- Windows PowerShell esté instalado. En Exchange 2010 o posterior, la versión de Windows PowerShell debe ser, como mínimo, 2.0.
- Microsoft .NET Framework esté instalado.
  En Exchange 2007, la versión de Microsoft .NET Framework debe ser, como mínimo, 2.0.
  En Exchange 2010 o posterior, la versión de Microsoft .NET Framework debe ser, como mínimo, 3.5.
- El escritor de Exchange para VSS está activado.

Nota
Agent for Exchange necesita un almacenamiento temporal para funcionar. De manera predeterminada, los archivos temporales se encuentran en `%ProgramData%\Acronis\Temp`. Asegúrese de que el espacio libre del volumen en el que se encuentra la carpeta `%ProgramData%` es, como mínimo, igual al 15 % del tamaño de una base de datos de Exchange. Como alternativa, puede cambiar la ubicación de los archivos temporales antes de crear las copias de seguridad de Exchange, según se describe en: https://kb.acronis.com/content/40040.

En un controlador de dominio, asegúrese de que:

- El escritor de Active Directory para VSS esté activado.

Al crear un plan de protección, asegúrese de que:

- En los equipos físicos, la opción de copia de seguridad Volume Shadow Copy Service (VSS) esté habilitada.
- En los equipos virtuales, la opción de copia de seguridad Volume Shadow Copy Service (VSS) para equipos virtuales esté habilitada.

Otros requisitos para copias de seguridad compatibles con la aplicación

Al crear un plan de protección, compruebe que **Todo el equipo** esté seleccionado para la copia de seguridad. Debe deshabilitarse la opción **Sector por sector** en el plan de protección o, de lo contrario, será imposible realizar una recuperación de datos de aplicaciones desde tales copias de seguridad. Si el plan se ejecuta en el modo **sector por sector** debido a un cambio automático a dicho modo, también será imposible recuperar los datos de aplicaciones.

Requisitos para equipos virtuales ESXi

Si la aplicación se ejecuta en un equipo virtual del que Agent para VMware hace una copia de seguridad, asegúrese de que:

- El equipo virtual del que se va a realizar una copia de seguridad cumple los requisitos de copia de seguridad y restauración consistentes con la aplicación que aparecen en el artículo "Implementaciones de la copia de seguridad de Windows" de la documentación de VMware: https://code.vmware.com/docs/1674/virtual-disk-programming-guide/doc/vddkBkupVadp.9.6.html
- Las herramientas de VMware están instaladas y actualizadas en el equipo.
- El control de cuentas de usuario (UAC) está deshabilitado en el equipo. Si no desea deshabilitar el UAC, debe proporcionar las credenciales de un administrador de dominios incorporados (DOMINIO\Administrador) al habilitar la copia de seguridad de la aplicación.

Requisitos de equipos virtuales Hyper-V

Si la aplicación se ejecuta en un equipo virtual del que Agent para Hyper-V hace una copia de seguridad, asegúrese de que:

- El sistema operativo invitado es Windows Server 2008 o posterior.
- Para Hyper-V 2008 R2: el sistema operativo invitado es Windows Server 2008/2008 R2/2012.
- El equipo virtual no tiene disco dinámico.
- Existe conexión de red entre el host de Hyper-V y el sistema operativo invitado. Esto es necesario para ejecutar consultas de WMI remotas dentro del equipo virtual.

- El control de cuentas de usuario (UAC) está deshabilitado en el equipo. Si no desea deshabilitar el UAC, debe proporcionar las credenciales de un administrador de dominios incorporados (DOMINIO\Administrador) al habilitar la copia de seguridad de la aplicación.
- La configuración del equipo virtual cumple los siguientes criterios:
  - Hyper-V Integration Services está instalado y actualizado. La actualización crítica es https://support.microsoft.com/en-us/help/3063109/hyper-v-integration-components-update-for-windows-virtual-machines
  - En la configuración del equipo virtual, la opción **Gestión** > **Integration Services** > **Copia de seguridad (punto de comprobación de volumen)** está habilitada.
  - Para Hyper-V 2012 y posterior: el equipo virtual no tiene puntos de comprobación.
  - Para Hyper-V 2012 R2 y posterior: el equipo virtual tiene un controlador SCSI (compruebe **Configuración** > **Hardware**).

Copia de seguridad de la base de datos

Antes de hacer una copia de seguridad de las bases de datos, asegúrese de cumplir con los requisitos recogidos en "Requisitos previos".

Seleccione las bases de datos tal como se describe a continuación y luego especifique otros ajustes del plan de protección según corresponda.

Seleccionar bases de datos de SQL

La copia de seguridad de una base de datos de SQL contiene archivos de base de datos (.mdf, .ndf), archivos de registro (.ldf) y otros archivos asociados. Los archivos son copiados con la ayuda del servicio Writer de SQL. El servicio se debe estar ejecutando a la vez que el Volume Shadow Copy Service (VSS) solicita una copia de seguridad o recuperación.

Los registros de transacción de SQL se truncan después de crear una copia de seguridad correctamente. El truncamiento de registros de SQL se puede deshabilitar en las opciones del plan de protección.

Para seleccionar bases de datos de SQL

1. Haga clic en **Dispositivos** > **Microsoft SQL**.
   El software muestra el árbol de los grupos de disponibilidad Always On (AAG) de SQL Server, equipos que ejecutan Microsoft SQL Server, instancias de SQL Server y bases de datos.
2. Busque los datos de los que desea realizar la copia de seguridad.
   Expanda los nodos del árbol o haga doble clic en los elementos de la lista de la parte derecha del árbol.
3. Seleccione los datos de los que desea realizar la copia de seguridad. Puede seleccionar los AAG, equipos que ejecuten SQL Server, instancias de SQL Server o bases de datos individuales.
   - Si selecciona un AAG, se realizará una copia de seguridad de todas las bases de datos que se incluyan en el AAG seleccionado. Para obtener más información acerca de la copia de seguridad de los AAG o las bases de datos AAG individuales, consulte "Protección de los

grupos de disponibilidad Always On (AAG)".

- Si selecciona un equipo que ejecute un SQL Server, se realizará una copia de seguridad de todas las bases de datos conectadas a todas las instancias de SQL Server que se ejecuten en el equipo seleccionado.
- Si selecciona un instancia de SQL Server, se realizará una copia de seguridad de todas las bases de datos conectadas a la instancia seleccionada.
- Si selecciona base de datos concretas, únicamente se realizarán copias de seguridad de las bases de datos seleccionadas.

4. Haga clic en **Proteger**. Si se le pide, proporcione las credenciales para acceder a los datos de SQL Server.

   Si usa la autenticación de Windows, la cuenta debe ser miembro del grupo **Operadores de copia de seguridad** o **Administradores** en el equipo y miembro de la función **administrador del sistema** en cada una de las instancias de las que va a realizar la copia de seguridad.

   Si usa la autenticación del Servidor SQL, la cuenta debe ser miembro de la función **administrador del sistema** en cada una de las instancias de las que va a realizar la copia de seguridad.

Seleccionar datos de Exchange Server

La siguiente tabla resume los datos de Microsoft Exchange Server que puede seleccionar para realizar la copia de seguridad y los permisos de usuario mínimos requeridos para realizar la copia de seguridad de los datos.

Versión de Exchange	Elementos de los datos	Permisos de usuario
2007	Grupos de almacenamiento	Asociación en el grupo de funciones **Administradores de la organización de Exchange**.
2010/2013/2016/2019	Bases de datos, grupos de disponibilidad de base de datos (DAG)	Pertenencia al grupo de funciones **Administración de servidores**.

Una copia de seguridad completa contiene todos los datos seleccionados de Exchange Server.

Una copia de seguridad incremental contiene los bloques cambiados de los archivos de la base de datos, los archivos de control y una pequeña cantidad de archivos de acceso que son más recientes que el punto de control de la base de datos correspondiente. Ya que los cambios en los archivos de la base de datos están incluidos en la copia de seguridad, no hay necesidad de realizar copias de seguridad de todos los registros de acceso de transacción desde la copia de seguridad anterior. Después de una recuperación, únicamente se necesita reproducir el acceso que sea más reciente que el punto de control. Esto garantiza una recuperación más rápida y que la copia de seguridad de la base de datos se realice con éxito, aun con el registro circular habilitado.

Los archivos de registro de transacción quedan truncados después de cada copia de seguridad realizada con éxito.

Para seleccionar datos de Exchange Server

1. Haga clic en **Dispositivos** > **Microsoft Exchange**.
   El software muestra el árbol de los grupos de disponibilidad de base de datos (DAG) de Exchange Server, equipos que ejecutan Microsoft Exchange Server y bases de datos de Exchange Server. Si ha configurado Agent for Exchange tal y como se describe en "Copia de seguridad de buzones de correo", los buzones de correo también se muestran en este árbol.
2. Busque los datos de los que desea realizar la copia de seguridad.
   Expanda los nodos del árbol o haga doble clic en los elementos de la lista de la parte derecha del árbol.
3. Seleccione los datos de los que desea realizar la copia de seguridad.
   - Si selecciona un DAG, se realizará una copia de seguridad de todas las bases de datos en clúster. Para obtener más información acerca de la copia de seguridad de los DAG, consulte "Protección de los grupos de disponibilidad de base de datos (DAG)".
   - Si selecciona un equipo que ejecute Microsoft Exchange Server, se realizará una copia de seguridad de todas las bases de datos montadas en Exchange Server que se ejecute en el equipo seleccionado.
   - Si selecciona base de datos concretas, únicamente se realizarán copias de seguridad de las bases de datos seleccionadas.
   - Si ha configurado Agent for Exchange tal y como se describe en "Copia de seguridad de buzones de correo", puede seleccionar los buzones de correo para la copia de seguridad.
4. Si se le pide, proporcione las credenciales para acceder a los datos.
5. Haga clic en **Proteger**.

Protección de los grupos de disponibilidad Alway sOn (AAG)

Descripción de soluciones de alta disponibilidad de SQL Server

La funcionalidad Clúster de conmutación por error de Windows (WSFC) permite configurar SQL Server con alta disponibilidad a través de la redundancia a nivel de la instancia (instancia de clúster de conmutación por error, FCI) o a nivel de la base de datos (grupo de disponibilidad AlwaysOn, AAG). También se pueden combinar ambos métodos.

En una instancia de clúster de conmutación por error, las bases de datos de SQL se ubican en un espacio de almacenamiento compartido. A este almacenamiento solo se puede tener acceso desde un nodo de clúster activo. Si se produce un error en el nodo activo, se genera una conmutación por error y se activa otro nodo.

En el caso de un grupo de disponibilidad, la réplica de cada base de datos reside en un nodo diferente. Si la réplica principal no está disponible, se asigna la función principal a una réplica secundaria que resida en un nodo diferente.

Por lo tanto, los clústeres ya sirven como soluciones de recuperación de desastres por sí mismos. Sin embargo, puede haber casos cuando los clústeres no pueden proporcionar protección de datos: por ejemplo, en caso de un daño en la lógica de la base de datos o cuando todo el clúster está caído. Además, las soluciones de clúster no protegen de los cambios de contenido dañinos, ya que normalmente se replican inmediatamente en todos los nodos de clúster.

Configuraciones de clúster compatibles

Este software de copia de seguridad es compatible *solo* con el grupo de disponibilidad Always On (AAG) para SQL Server 2012 o posterior. Otras configuraciones de clúster, tales como instancia del clúster de conmutación por error, creación de reflejo de la base de datos y trasvase de registros *no* son compatibles.

¿Cuántos agentes se necesitan para la copia de seguridad y recuperación de los datos del clúster?

Para una copia de seguridad y recuperación de datos correcta de un clúster, Agent for SQL debe estar instalado en cada nodo del clúster de WSFC.

Copias de seguridad de bases de datos incluidas en AAG

1. Instale Agent por SQL en cada nodo del clúster WSFC.

   Nota
   Después de instalar el agente en uno de los nodos, el software muestra el AAG y sus nodos bajo **Dispositivos** > **Microsoft SQL** > **Bases de datos**. Para instalar Agents for SQL en el resto de los nodos, seleccione el AAG, haga clic **Detalles** y, a continuación, haga clic en **Instalar el agente** junto a cada uno de los nodos.

2. Seleccione el AAG o el conjunto de bases de datos para realizar una copia de seguridad según se describe en "Seleccionar bases de datos SQL".
   Debe seleccionar el propio AAG para realizar una copia de seguridad de todas las bases de datos del AAG. Para realizar una copia de seguridad de todas las bases de datos, defina este conjunto de bases de datos en todos los nodos del AAG.

   Advertencia.
   El conjunto de bases de datos debe ser exactamente igual en todos los nodos. Si uno de los conjuntos es diferente o no se ha definido en todos los nodos, la copia de seguridad del clúster no funcionará correctamente.

3. Configure la opción de copia de seguridad «Modo de copia de seguridad de clústeres»

Recuperación de bases de datos incluidas en un AAG

1. Seleccione las bases datos que desea recuperar y, a continuación, seleccione el punto de recuperación desde el cual desea recuperar las bases de datos.

   Al seleccionar una base de datos en clúster bajo **Dispositivos** > **Microsoft SQL** > **Bases de datos** y, a continuación, haga clic en **Recuperar**, el software muestra solo los puntos de recuperación que corresponden a las veces cuando se ha realizado una copia de seguridad de la copia seleccionada de la base de datos.

   La manera más fácil para ver todos los puntos de recuperación de una base de datos en clúster es seleccionar la copia de seguridad del AAG entero en la pestaña Almacenamiento de copias de seguridad. Los nombres de copias de seguridad del AAG están basados en la plantilla siguiente `<AAG name> - <protection plan name>` y tienen un icono especial.
2. Para configurar la recuperación, siga los pasos descritos en «Recuperación de base de datos SQL», a partir del paso 5.

   El software define automáticamente un nodo de clúster en donde se recuperarán los datos. El nombre del nodo se visualizará en el campo **Recuperar a**. Puede cambiar manualmente el nodo de destino.

Importante
Microsoft SQL Server no permite que se sobrescriba una base de datos incluida en un grupo de disponibilidad Always On durante una recuperación. Debe excluir la base de datos de destino del AAG antes de la recuperación. O bien, puede recuperar la base de datos como una nueva que no pertenezca al AAG. Una vez que se haya completado la recuperación, puede restablecer la configuración original del AAG.

Protección de los grupos de disponibilidad de bases de datos (DAG)

Generalidades de clústeres de Exchange Server

La idea principal de los clústeres de Exchange es proporcionar una alta disponibilidad de la base de datos con recuperación de fallos rápida y sin pérdida de datos. Generalmente, se logra al tener una o más copias de las bases de datos o los grupos de almacenamiento en los miembros del clúster (nodos de clúster). Si el nodo de clúster que alberga la copia activa de la base de datos o la copia activa de la base de datos misma falla, el otro nodo que alberga la copia pasiva toma control automáticamente de las operaciones del nodo que falló y proporciona acceso a los servicios de Exchange con un tiempo de inactividad mínimo. Por lo tanto, los clústeres ya sirven como soluciones de recuperación de desastres por sí mismos.

Sin embargo, es posible que existan casos en donde las soluciones de clúster de recuperación de fallos no proporcionen una protección de los datos: por ejemplo, en caso de un daño en la lógica de la base de datos o cuando una base de datos en particular en un clúster no tiene copia (réplica), o cuando todo el clúster está caído. Además, las soluciones de clúster no protegen de los cambios de contenido dañinos, ya que normalmente se replican inmediatamente en todos los nodos de clúster.

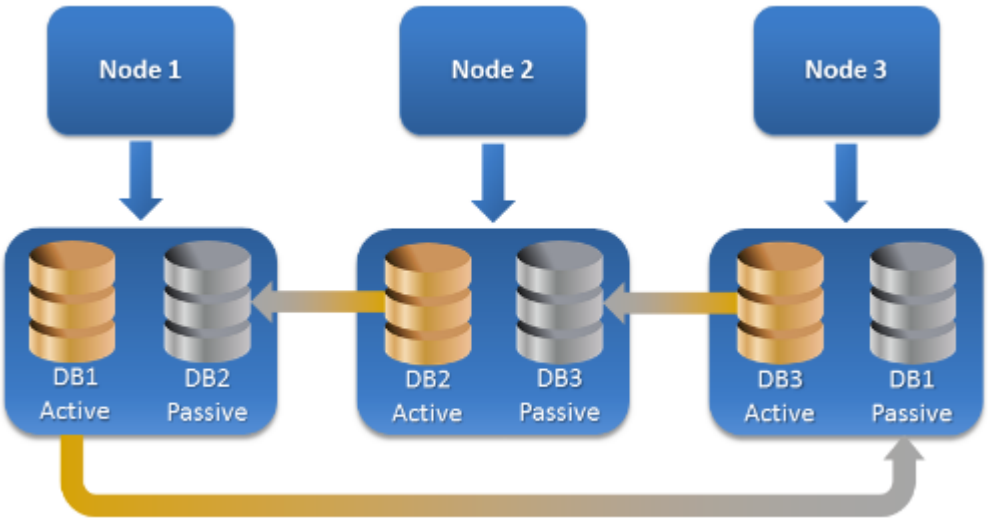
Copia de seguridad compatible con el clúster

En la copia de seguridad compatible con el clúster, solo se realiza una copia de seguridad de los datos en clúster. Si cambia la ubicación de los datos dentro del clúster (debido a un cambio o conmutación por error), el software realizará el seguimiento de todas las reubicaciones de estos datos y creará una copia de seguridad de forma segura.

Configuraciones de clúster compatibles

La copia de seguridad compatible con el clúster *solo* se admite con Grupo de disponibilidad de base de datos (DAG) en Exchange Server 2010 o versiones posteriores. Otras configuraciones de clústeres, como el clúster de copia única (SCC) y la replicación continua en clústeres (CCR) para Exchange 2007, *no* son compatibles.

DAG es un grupo de hasta 16 servidores de buzones de correo de Exchange. Cualquier nodo puede albergar una copia de la base de datos del buzón de correo de cualquier otro nodo. Cada nodo puede albergar copias de base de datos activas y pasivas. Es posible crear hasta 16 copias de cada base de datos.



¿Cuántos agentes se necesitan para la copia de seguridad y recuperación compatible con el clúster?

Para una copia de seguridad y recuperación correcta de bases de datos en clúster, Agent for Exchange debe estar instalado en cada nodo del clúster de Exchange.

Nota
Después de instalar el agente en uno de los nodos, la consola web de Cyber Protect muestra el DAG y sus nodos en **Dispositivos** > **Microsoft Exchange** > **Bases de datos**. Para instalar Agents for Exchange en el resto de los nodos, seleccione el DAG, haga clic **Detalles** y, a continuación, haga clic en **Instalar el agente** junto a cada uno de los nodos.

Copia de seguridad de los datos del clúster de Exchange

1. Al crear un plan de protección, seleccione el DAG según se describe en "Seleccionar datos de Exchange Server".
2. Configure la opción de copia de seguridad «Modo de copia de seguridad de clústeres»
3. Especifique las demás opciones de configuración del plan de protección según corresponda.

Importante
Para la copia de seguridad compatible con el clúster, asegúrese de seleccionar el propio DAG. Si selecciona nodos individuales o bases de datos dentro del DAG, solo se realizará la copia de seguridad de los elementos seleccionados y se omitirá la opción **Modo de copia de seguridad de clústeres**.

Recuperación de los datos del clúster de Exchange

1. Seleccione el punto de recuperación de la base datos que desea recuperar. No se puede seleccionar todo un clúster para la recuperación.

   Al seleccionar una copia de una base de datos en clúster en **Dispositivos** > **Microsoft Exchange** > **Bases de datos** > `<cluster name>` > `<node name>` y hacer clic en **Recuperar**, el software muestra solo los puntos de recuperación que se correspondan con las horas a las que se realizó la copia de seguridad de la copia.

   La manera más fácil para ver todos los puntos de recuperación de una base de datos en clúster es seleccionar su copia de seguridad en la pestaña Almacenamiento de copias de seguridad.
2. Siga los pasos descritos en "Recuperación de base de datos de Exchange", a partir del paso 5.

   El software define automáticamente un nodo de clúster en donde se recuperarán los datos. El nombre del nodo se visualizará en el campo **Recuperar a**. Puede cambiar manualmente el nodo de destino.

Copia de seguridad compatible con la aplicación

La copia de seguridad a nivel de disco compatible con la aplicación está disponible para equipos físicos, equipos virtuales ESXi y equipos virtuales Hyper-V.

Al realizar una copia de seguridad de un equipo que ejecute Microsoft SQL Server, Microsoft Exchange Server o Servicios de dominio de Active Directory, habilite **Copia de seguridad de aplicaciones** para dotar de mayor seguridad a los datos de estas aplicaciones.

Motivos para usar la copia de seguridad compatible con la aplicación

Al usar la copia de seguridad compatible con la aplicación, se asegura de lo siguiente:

1. Se realiza una copia de seguridad de las aplicaciones en un estado coherente y, por consiguiente, estarán disponibles inmediatamente después de la recuperación del equipo.
2. Puede recuperar las bases de datos de SQL y Exchange, los buzones de correo y los elementos de buzón de correo sin tener que recuperar todo el equipo.
3. Los registros de transacción de SQL se truncan después de crear una copia de seguridad correctamente. El truncamiento de registros de SQL se puede deshabilitar en las opciones del plan de protección. Los registros de transacción de Exchange solo se truncan en los equipos virtuales. Puede habilitar la opción de copia de seguridad completa de VSS si quiere truncar los registros de transacción de Exchange en un equipo físico.
4. Si un dominio contiene más de un controlador de dominios y desea recuperar alguno de ellos, se realizará una restauración no autorizada y no habrá reversión USN alguna después de la recuperación.

¿Qué necesito para usar la copia de seguridad compatible con la aplicación?

En un equipo físico, hay que tener instalado Agente para SQL o Agent for Exchange además de Agente para Windows.

En un equipo virtual no es necesario instalar ningún agente; se presupone que Agent para VMware (Windows) o Agent para Hyper-V hacen una copia de seguridad del equipo.

Nota
Para las máquinas virtuales de Hyper-V con Windows Server 2022, la copia de seguridad con información de aplicaciones no es compatible en el modo sin agente, es decir, cuando la copia de seguridad la realiza el Agente para Hyper-V. Para proteger las aplicaciones de Microsoft en estas máquinas, instale el Agente para Windows dentro del sistema operativo invitado.

Agente para VMware (dispositivo virtual) y Agente para VMware (Linux) pueden crear copias de seguridad compatibles con la aplicación, pero no pueden recuperar datos de aplicaciones de estas. Para recuperar datos de aplicaciones de copias de seguridad creadas por estos agentes, necesita Agente para VMware (Windows), Agent for SQL o Agent for Exchange en un equipo con acceso a la ubicación en la que se almacenan las copias de seguridad. Al configurar la recuperación de los datos de aplicaciones, seleccione el punto de recuperación en la pestaña **Almacenamiento de copias de seguridad** y, a continuación, seleccione este equipo en **Equipo desde el cual examinar**.

En "Requisitos previos" (p. 499) y "Se requieren derechos de usuario para la copia de seguridad con información de aplicaciones" (p. 508) se enumeran otros requisitos.

Se requieren derechos de usuario para la copia de seguridad con información de aplicaciones

Una copia de seguridad compatible con la aplicación contiene metadatos de aplicaciones compatibles con VSS que están presentes en el disco. Para acceder a estos metadatos, el agente

necesita una cuenta con los derechos apropiados, que se indican a continuación. Se le pedirá que especifique esta cuenta al habilitar la copia de seguridad de la aplicación.

- Para SQL Server:

  La cuenta debe ser un miembro del grupo **Operadores de copias de seguridad** o **Administradores** en el equipo y miembro de la función **administrador del sistema** en cada una de las instancias de las que va a realizar la copia de seguridad.

  Nota
  Solo se admite la autenticación de Windows.

- Para Exchange Server:

  Exchange 2007: La cuenta debe pertenecer al grupo **Administradores** del equipo y al grupo de funciones **Administradores de la organización de Exchange**.

  Exchange 2010 y posterior: La cuenta debe pertenecer al grupo **Administradores** del equipo y al grupo de funciones **Gestión de la organización**.
- Para Active Directory:

  La cuenta debe ser un administrador de dominios.

Otros requisitos para equipos virtuales

Si la aplicación se ejecuta en un equipo virtual del que Agent para VMware o Agent para Hyper-V hace una copia de seguridad, asegúrese de que el control de cuentas de usuario (UAC) está deshabilitado en el equipo. Si no desea deshabilitar el UAC, debe proporcionar las credenciales de un administrador de dominios incorporados (DOMINIO\Administrador) al habilitar la copia de seguridad de la aplicación.

Requisitos adicionales para equipos con Windows

En todas las versiones de Windows es necesario deshabilitar las directivas de Control de la cuenta de usuario (UAC) para permitir las copias de seguridad con información de aplicaciones. Si no desea deshabilitar las directivas UAC, debe proporcionar las credenciales de un administrador de dominios integrado (DOMINIO\Administrador) al configurar las copias de seguridad con información de aplicaciones.

Para deshabilitar las directivas UAC en Windows

1. En el Editor del Registro, localice la siguiente clave de registro:
   `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System`
2. Cambie el valor de **EnableLUA** a **0**.
3. Reinicie el equipo.

Copia de seguridad de casillas de correo

La copia de seguridad del buzón de correo es compatible con Microsoft Exchange Server 2010 servicio Pack 1 (SP1) o versión posterior.

La copia de seguridad de los buzones de correo está disponible si se ha registrado por lo menos un Agente for Exchange en el servidor de gestión. El agente tiene que estar instalado en un equipo que pertenezca al mismo bosque de Active Directory que Microsoft Exchange Server.

Antes de realizar la copia de seguridad de los buzones de correo electrónico, debe conectar Agent for Exchange al equipo que ejecuta el rol del servidor **Acceso de cliente** (CAS) de Microsoft Exchange Server. En Exchange 2016 y versiones posteriores, el rol CAS no está disponible como opción de instalación independiente. Se instala automáticamente como parte del rol de servidor Buzón de correo. Por lo tanto, puede conectar el agente a cualquier servidor que ejecute el **Rol de buzón de correo**.

Para conectar Agent for Exchange a CAS

1. Haga clic en **Dispositivos** > **Añadir**.
2. Haga clic en **Microsoft Exchange Server**.
3. Haga clic en **Buzones de correo de Exchange**.
   Si no hay ningún Agent for Exchange registrado en el servidor de gestión, el software le sugerirá que instale el agente. Después de la instalación, repita este procedimiento desde el paso 1.
4. [Opcional] Si hay registrados varios Agents for Exchange en el servidor de gestión, haga clic en **Agente** y cambie el agente que llevará a cabo la copia de seguridad.
5. En **Servidor de acceso de cliente**, indique el nombre de dominio completo (FQDN) del equipo donde está habilitado el rol **Acceso de cliente** de Microsoft Exchange Server.
   En Exchange 2016 y versiones posteriores, los servicios de acceso de cliente se instalan automáticamente como parte del rol de servidor Buzón de correo. Por lo tanto, puede especificar cualquier servidor que ejecute el **Rol de buzón de correo**. En adelante, en este apartado llamaremos CAS a este servidor.
6. En **Tipo de autenticación**, seleccione el tipo de autenticación utilizada por CAS. Puede seleccionar **Kerberos** (opción predeterminada) o **Básica**.
7. [Solo para una autenticación básica] Seleccione qué protocolo se debe utilizar. Puede seleccionar **HTTPS** (opción predeterminada) o **HTTP**.
8. [Solo para una autenticación básica con el protocolo HTTPS] Si CAS utiliza un certificado SSL obtenido de una entidad de certificación y desea que el software compruebe el certificado al conectarse a CAS, active la casilla de verificación **Comprobar certificado SSL**. De lo contrario, omita este paso.
9. Proporcione las credenciales de la cuenta que se utilizará para acceder a CAS. Los requisitos de esta cuenta aparecen en la sección Derechos de usuario necesarios.
10. Haga clic en **Agregar**.

Como resultado, los buzones de correo aparecen bajo **Dispositivos** > **Microsoft Exchange** > **Buzones de correo**.

Selección de los buzones de correo de Exchange Server

Seleccione los buzones de correo tal como se describe a continuación y luego especifique otros ajustes del plan de protección según corresponda.

Para seleccionar buzones de correo de Exchange

1. Haga clic en **Dispositivos** > **Microsoft Exchange**.
   El software muestra el árbol de bases de datos y buzones de correo de Exchange.
2. Haga clic en **Buzones de correo** y después seleccione los buzones de correo de los que desee realizar una copia de seguridad.
3. Haga clic en **Copia de seguridad**.

Derechos de usuario necesarios

Para acceder a estos buzones de correo, Agent for Exchange necesita una cuenta con los derechos apropiados. Se le pedirá que especifique esta cuenta al configurar varias operaciones con buzones de correo.

Si la cuenta pertenece al grupo de funciones **Gestión de la organización**, podrá acceder a cualquier buzón de correo, incluidos aquellos que se creen en el futuro.

Los derechos de usuario mínimos necesarios son los siguientes:

- La cuenta debe pertenecer a los grupos de roles **Gestión de servidores** y **Gestión de destinatarios**.
- La cuenta debe tener activada la función de gestión **ApplicationImpersonation** para todos los usuarios o grupos de usuarios a cuyos buzones de correo accederá el agente.
  Para obtener más información sobre cómo configurar la función de gestión **ApplicationImpersonation**, consulte el siguiente artículo de la Microsoft Knowledge Base: https://msdn.microsoft.com/en-us/library/office/dn722376.aspx.

Recuperación de bases de datos SQL

En esta sección se describe la recuperación desde copias de seguridad de bases de datos y desde copias de seguridad compatibles con la aplicación.

Es posible recuperar bases de datos SQL en una instancia de SQL Server si el equipo que ejecuta la instancia tiene instalado el Agente para SQL.

Si usa la autenticación de Windows, necesitará proporcionar las credenciales de una cuenta que sea miembro del grupo **Operadores de copia de seguridad** o **Administradores** en el equipo y miembro de la función **administrador del sistema** en la instancia de destino. Si usa la autenticación del Servidor SQL, necesitará proporcionar las credenciales de una cuenta que sea miembro de la función **administrador del sistema** en la instancia de destino.

También tiene la opción de recuperar las bases de datos como archivos. Esta opción puede serle útil si necesita extraer datos para minería de datos, controles u otros procesamientos con herramientas de terceros. Puede conectar los archivos de SQL database a una instancia de SQL Server, tal como se describe en "Adjuntar bases de datos SQL Server".

Si solo usa Agente para VMware (Windows), el único método de recuperación disponible será la recuperación de bases de datos como archivos. No se puede usar Agente para VMware (dispositivo virtual) para recuperar bases de datos.

Las bases de datos del sistema se recuperan básicamente de la misma manera que las bases de datos de usuarios. Las peculiaridades de la recuperación de las bases de datos del sistema se detallan en "Recuperación de bases de datos del sistema".

Para recuperar bases de datos de SQL a una instancia de SQL Server

1. Realice uno de los siguientes procedimientos:
   - Si recupera desde una copia de seguridad compatible con la aplicación: en **Dispositivos**, seleccione el equipo que contenía originalmente los datos que desea recuperar.
   - Si recupera desde una copia de seguridad compatible con la aplicación, haga clic en **Dispositivos** > **Microsoft SQL** y seleccione las bases de datos que desea recuperar.
2. Haga clic en **Recuperación**.
3. Seleccione un punto de recuperación. Tenga en cuenta que los puntos de recuperación se filtran por ubicación.

   Si el equipo no está conectado a Internet, no se muestran los puntos de recuperación. Realice uno de los siguientes procedimientos:
   - [Solo si recupera desde una copia de seguridad compatible con la aplicación] Si la copia de seguridad se encuentra en el almacenamiento compartido o en la cloud (es decir, otros agentes pueden acceder a ella), haga clic en **Seleccionar equipo**, seleccione un equipo conectado que tenga instalado el Agente para SQL y seleccione un punto de recuperación.
   - Seleccione un punto de recuperación en la pestaña de almacenamiento de copia de seguridad.

   El equipo elegido para examinar en cualquiera de las acciones anteriores se convierte en el equipo de destino para la recuperación de las bases de datos SQL.
4. Realice uno de los siguientes procedimientos:
   - Si recupera desde una copia de seguridad compatible con la aplicación, haga clic en **Recuperar** > **Base de datos SQL**, seleccione las bases de datos que desea recuperar y, a continuación, haga clic en **Recuperar**.
   - Si recupera desde una copia de seguridad de base de datos, haga clic en **Recuperar** > **Bases de datos en una instancia**.
5. De manera predeterminada, las bases de datos se recuperan en las originales. Si no existe la base de datos original, se volverá a crear. Puede seleccionar otra instancia de SQL Server (ejecutándose en el mismo equipo) donde recuperar las bases de datos.

   Para recuperar una base de datos como una diferente en la misma instancia:

a. Haga clic en el nombre de la base de datos.

b. Seleccione **Nueva base de datos** en **Recuperar en**.

c. Especifique el nuevo nombre de la base de datos.

d. Especifique la nueva ruta de la base de datos y la ruta de acceso. La carpeta que especifique no debe contener la base de datos original ni los archivos de registro.

6. [Opcional] [No disponible para una base de datos recuperada a su instancia original como nueva base de datos] Para cambiar el estado de la base de datos después de la recuperación, haga clic en el nombre de la base de datos y elija uno de los siguientes estados:
   - **Listo para su uso (RESTAURAR CON RECUPERACIÓN)** (opción predeterminada)

     Una vez que se complete la recuperación, la base de datos estará lista para su uso. Los usuarios tendrán el acceso total. El software revertirá todas las transacciones no confirmadas de la base de datos recuperada que se guardaron en los registros de las transacciones. No se podrán recuperar los registros de transacciones adicionales desde las copias de seguridad nativas de Microsoft SQL.
   - **No operativo (RESTAURAR SIN RECUPERACIÓN)**

     Una vez que se haya completado la recuperación, la base de datos dejará de ser operativa. Los usuarios no podrán tener acceso a ella. El software conservará todas las transacciones no confirmadas de la base de datos recuperada. No se podrán recuperar los registros de transacciones adicionales desde las copias de seguridad nativas de Microsoft SQL y así alcanzar el punto de recuperación necesario.
   - **Solo lectura (RESTAURAR CON ESPERA)**

     Una vez que se completa la recuperación, los usuarios tendrán un acceso de solo lectura a la base de datos. El software deshará todas las transacciones no confirmadas. Sin embargo, guardará las acciones deshechas en un archivo temporal en espera, de manera que se puedan revertir los efectos de la recuperación.

     Este valor se utiliza principalmente para detectar el momento específico en que se produjo un error en SQL Server.
7. Haga clic en **Iniciar recuperación**.

El proceso de recuperación se muestra en la pestaña **Actividades**.

Para recuperar bases de datos SQL como archivos

1. Realice uno de los siguientes procedimientos:
   - Si recupera desde una copia de seguridad compatible con la aplicación: en **Dispositivos**, seleccione el equipo que contenía originalmente los datos que desea recuperar.
   - Si recupera desde una copia de seguridad compatible con la aplicación, haga clic en **Dispositivos** > **Microsoft SQL** y seleccione las bases de datos que desea recuperar.
2. Haga clic en **Recuperación**.
3. Seleccione un punto de recuperación. Tenga en cuenta que los puntos de recuperación se filtran por ubicación.

   Si el equipo no está conectado a Internet, no se muestran los puntos de recuperación. Realice uno de los siguientes procedimientos:

- [Solo si recupera desde una copia de seguridad compatible con la aplicación] Si la copia de seguridad se encuentra en el almacenamiento compartido o en la cloud (es decir, otros agentes pueden acceder a ella), haga clic en **Seleccionar equipo**, seleccione un equipo conectado que tenga instalado Agent for SQL o Agent for VMware y, a continuación, seleccione un punto de recuperación.
- Seleccione un punto de recuperación en la pestaña de almacenamiento de copia de seguridad.

El equipo elegido para examinar en cualquiera de las acciones anteriores se convierte en el equipo de destino para la recuperación de las bases de datos SQL.

4. Realice uno de los siguientes procedimientos:
   - Si recupera desde una copia de seguridad compatible con la aplicación, haga clic en **Recuperar** > **Bases de datos SQL**, seleccione las bases de datos que desea recuperar y, a continuación, haga clic en **Recuperar como archivos**.
   - Si recupera desde una copia de seguridad de base de datos, haga clic en **Recuperar** > **Bases de datos como archivos**.
5. Haga clic en **Examinar** y, a continuación, seleccione una carpeta local o de red en que guardar los archivos.
6. Haga clic en **Iniciar recuperación**.

El proceso de recuperación se muestra en la pestaña **Actividades**.

Recuperación de bases de datos del sistema

Todas las bases de datos del sistema de una instancia se recuperan a la vez. Cuando se recuperan bases de datos del sistema, el software reinicia automáticamente la instancia de destino en el modo de usuario único. Una vez que se completa la recuperación, el software reinicia la instancia y recupera las demás bases de datos (si las hubiera).

Otros aspectos que debe tener en cuenta cuando se recuperan bases de datos del sistema:

- Las bases de datos del sistema únicamente se pueden recuperar en una instancia de la misma versión que la instancia original.
- Las bases de datos del sistema siempre se recuperan en el estado «listo para su uso».

Recuperación de la base de datos maestra

Las bases de datos del sistema incluyen la base de datos **maestra**. La base de datos **maestra** registra información sobre todas las bases de datos de la instancia. Por lo tanto, la base de datos **maestra** de una copia de seguridad contiene información sobre las bases de datos, la cual ya existía en la instancia al momento de realizar la copia de seguridad. Es posible que después de recuperar la base de datos **maestra** deba realizar lo siguiente:

- Las bases de datos que aparecieron en la instancia después de realizar la copia de seguridad no se pueden visualizar en la instancia. Para recuperar esas bases de datos, adjúntelas a la instancia manualmente usando SQL Server Management Studio.

- Las bases de datos que se eliminaron en la instancia después de realizar la copia de seguridad se muestran sin conexión en la instancia. Elimine estas bases de datos mediante SQL Server Management Studio.

Adjuntar bases de datos de SQL Server

Esta sección describe cómo adjuntar una base de datos en SQL Server utilizando SQL Server Management Studio. Solo se puede adjuntar una base de datos por vez.

Adjuntar una base de datos requiere uno de los siguientes permisos: **CREAR BASE DE DATOS**, **CREAR CUALQUIER BASE DE DATOS** o **MODIFICAR CUALQUIER BASE DE DATOS**. Generalmente, estos permisos se conceden al rol de la instancia **sysadmin**.

Para adjuntar una base de datos

1. Ejecute Microsoft SQL Server Management Studio.
2. Conéctese a la instancia de SQL Server necesaria y después expanda la instancia.
3. Haga clic con el botón derecho en **Bases de datos** y luego en **Adjuntar**.
4. Haga clic en **Agregar**.
5. En el cuadro de diálogo **Localizar archivos de la base de datos**, busque y seleccione el archivo .mdf de la base de datos.
6. En la sección **Detalles de la base de datos**, asegúrese de que se encuentre el resto de los archivos de la base de datos (archivos .ndf y .ldf).

   Detalles. Quizás los archivos de la base de datos de SQL Server no se puedan encontrar automáticamente si:
   - No están en la ubicación predeterminada o no están en la misma carpeta que el archivo de la base de datos principal (.mdf). Solución: Especifique manualmente la ruta hasta los archivos necesarios en la columna **Ruta actual del archivo**.
   - Recuperó un conjunto incompleto de archivos que forman la base de datos. Solución: Recupere los archivos de la base de datos de SQL Server faltantes desde la copia de seguridad.
7. Cuando se hayan encontrado todos los archivos, haga clic en **Aceptar**.

Recuperación de bases de datos de Exchange

En esta sección se describe la recuperación desde copias de seguridad de bases de datos y desde copias de seguridad compatibles con la aplicación.

Puede recuperar datos de Exchange Server en un servidor de Exchange activo. Puede ser el servidor de Exchange original o un servidor de Exchange de la misma versión que se ejecute en el equipo que tenga el mismo nombre de dominio completo (FQDN). Agent for Exchange debe estar instalado en el equipo de destino.

La siguiente tabla resume los datos de Exchange Server que puede seleccionar para recuperar y los permisos de usuario mínimos que se requieren para recuperar los datos.

Versión de Exchange	Elementos de los datos	Permisos de usuario
2007	Grupos de almacenamiento	Asociación en el grupo de funciones **Administradores de organización de Exchange**.
2010/2013/2016/2019	Bases de datos	Pertenencia al grupo de funciones **Administración de servidores**.

También tiene la opción de recuperar las bases de datos (grupos de almacenamiento) como archivos. Los archivos de bases de datos, junto con los archivos de registro de transacción, se extraerán de la copia de seguridad a la carpeta que especifique. Esta opción puede serle útil si necesita extraer información para un control o procesos futuros con herramientas adicionales, o cuando la recuperación falle por alguna razón y necesite una solución para montar las bases de datos manualmente.

Si solo usa Agente para VMware (Windows), el único método de recuperación disponible será la recuperación de bases de datos como archivos. No se puede usar Agente para VMware (dispositivo virtual) para recuperar bases de datos.

Nos referiremos tanto a las bases de datos como a los grupos de almacenamiento como "bases de datos" en estos procedimientos.

Para recuperar bases de datos de Exchange a un servidor activo de Exchange Server

1. Realice uno de los siguientes procedimientos:
   - Si recupera desde una copia de seguridad compatible con la aplicación: en **Dispositivos**, seleccione el equipo que contenía originalmente los datos que desea recuperar.
   - Si recupera desde una copia de seguridad compatible con la aplicación, haga clic en **Dispositivos** > **Microsoft Exchange** > **Bases de datos** y, a continuación, seleccione las bases de datos que desea recuperar.
2. Haga clic en **Recuperación**.
3. Seleccione un punto de recuperación. Tenga en cuenta que los puntos de recuperación se filtran por ubicación.

   Si el equipo no está conectado a Internet, no se muestran los puntos de recuperación. Realice uno de los siguientes procedimientos:
   - [Solo si recupera desde una copia de seguridad compatible con la aplicación] Si la copia de seguridad se encuentra en el almacenamiento compartido o en la cloud (es decir, otros agentes pueden acceder a ella), haga clic en **Seleccionar equipo**, seleccione un equipo conectado que tenga instalado Agent for Exchange y seleccione un punto de recuperación.
   - Seleccione un punto de recuperación en la pestaña de almacenamiento de copia de seguridad.

   El equipo elegido para examinar en cualquiera de las acciones anteriores se convierte en el equipo de destino para la recuperación de datos de Exchange.

4. Realice uno de los siguientes procedimientos:
   - Si recupera desde una copia de seguridad compatible con la aplicación, haga clic en **Recuperar** > **Bases de datos de Exchange**, seleccione las bases de datos que desea recuperar y, a continuación, haga clic en **Recuperar**.
   - Si recupera desde una copia de seguridad de base de datos, haga clic en **Recuperar** > **Bases de datos a un servidor de Exchange**.
5. De manera predeterminada, las bases de datos se recuperan en las originales. Si no existe la base de datos original, se volverá a crear.

   Para recuperar una base de datos como una diferente:
   a. Haga clic en el nombre de la base de datos.
   b. Seleccione **Nueva base de datos** en **Recuperar en**.
   c. Especifique el nuevo nombre de la base de datos.
   d. Especifique la nueva ruta de la base de datos y la ruta de acceso. La carpeta que especifique no debe contener la base de datos original ni los archivos de registro.
6. Haga clic en **Iniciar recuperación**.

El proceso de recuperación se muestra en la pestaña **Actividades**.

Para recuperar los bases de datos como archivos de Exchange

1. Realice uno de los siguientes procedimientos:
   - Si recupera desde una copia de seguridad compatible con la aplicación: en **Dispositivos**, seleccione el equipo que contenía originalmente los datos que desea recuperar.
   - Si recupera desde una copia de seguridad compatible con la aplicación, haga clic en **Dispositivos** > **Microsoft Exchange** > **Bases de datos** y, a continuación, seleccione las bases de datos que desea recuperar.
2. Haga clic en **Recuperación**.
3. Seleccione un punto de recuperación. Tenga en cuenta que los puntos de recuperación se filtran por ubicación.

   Si el equipo no está conectado a Internet, no se muestran los puntos de recuperación. Realice uno de los siguientes procedimientos:
   - [Solo si recupera desde una copia de seguridad compatible con la aplicación] Si la copia de seguridad se encuentra en el almacenamiento compartido o en la cloud (es decir, otros agentes pueden acceder a ella), haga clic en **Seleccionar equipo**, seleccione un equipo conectado que tenga instalado Agent for Exchange o Agent for VMware, y seleccione un punto de recuperación.
   - Seleccione un punto de recuperación en la pestaña de almacenamiento de copia de seguridad.

   El equipo elegido para examinar en cualquiera de las acciones anteriores se convierte en el equipo de destino para la recuperación de datos de Exchange.
4. Realice uno de los siguientes procedimientos:
   - Si recupera desde una copia de seguridad compatible con la aplicación, haga clic en **Recuperar** > **Bases de datos de Exchange**, seleccione las bases de datos que desea

recuperar y, a continuación, haga clic en **Recuperar como archivos**.

- Si recupera desde una copia de seguridad de base de datos, haga clic en **Recuperar** > **Bases de datos como archivos**.

5. Haga clic en **Examinar** y, a continuación, seleccione una carpeta local o de red en que guardar los archivos.
6. Haga clic en **Iniciar recuperación**.

El proceso de recuperación se muestra en la pestaña **Actividades**.

Montaje de bases de datos de Exchange Server

Después de recuperar los archivos de bases de datos, puede conectar las bases de datos al montarlas. El montaje se realiza por medio de la consola de gestión de Exchange, Exchange System Manager o Exchange Management Shell.

Las bases de datos recuperadas se encontrarán en el estado de Cierre con errores. Una base de datos que se encuentra en el estado de Cierre con errores puede montarse por medio del sistema si se recupera en su ubicación original (es decir, la información sobre la base de datos original está presente en Active Directory). Cuando se recupera una base de datos en una ubicación alternativa, (como una base de datos nueva o como la base de datos de recuperación), la base de datos no se puede montar hasta que se encuentre en el estado de Cierre correcto; para ello se utiliza el comando `Eseutil /r <Enn>`. `<Enn>` especifica el prefijo del archivo de registro para la base de datos (o el grupo de almacenamiento que contiene la base de datos) a la cual debe aplicar los archivos de registro de transacciones.

La cuenta que usa para adjuntar una base de datos debe tener asignado un rol de Administrador de Exchange Server y un grupo de administradores locales para el servidor de destino.

Para obtener información sobre cómo montar las bases de datos, consulte los siguientes artículos:

- Exchange 2010 o versiones posteriores: http://technet.microsoft.com/en-us/library/aa998871.aspx
- Exchange 2007: http://technet.microsoft.com/es-es/library/aa998871(v=EXCHG.80).aspx

Recuperación de elementos de buzón de correo y de buzones de correo de Exchange

En esta sección se describe cómo recuperar elementos de buzón de correo y buzones de correo de Exchange a partir de copias de seguridad de bases de datos, copias de seguridad compatibles con la aplicación y copias de seguridad de buzones de correo. Los buzones de correo o elementos de los buzones de correo pueden recuperarse a un servidor activo de Exchange Server o a Microsoft 365.

Se pueden recuperar los siguientes elementos:

- Buzones de correo (salvo los buzones de correo de archivo)
- Carpetas públicas

Nota
Disponible solo desde copias de seguridad de bases de datos. Consulte "Seleccionar datos de Exchange Server" (p. 502)

- Elementos de la carpeta pública
- Carpetas de correo electrónico
- Mensajes de correo electrónico
- Eventos del calendario
- Tareas
- Contactos
- Entradas del diario
- Notas

Puede usar la búsqueda para localizar los elementos.

Recuperación a Exchange Server

La recuperación granular se puede realizar en Microsoft Exchange Server 2010 Service Pack 1 (SP1) y versiones posteriores. La copia de seguridad de origen puede contener bases de datos o buzones de correo de cualquier versión compatible de Exchange.

La recuperación granular la pueden realizar Agent for Exchange o Agente para VMware (Windows). La aplicación Exchange Server de destino y el equipo donde se ejecute el agente deben pertenecer al mismo bosque de Active Directory.

Cuando se recupera un buzón de correo sobre un buzón de correo existente, los elementos anteriores que tengan los mismos ID se sobrescriben.

Al recuperar elementos de buzón de correo no se sobrescribe nada. En su lugar, en la carpeta de destino se reproduce la ruta completa al elemento del buzón de correo.

Requisitos de las cuentas de usuario

Un buzón de correo que se recupera desde una copia de seguridad debe tener una cuenta de usuario asociada en Active Directory.

Los buzones de correo del usuario y su contenido solo pueden recuperarse si las cuentas de usuario asociadas están *habilitadas*. Los buzones de correo compartidos, de sala y equipo pueden recuperarse solo si sus cuentas de usuario asociadas están *deshabilitadas*.

Un buzón de correo que no cumpla con las condiciones anteriores se omitirá durante la recuperación.

Si se omiten algunos buzones de correo, la recuperación finalizará correctamente con advertencias. Si se omiten todos los buzones de correo, la recuperación fallará.

Recuperar a Microsoft 365

La recuperación puede realizarse desde copias de seguridad de Microsoft Exchange Server 2010 y versiones posteriores.

Cuando se recupera un buzón de correo a un buzón de Microsoft 365 existente, los elementos anteriores se mantienen intactos y los elementos recuperados se colocan junto a ellos.

Si recupera un único buzón de correo, deberá seleccionar el buzón de Microsoft 365 de destino. Si recupera varios buzones de correo en una única operación de recuperación, el software intentará recuperar cada buzón de correo al buzón del usuario que tenga el mismo nombre. Si no se encuentra un usuario con estas características, se omite el buzón de correo. Si se omiten algunos buzones de correo, la recuperación finalizará correctamente con advertencias. Si se omiten todos los buzones de correo, la recuperación fallará.

Para obtener más información sobre la recuperación Microsoft 365, consulte "Protección de buzones de correo de Microsoft 365" (p. 527).

Recuperación de buzones de correo

Para recuperar buzones de correo a partir de una copia de seguridad compatible con la aplicación o una copia de seguridad de base de datos

1. [Solo al recuperar desde una copia de seguridad de base de datos a Microsoft 365] Si el Agente para Office 365 no está instalado en la máquina que ejecuta Exchange Server y de la que se ha realizado la copia de seguridad, haga una de las acciones siguientes:
   - Si no tiene el Agente para Office 365 en su organización, instale el Agente para Office 365 en el equipo del que se ha realizado la copia de seguridad (u otro equipo con la misma versión de Microsoft Exchange Server).
   - Si ya tiene el Agente para Office 365 en su organización, copie las bibliotecas desde el equipo del que se ha realizado la copia de seguridad (o desde otro equipo con la misma versión de Microsoft Exchange Server) al equipo con el Agente para Office 365, como se describe en "Copia de bibliotecas de Microsoft Exchange".
2. Realice uno de los siguientes procedimientos:
   - Si recupera desde una copia de seguridad compatible con la aplicación: en **Dispositivos**, seleccione el equipo que contenía originalmente los datos que desea recuperar.
   - Si recupera desde una copia de seguridad compatible con la aplicación, haga clic en **Dispositivos** > **Microsoft Exchange** > **Bases de datos** y, a continuación, seleccione la base de datos que contenía originalmente los datos que desea recuperar.
3. Haga clic en **Recuperación**.
4. Seleccione un punto de recuperación. Tenga en cuenta que los puntos de recuperación se filtran por ubicación.

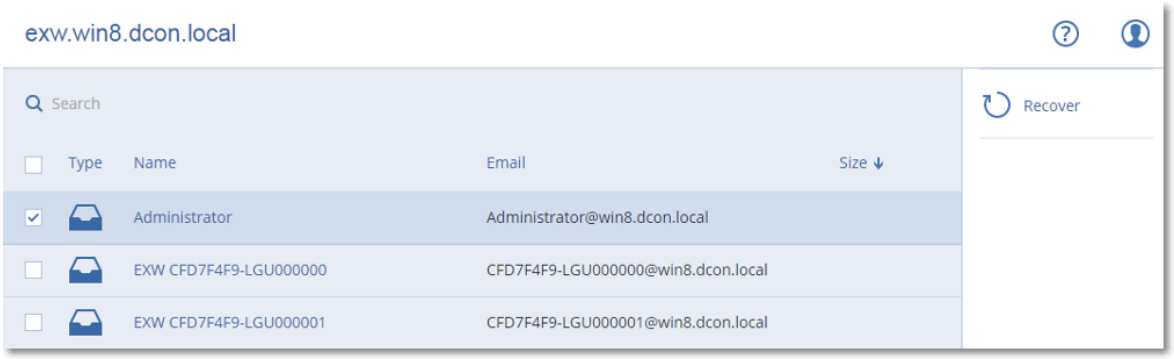
Si el equipo no está conectado a Internet, no se muestran los puntos de recuperación. Use otros métodos de recuperación:

- [Solo si recupera desde una copia de seguridad compatible con la aplicación] Si la copia de seguridad se encuentra en el almacenamiento compartido o en la cloud (es decir, otros agentes pueden acceder a ella), haga clic en **Seleccionar equipo**, seleccione un equipo conectado que tenga instalado Agent for Exchange o Agent for VMware, y seleccione un punto de recuperación.
- Seleccione un punto de recuperación en la pestaña de almacenamiento de copia de seguridad.

El equipo elegido para examinar en cualquiera de las acciones anteriores realizará la recuperación en lugar del equipo original que está desconectado.

5. Haga clic en **Recuperar** > **Buzones de correo de Exchange**.
6. Seleccione los buzones de correo que desea recuperar.

   Puede buscar los buzones de correo por el nombre. No se pueden usar caracteres comodín.



7. Haga clic en **Recuperar**.
8. [Solo al recuperar a Microsoft 365]:
   a. En **Recuperar a**, seleccione **Microsoft Office 365**.
   b. [Si solo ha seleccionado un buzón de correo en el paso 6] En **Buzón de correo de destino**, especifique el buzón de correo de destino.
   c. Haga clic en **Iniciar recuperación**.

   No se requieren más pasos para este procedimiento.
9. Haga clic en **Equipo de destino con Microsoft Exchange Server** para seleccionar o cambiar el equipo de destino. Este paso permite recuperar en un equipo que no esté ejecutando Agent for Exchange.

   Especifique el nombre de dominio completo (FQDN) de un equipo en el que esté habilitado el rol **Acceso de cliente** (en Microsoft Exchange Server 2010/2013) o el **rol Buzón de correo** (en Microsoft Exchange Server 2016 o versiones posteriores). El equipo debe pertenecer al mismo bosque de Active Directory que el equipo que realiza la recuperación.

   Si se le pide, proporcione las credenciales de la cuenta que se utilizará para acceder al equipo. Los requisitos de esta cuenta aparecen en "Derechos de usuario necesarios" (p. 511).
10. [Opcional] Haga clic en **Base de datos para volver a crear buzones de correo faltantes** para cambiar la base de datos seleccionada automáticamente.

11. Haga clic en **Iniciar recuperación**.

El proceso de recuperación se muestra en la pestaña **Actividades**.

Para recuperar un buzón de correo desde una copia de seguridad de buzón de correo

1. Haga clic en **Dispositivos** > **Microsoft Exchange** >**Buzones de correo**.
2. Seleccione el buzón de correo que desea recuperar y, a continuación, haga clic en **Recuperar**.

   Puede buscar los buzones de correo por el nombre. No se pueden usar caracteres comodín.

   Si el buzón de correo se ha eliminado, selecciónelo en la pestaña Almacenamiento de copias de seguridad y, a continuación, haga clic en **Mostrar copias de seguridad**.
3. Seleccione un punto de recuperación. Tenga en cuenta que los puntos de recuperación se filtran por ubicación.
4. Haga clic en **Recuperar** > **Buzón de correo**.
5. Siga los pasos 8 a 11 del procedimiento anterior.

Recuperación de elementos de buzón de correo

Para recuperar elementos de buzones de correo a partir de una copia de seguridad compatible con la aplicación o una copia de seguridad de base de datos

1. [Solo al recuperar desde una copia de seguridad de base de datos a Microsoft 365] Si el Agente para Office 365 no está instalado en la máquina que ejecuta Exchange Server y de la que se ha realizado la copia de seguridad, haga una de las acciones siguientes:
   - Si no tiene el Agente para Office 365 en su organización, instale el Agente para Office 365 en el equipo del que se ha realizado la copia de seguridad (u otro equipo con la misma versión de Microsoft Exchange Server).
   - Si ya tiene el Agente para Office 365 en su organización, copie las bibliotecas desde el equipo del que se ha realizado la copia de seguridad (o desde otro equipo con la misma versión de Microsoft Exchange Server) al equipo con el Agente para Office 365, como se describe en "Copia de bibliotecas de Microsoft Exchange".
2. Realice uno de los siguientes procedimientos:
   - Si recupera desde una copia de seguridad compatible con la aplicación: en **Dispositivos**, seleccione el equipo que contenía originalmente los datos que desea recuperar.
   - Si recupera desde una copia de seguridad compatible con la aplicación, haga clic en **Dispositivos** > **Microsoft Exchange** > **Bases de datos** y, a continuación, seleccione la base de datos que contenía originalmente los datos que desea recuperar.
3. Haga clic en **Recuperación**.
4. Seleccione un punto de recuperación. Tenga en cuenta que los puntos de recuperación se filtran por ubicación.

   Si el equipo no está conectado a Internet, no se muestran los puntos de recuperación. Use otros métodos de recuperación:
   - [Solo si recupera desde una copia de seguridad compatible con la aplicación] Si la copia de seguridad se encuentra en el almacenamiento compartido o en la cloud (es decir, otros

agentes pueden acceder a ella), haga clic en **Seleccionar equipo**, seleccione un equipo conectado que tenga instalado Agent for Exchange o Agent for VMware, y seleccione un punto de recuperación.

- Seleccione un punto de recuperación en la pestaña de almacenamiento de copia de seguridad.

El equipo elegido para examinar en cualquiera de las acciones anteriores realizará la recuperación en lugar del equipo original que está desconectado.

5. Haga clic en **Recuperar** > **Buzones de correo de Exchange**.
6. Haga clic en el buzón de correo que contenía originalmente los elementos que desea recuperar.
7. Seleccione los elementos que desea recuperar.

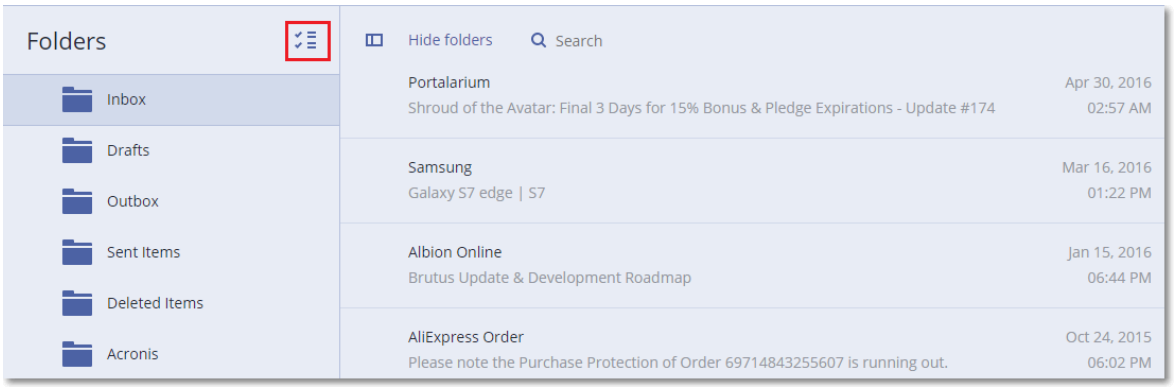
   Tiene a su disposición las siguientes opciones de búsqueda. No se pueden usar caracteres comodín.

   - Para los mensajes de correo electrónico: búsqueda por asunto, remitente, destinatario y fecha.
   - Para los eventos: búsqueda por título y fecha.
   - Para las tareas: búsqueda por asunto y fecha.
   - Para los contactos: búsqueda por nombre, dirección de correo electrónico y número de teléfono.

   Cuando se selecciona un mensaje de correo electrónico, puede hacer clic en **Mostrar contenido** para ver el contenido, incluidos los documentos adjuntos.

   Nota
   Haga clic en el nombre de un archivo adjunto para descargarlo.

   Para poder seleccionar carpetas, haga clic en el icono de recuperar carpetas.



8. Haga clic en **Recuperar**.
9. Para recuperar a Microsoft 365, seleccione **Microsoft Office 365** en **Recuperar a**.

   Para recuperar a un Exchange Server, mantenga el valor predeterminado de **Microsoft Exchange** en **Recuperar a**.
10. [Solo al recuperar a Exchange Server] Haga clic en **Equipo de destino con Microsoft Exchange Server** para seleccionar o cambiar el equipo de destino. Este paso permite recuperar en un

equipo que no esté ejecutando Agent for Exchange.

Especifique el nombre de dominio completo (FQDN) de un equipo en el que esté habilitado el rol **Acceso de cliente** (en Microsoft Exchange Server 2010/2013) o el **rol Buzón de correo** (en Microsoft Exchange Server 2016 o versiones posteriores). El equipo debe pertenecer al mismo bosque de Active Directory que el equipo que realiza la recuperación.

Si se le pide, proporcione las credenciales de la cuenta que se utilizará para acceder al equipo. Los requisitos de esta cuenta aparecen en "Derechos de usuario necesarios" (p. 511).

11. En **Buzón de correo de destino** puede consultar, cambiar o especificar el buzón de correo de destino.

    De manera predeterminada, se selecciona el buzón de correo original. Si este buzón de correo no existe o se selecciona un equipo de destino que no es el original, debe indicar el buzón de correo de destino.
12. [Solo al recuperar mensajes de correo electrónico] En **Carpeta de destino** puede consultar o cambiar la carpeta de destino en el buzón de correo de destino. De manera predeterminada, se selecciona la carpeta **Elementos recuperados**. Debido a las limitaciones de Microsoft Exchange, los eventos, las tareas, las notas y los contactos se restauran en su ubicación de origen independientemente de que se haya indicado cualquier otra **carpeta de destino**.
13. Haga clic en **Iniciar recuperación**.

El proceso de recuperación se muestra en la pestaña **Actividades**.

Para recuperar un elemento del buzón de correo de una copia de seguridad de buzón de correo

1. Haga clic en **Dispositivos** > **Microsoft Exchange** >**Buzones de correo**.
2. Seleccione el buzón de correo que contenía originalmente los elementos que desea recuperar y, a continuación, haga clic en **Recuperar**.

   Puede buscar los buzones de correo por el nombre. No se pueden usar caracteres comodín.

   Si el buzón de correo se ha eliminado, selecciónelo en la pestaña Almacenamiento de copias de seguridad y, a continuación, haga clic en **Mostrar copias de seguridad**.
3. Seleccione un punto de recuperación. Tenga en cuenta que los puntos de recuperación se filtran por ubicación.
4. Haga clic en **Recuperar** > **Mensajes de correo electrónico**.
5. Seleccione los elementos que desea recuperar.

   Tiene a su disposición las siguientes opciones de búsqueda. No se pueden usar caracteres comodín.

   - Para los mensajes de correo electrónico: búsqueda por asunto, remitente, destinatario y fecha.
   - Para los eventos: búsqueda por título y fecha.
   - Para las tareas: búsqueda por asunto y fecha.
   - Para los contactos: búsqueda por nombre, dirección de correo electrónico y número de teléfono.

   Cuando se selecciona un mensaje de correo electrónico, puede hacer clic en **Mostrar contenido** para ver el contenido, incluidos los documentos adjuntos.

Nota
Haga clic en el nombre de un archivo adjunto para descargarlo.

Cuando se selecciona un mensaje de correo electrónico, puede hacer clic en **Enviar como correo electrónico** para enviar el mensaje a una dirección de correo electrónico. El mensaje se envía desde el correo electrónico de su cuenta de administrador.

Para poder seleccionar carpetas, haga clic en el icono de recuperar carpetas: 

6. Haga clic en **Recuperar**.
7. Siga los pasos 9 a 13 del procedimiento anterior.

Copia de bibliotecas de Microsoft Exchange Server

Al recuperar los buzones de correo de Exchange o los elementos de buzón de correo en Microsoft 365, es posible que necesite copiar las bibliotecas siguientes desde la máquina de la que se ha realizado la copia de seguridad (o desde otra máquina con la misma versión de Microsoft Exchange Server) a la máquina con el Agente para Office 365.

Copie los archivos siguientes, en función de la versión de Microsoft Exchange Server de la que se ha realizado la copia de seguridad.

Versión de Microsoft Exchange Server	Bibliotecas	Ubicación predeterminada
Microsoft Exchange Server 2010	ese.dll esebcli2.dll store.exe	%ProgramFiles%\Microsoft\Exchange Server\V14\bin
Microsoft Exchange Server 2013	ese.dll	%ProgramFiles%\Microsoft\Exchange Server\V15\bin
	msvcr110.dll	%WINDIR%\system32
Microsoft Exchange Server 2016, 2019	ese.dll	%ProgramFiles%\Microsoft\Exchange Server\V15\bin
	msvcr110.dll msvcp110.dll	%WINDIR%\system32

Las bibliotecas deben ubicarse en la carpeta **%ProgramData%\Acronis\ese**. Si esta carpeta no existe, créela manualmente.

Cambio de las credenciales de acceso de SQL Server o Exchange Server

Puede cambiar las credenciales de acceso de SQL Server o Exchange Server sin tener que volver a instalar el agente.

Para cambiar las credenciales de acceso de SQL Server o Exchange Server

1. Haga clic en **Dispositivos** y, a continuación, en **Microsoft SQL** o **Microsoft Exchange**.
2. Seleccione el Grupo de disponibilidad de Always On, el Grupo de disponibilidad de base de datos, la instancia de SQL Server o el servidor de Exchange Server cuyas credenciales de acceso desee cambiar.
3. Haga clic en **Especificar credenciales**.
4. Especifique las nuevas credenciales de acceso y, a continuación, haga clic en **Aceptar**.

Para cambiar las credenciales de acceso de Exchange Server para la copia de seguridad de buzón de correo

1. Haga clic en **Dispositivos** > **Microsoft Exchange** y expanda los **Buzones de correo**.
2. Seleccione el Exchange Server cuyas credenciales de acceso desee cambiar.
3. Haga clic en **Configuración**.
4. En **Cuenta de administrador de Exchange**, especifique las nuevas credenciales de acceso y, a continuación, haga clic en **Guardar**.

Protección de buzones de correo de Microsoft 365

Importante
Importante Esta sección es válida para las implementaciones locales de Acronis Cyber Protect. Si utiliza una implementación de nube, consulte https://www.acronis.com/support/documentation/CyberProtectionService/#protecting-microsoft-365-data.html.

Para obtener más información acerca de las opciones de licencia, consulte Acronis Cyber Protect para licencias de Microsoft 365.

Motivos por los que hacer una copia de seguridad de los buzones de correo de Microsoft 365

Si bien Microsoft 365 es un servicio en la nube, las copias de seguridad periódicas le proporcionan una capa de protección adicional ante errores de los usuarios y acciones malintencionadas. Puede recuperar los elementos eliminados desde una copia de seguridad incluso después de que el periodo de retención de Microsoft 365 haya caducado. Asimismo, puede conservar una copia local de los buzones de correo de Microsoft 365 si así lo requiere un cumplimiento normativo.

Recuperación

Los siguientes elementos pueden recuperarse de la copia de seguridad de buzones de correo:

- Buzones de correo
- Carpetas de correo electrónico
- Mensajes de correo electrónico
- Eventos del calendario
- Tareas
- Contactos
- Entradas del diario
- Notas

Puede usar la búsqueda para localizar los elementos.

La recuperación puede realizarse a Microsoft 365 o a un servidor activo de Exchange Server.

Cuando se recupera un buzón de correo sobre un buzón de correo de Microsoft 365 existente, los elementos anteriores que tengan los mismos ID se sobrescriben. Cuando se recupera un buzón de correo a un buzón de Exchange Server existente, los elementos anteriores se mantendrán intactos. Los elementos recuperados se colocan junto a ellos.

Al recuperar elementos de buzón de correo no se sobrescribe nada. En su lugar, en la carpeta de destino se reproduce la ruta completa al elemento del buzón de correo.

Limitaciones

- Aplicar un plan de protección a más de 500 buzones de correo puede provocar una degradación del rendimiento de la copia de seguridad. Para proteger un gran número de buzones de correo, cree varios planes de protección y prográmelos para ejecutarlos en momentos diferentes.
- No se puede realizar una copia de seguridad de los buzones de correo de archivo (**Archivo local**).
- Una copia de seguridad de un buzón de correo incluye solo las carpetas visibles para los usuarios. La carpeta **Elementos recuperables** y sus subcarpetas (**Eliminaciones**, **Versiones**, **Depuraciones**, **Auditorías**, **Retenciones**, **Registro del calendario**) no se incluyen en la copia de seguridad de un buzón de correo.
- No es posible la recuperación en un nuevo buzón de correo de Microsoft 365. Primero, debe crear un usuario de Microsoft 365 nuevo manualmente y, a continuación, recuperar los elementos en el buzón de correo del usuario.
- No se admite la recuperación a otra organización de Microsoft 365.
- Es posible que algunos tipos o propiedades de elementos admitidos en Microsoft 365 no sean compatibles con Exchange Server. Se omitirán en una recuperación a Exchange Server.

Cómo añadir una organización de Microsoft 365

Para añadir una organización de Microsoft, debe saber su ID de la aplicación, el código secreto y la ID de inquilino de Microsoft 365. Consulte Obtener la ID y el código secreto de la aplicación para obtener más información sobre cómo obtenerlos.

Para añadir una organización de Microsoft 365

1. Instale el Agente para Office 365 en un equipo que ejecute Windows y esté conectado a Internet. Solo puede haber un Agente para Office 365 en una organización.
2. En la consola web de Cyber Protect, haga clic en **Microsoft Office 365**.
3. En la ventana que se abra, introduzca su ID de la aplicación, el código secreto y la ID de inquilino de Microsoft 365.
4. Haga clic en **Iniciar sesión**.

Los elementos de datos de su organización aparecerán en la consola web de Cyber Protect de la pestaña **Microsoft Office 365**.

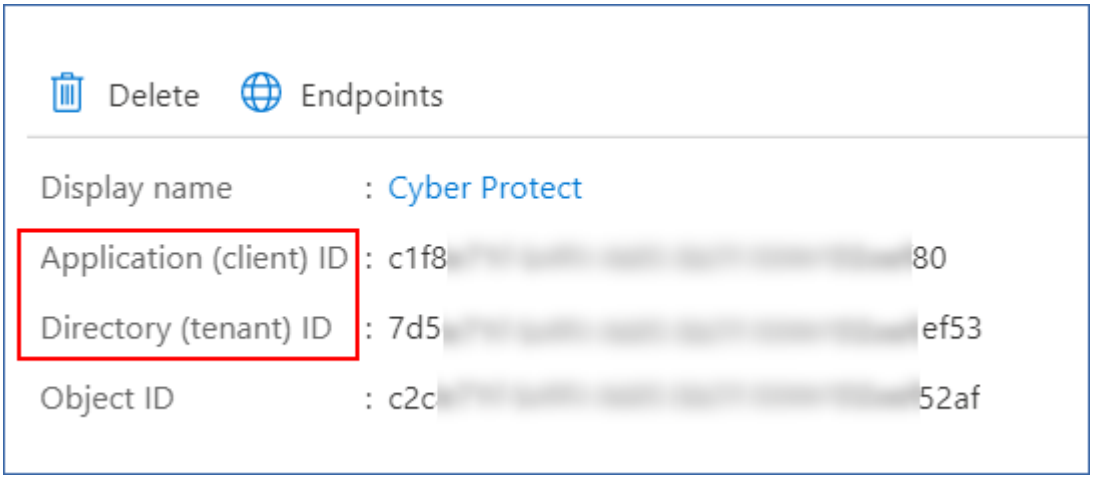
Obtener el ID y el secreto de la aplicación

Para usar la autenticación moderna de Microsoft 365, debe crear una aplicación personalizada en Azure Active Directory y conceder permisos API concretos. Así, obtendrá el **ID de la aplicación**, el **secreto de la aplicación** y el **ID del directorio (inquilino)** que necesita para acceder a la consola web de Cyber Protect.

Pasos para crear una aplicación en Azure Active Directory

1. Inicie sesión en el Portal de Azure como administrador.
2. Vaya a **Azure Active Directory** > **Registros de aplicaciones**, y haga clic en **Nuevo registro**.
3. Especifique un nombre para su aplicación personalizada, por ejemplo, Cyber Protect.
4. En **Tipos de cuenta compatibles**, seleccione **Solo cuentas de este directorio organizativo**.
5. Haga clic en **Registrar**.

Se ha creado su aplicación. En el portal de Azure, vaya a la página **Información general** de la aplicación y compruebe su ID (cliente) de la aplicación y su directorio (ID del inquilino).



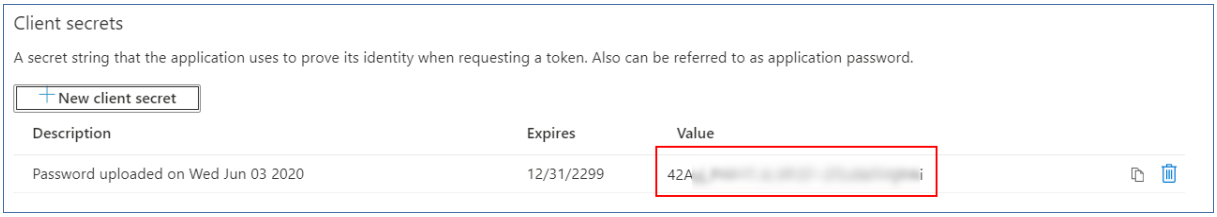
Para obtener más información sobre cómo crear una aplicación en el portal de Azure, consulte la documentación de Microsoft.

Pasos para otorgar los permisos API necesarios a su aplicación

1. En el portal Azure, vaya a los **permisos API** de la aplicación y haga clic en **Añadir un permiso**.
2. Seleccione la pestaña **API que usa mi organización** y luego busque **Office 365 Exchange Online**.
3. Haga clic en **Office 365 Exchange Online** y luego en **Permisos de aplicación**.
4. Seleccione la casilla **full_access_as_app** y haga clic en **Añadir permisos**.
5. En **Permisos API**, haga clic en **Añadir un permiso**.
6. Seleccione **Microsoft Graph**.
7. Seleccione **Permisos de aplicación**.
8. Expanda la pestaña **Directorio**, y seleccione la casilla de verificación **Directory.Read.All**. Haga clic en **Agregar permisos**.
9. Compruebe todos los permisos y haga clic en **Conceder permiso de administrador para <your application's name>**.
10. Haga clic en **Sí** para confirmar su elección.

Pasos para crear un secreto de la aplicación

1. En el portal Azure, vaya a las opciones de la aplicación **Certificados y secretos** > **Nuevo secreto de cliente**.
2. En el cuadro de diálogo que se abra, seleccione Caduca: **Nunca**, y, a continuación, haga clic en **Añadir**.
3. Compruebe el secreto de su aplicación en el campo **Valor** y asegúrese de recordarlo.



Para obtener más información sobre el secreto de la aplicación, consulte la documentación de Microsoft.

Cambio de las credenciales de acceso de Microsoft 365

Puede cambiar las credenciales de acceso de Microsoft 365 sin tener que volver a instalar el agente.

Pasos para cambiar las credenciales de acceso de Microsoft 365

1. En la consola web de Cyber Protect, vaya a **Dispositivos** > **Microsoft Office 365**.
2. Seleccione la organización de Microsoft 365.
3. Haga clic en **Especificar credenciales**.
4. Introduzca su ID de la aplicación, el código secreto y la ID de inquilino de Microsoft 365. Consulte Obtener la ID y el código secreto de la aplicación para obtener más información sobre cómo obtenerlos.
5. Haga clic en **Iniciar sesión**.

Selección de buzones de correo

Seleccione los buzones de correo tal como se describe a continuación y luego especifique otros ajustes del plan de protección según corresponda.

Pasos para seleccionar buzones de correo

1. En la consola web de Cyber Protect, vaya a **Dispositivos** > **Microsoft Office 365**.
2. Seleccione los buzones de correo de los que desea realizar una copia de seguridad.
3. Haga clic en **Copia de seguridad**.

Recuperación de buzones de correo y elementos de los buzones

Recuperación de buzones de correo

1. [Solo al recuperar a Exchange Server] Asegúrese de que haya un usuario de Exchange con el mismo nombre de inicio de sesión que el nombre del usuario cuyo buzón de correo se está recuperando. De lo contrario, cree el usuario. Consulte la lista completa de requisitos de este usuario en "Requisitos de las cuentas de usuario" (p. 519).
2. En la consola web de Cyber Protect, vaya a **Dispositivos** > **Microsoft Office 365**.
3. Seleccione el buzón de correo que desea recuperar y, a continuación, haga clic en **Recuperar**.
   Puede buscar los buzones de correo por el nombre. No se pueden usar caracteres comodín.
   Si el buzón de correo se ha eliminado, selecciónelo en la pestaña Almacenamiento de copias de seguridad y, a continuación, haga clic en **Mostrar copias de seguridad**.
4. Seleccione un punto de recuperación. Tenga en cuenta que los puntos de recuperación se filtran por ubicación.
5. Haga clic en **Recuperar** > **Buzón de correo**.
6. Para recuperar a un Exchange Server, seleccione **Microsoft Exchange** en **Recuperar a**. Siga la recuperación según se describe en "Recuperación de buzones de correo" (p. 520), a partir del paso 9. No se requieren más pasos para este procedimiento.
   Para recuperar a Microsoft 365, mantenga el valor predeterminado de **Microsoft Office 365** en **Recuperar a**.
7. En **Buzón de correo de destino** puede consultar, cambiar o especificar el buzón de correo de destino.
   De manera predeterminada, se selecciona el buzón de correo original. Si este buzón de correo no existe, debe indicar el buzón de correo de destino.
8. Haga clic en **Iniciar recuperación**.

Recuperación de elementos de buzón de correo

1. [Solo al recuperar a Exchange Server] Asegúrese de que haya un usuario de Exchange con el mismo nombre de inicio de sesión que el nombre del usuario cuyo buzón de correo se está recuperando. De lo contrario, cree el usuario. Consulte la lista completa de requisitos de este usuario en "Requisitos de las cuentas de usuario" (p. 519).
2. En la consola web de Cyber Protect, vaya a **Dispositivos** > **Microsoft Office 365**.
3. Seleccione el buzón de correo que contenía originalmente los elementos que desea recuperar y, a continuación, haga clic en **Recuperar**.
   Puede buscar los buzones de correo por el nombre. No se pueden usar caracteres comodín.

Si el buzón de correo se ha eliminado, selecciónelo en la pestaña Almacenamiento de copias de seguridad y, a continuación, haga clic en **Mostrar copias de seguridad**.

4. Seleccione un punto de recuperación. Tenga en cuenta que los puntos de recuperación se filtran por ubicación.
5. Haga clic en **Recuperar** > **Mensajes de correo electrónico**.
6. Seleccione los elementos que desea recuperar.

   Tiene a su disposición las siguientes opciones de búsqueda. No se pueden usar caracteres comodín.

   - Para los mensajes de correo electrónico: búsqueda por asunto, remitente, destinatario y fecha.
   - Para los eventos: búsqueda por título y fecha.
   - Para las tareas: búsqueda por asunto y fecha.
   - Para los contactos: búsqueda por nombre, dirección de correo electrónico y número de teléfono.

   Cuando se selecciona un mensaje de correo electrónico, puede hacer clic en **Mostrar contenido** para ver el contenido, incluidos los documentos adjuntos.

   Nota
   Haga clic en el nombre de un archivo adjunto para descargarlo.

   Cuando se selecciona un mensaje de correo electrónico, puede hacer clic en **Enviar como correo electrónico** para enviar el mensaje a una dirección de correo electrónico. El mensaje se envía desde el correo electrónico de su cuenta de administrador.

   Para poder seleccionar carpetas, haga clic en el icono de recuperar carpetas: 
7. Haga clic en **Recuperar**.
8. Para recuperar a un Exchange Server, seleccione **Microsoft Exchange** en **Recuperar a**.

   Para recuperar a Microsoft 365, mantenga el valor predeterminado de **Microsoft Office 365** en **Recuperar a**.
9. [Solo al recuperar a Exchange Server] Haga clic en **Equipo de destino con Microsoft Exchange Server** para seleccionar o cambiar el equipo de destino. Este paso permite recuperar en un equipo que no esté ejecutando Agent for Exchange.

   Indique el nombre de dominio completo (FQDN) del equipo donde está habilitado el rol **Acceso de cliente** de Microsoft Exchange Server. El equipo debe pertenecer al mismo bosque de Active Directory que el equipo que realiza la recuperación.

   Si se le pide, proporcione las credenciales de la cuenta que se utilizará para acceder al equipo. Los requisitos de esta cuenta aparecen en "Derechos de usuario necesarios" (p. 511).
10. En **Buzón de correo de destino** puede consultar, cambiar o especificar el buzón de correo de destino.

    De manera predeterminada, se selecciona el buzón de correo original. Si este buzón de correo no existe, debe indicar el buzón de correo de destino.

11. [Solo al recuperar mensajes de correo electrónico] En **Carpeta de destino** puede consultar o cambiar la carpeta de destino en el buzón de correo de destino. De manera predeterminada, se selecciona la carpeta **Elementos recuperados**.
12. Haga clic en **Iniciar recuperación**.

Protección de datos de Google Workspace

Esta opción está disponible solamente en las implementaciones en la nube de Acronis Cyber Protect. Para obtener una descripción detallada de esta funcionalidad, consulte https://www.acronis.com/support/documentation/CyberProtectionService/#protecting-google-workspace-data.html.

Protección de Oracle Database

La protección de Oracle Database se describe en un documento independiente disponible en https://dl.managed-protection.com/u/pdf/AcronisCyberProtect_15_OracleBackup_whitepaper.pdf.

Operaciones especiales con equipos virtuales

Ejecución de un equipo virtual desde una copia de seguridad (Instant Restore)

Puede ejecutar un equipo virtual desde una copia de seguridad a nivel de disco que contenga un sistema operativo. Esta operación, también conocida como "restauración instantánea", le permite iniciar un servidor virtual en cuestión de segundos. Las unidades de disco virtual se emulan directamente desde la copia de seguridad y, por consiguiente, no consumen espacio en el almacén de datos (almacenamiento). El espacio de almacenamiento es necesario solo para mantener los cambios en las unidades de disco virtuales.

Se recomienda ejecutar este equipo virtual temporal durante un plazo máximo de tres días. Entonces puede eliminarlo por completo o convertirlo en un equipo virtual normal (finalizarlo) sin tiempo de inactividad.

Mientras exista el equipo virtual temporal, las reglas de retención no podrán aplicarse a la copia de seguridad que use dicho equipo. Las copias de seguridad del equipo original pueden seguir en ejecución.

Ejemplos de uso

- **Recuperación ante desastres**
  Coloque una copia de un equipo con error en línea de forma instantánea.
- **Prueba de una copia de seguridad**
  Ejecute el equipo desde la copia de seguridad y asegúrese de que el SO invitado y las aplicaciones huéspedes funcionan correctamente.
- **Acceso a los datos de la aplicación**
  Mientras el equipo está en ejecución, use las herramientas de gestión nativas de la aplicación para acceder y extraer los datos necesarios.

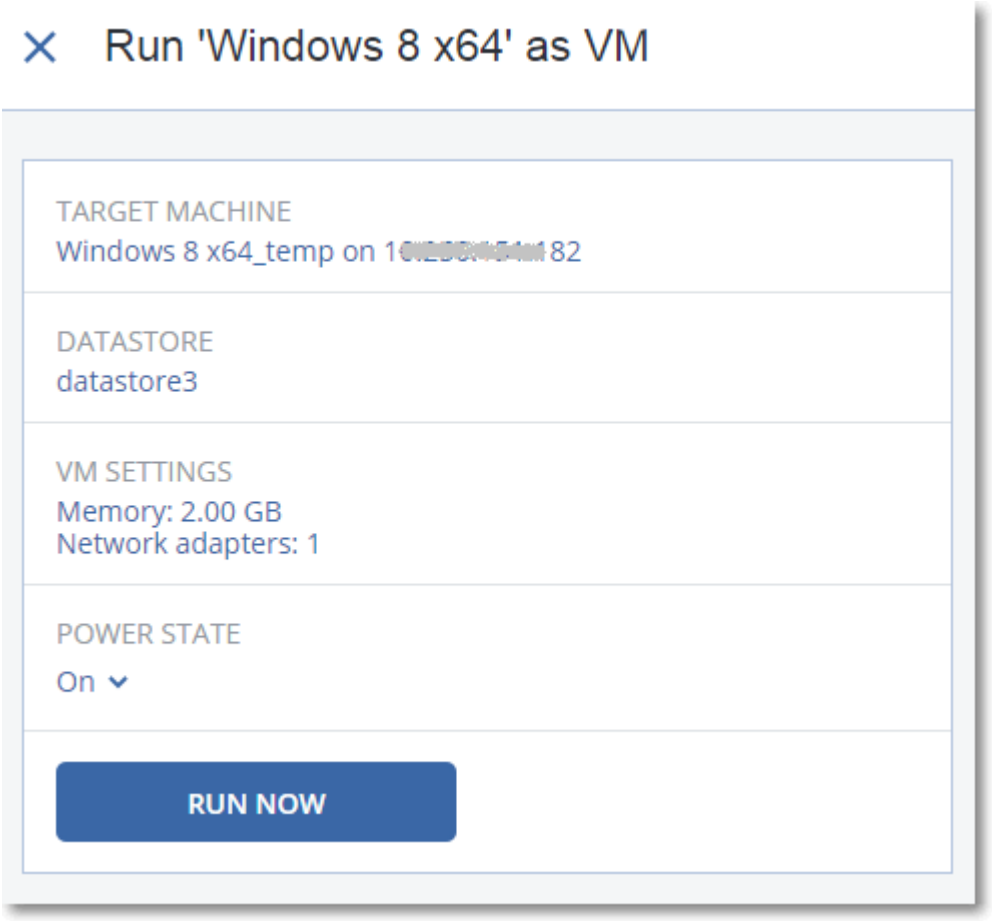
Requisitos previos

- Debe haber por lo menos un Agente para VMware o un Agente para Hyper-V registrado en el servicio de ciberprotección.
- La copia de seguridad puede almacenarse en una carpeta de red, en un nodo de almacenamiento o en una carpeta local del equipo en el que está instalado Agente para VMware o Agente para Hyper-V. Si selecciona una carpeta de red, debe ser accesible desde ese equipo. Un equipo virtual también se puede ejecutar desde una copia de seguridad almacenada en la cloud, pero el rendimiento será más lento porque la operación requiere una lectura intensa mediante accesos aleatorios de la copia de seguridad. No se puede ejecutar un equipo virtual desde una copia de seguridad almacenada en un servidor SFTP, un dispositivo de cintas o Secure Zone.

- La copia de seguridad debe contener un equipo completo o todos los volúmenes necesarios para que el sistema operativo se inicie.
- Pueden usarse las copias de seguridad tanto de los equipos físicos como de los virtuales. No pueden usarse las copias de seguridad de *contenedores* Virtuozzo.
- Las copias de seguridad que contienen volúmenes lógicos (LVM) de Linux deben crearse con Agente para VMware o Agente para Hyper-V. El equipo virtual debe ser del mismo tipo que el equipo original (ESXi o Hyper-V).

Ejecución del equipo

1. Realice uno de los siguientes procedimientos:
   - Seleccione un equipo incluido en la copia de seguridad, haga clic en **Recuperación** y luego seleccione un punto de recuperación.
   - Seleccione un punto de recuperación en la pestaña de almacenamiento de copia de seguridad.
2. Haga clic en **Ejecutar como equipo virtual**.
   El software selecciona automáticamente el servidor y otros parámetros necesarios.



3. [Opcional] Haga clic en **Equipo de destino** y, a continuación, cambie el tipo de equipo virtual (ESXi o Hyper-V), el servidor o el nombre del equipo virtual.

4. [Opcional] Haga clic en **Almacén de datos** para ESXi o **Ruta** para Hyper-V y, a continuación, seleccione el almacén de datos para el equipo virtual.

   Los cambios realizados a los discos virtuales se acumulan durante la ejecución del equipo. Asegúrese de que el almacén de datos seleccionado tiene suficiente espacio libre. Si desea mantener los cambios al hacer que el equipo virtual sea permanente, seleccione un almacén de datos adecuado para ejecutar el equipo de producción.
5. [Opcional] Haga clic en **Configuración de equipo virtual** para modificar el tamaño de la memoria y las conexiones de red del equipo virtual.
6. [Opcional] Seleccione el estado de energía del equipo virtual (**Activado**/**Desactivado**).
7. Haga clic en **Ejecutar ahora**.

Como resultado, el equipo aparecerá en la interfaz web con uno de los siguientes iconos:  o  . Los equipos virtuales de este tipo no se pueden seleccionar para hacer una copia de seguridad.

Eliminación del equipo

No se recomienda eliminar ningún equipo virtual temporal directamente en vSphere/Hyper-V porque podrían originarse anomalías en la interfaz web. Además, la copia de seguridad desde la que se ejecutaba el equipo podría permanecer bloqueada por un tiempo (no puede eliminarse mediante reglas de retención).

Para eliminar un equipo virtual que se ejecuta desde una copia de seguridad

1. En la pestaña **Todos los dispositivos**, seleccione un equipo que se ejecute desde una copia de seguridad.
2. Haga clic en **Eliminar**.

El equipo se elimina de la interfaz web. También se elimina del inventario y del almacén de datos (almacenamiento) de vSphere o Hyper-V. Se perderán todos los cambios que se realicen a los datos durante la ejecución del equipo.

Finalización del equipo

Mientras un equipo virtual se ejecuta desde una copia de seguridad, el contenido de los discos virtuales se toma directamente de dicha copia de seguridad. Por tanto, el equipo se volverá inaccesible o incluso corrupto si se pierde la conexión a la ubicación de la copia de seguridad o al agente de protección.

Puede optar por hacer el equipo permanente, es decir, recuperar todos sus discos virtuales junto con los cambios que tuvieron lugar mientras se ejecutaba el equipo, en el almacén de datos que almacena dichos cambios. Este proceso se denomina "finalización".

La finalización se lleva a cabo sin tiempo de inactividad. El equipo virtual *no* se apagará durante la finalización.

La ubicación de los discos virtuales finales se define en los parámetros de la operación **Ejecutar como VM** (**Almacén de datos** para ESXi o **Ruta** para Hyper-V). Antes de completar la finalización, garantice que el espacio libre, las capacidades para compartir y el rendimiento de este almacén de datos son adecuados para ejecutar el equipo en la producción.

Nota
La finalización no es compatible con Hyper-V ejecutándose en Windows Server 2008/2008 R2 y Microsoft Hyper-V Server 2008/2008 R2 porque la API necesaria falta en estas versiones de Hyper-V.

Para finalizar un equipo que se ejecuta desde una copia de seguridad

1. En la pestaña **Todos los dispositivos**, seleccione un equipo que se ejecute desde una copia de seguridad.
2. Haga clic en **Finalizar**.
3. [Opcional] Especifique un nuevo nombre para el equipo.
4. [Opcional] Cambie el modo de aprovisionamiento del disco. El valor predeterminado es el de **Fino**.
5. Haga clic en **Finalizar**.

El nombre del equipo cambia inmediatamente. El proceso de recuperación se muestra en la pestaña **Actividades**. Una vez completada la recuperación, el icono del equipo cambia al de un equipo virtual normal.

Lo que necesita saber sobre la finalización

Comparación entre la finalización y una recuperación estándar

El proceso de finalización es más lento que la recuperación estándar debido a estos motivos:

- Durante la finalización, el agente accede aleatoriamente a varias partes de la copia de seguridad. Al recuperar todo un equipo, el agente lee los datos de la copia de seguridad de forma secuencial.
- Si el equipo virtual se está ejecutando durante la finalización, el agente lee los datos de la copia de seguridad más a menudo para mantener ambos procesos al mismo tiempo. Durante una recuperación estándar, se detiene el equipo virtual.

Finalización de equipos en ejecución a partir de copias de seguridad en la nube

Debido al acceso intensivo a los datos de la copia de seguridad, la velocidad de finalización depende enormemente del ancho de banda de la conexión entre la ubicación de la copia de seguridad y el agente. La finalización será más lenta para las copias de seguridad ubicadas en la nube que para aquellas locales. Si la conexión a Internet es muy lenta o inestable, la finalización de un equipo en ejecución desde una copia de seguridad en la nube puede generar errores. Si quiere realizar la

finalización y puede elegir, le recomendamos que ejecute equipos virtuales desde copias de seguridad locales.

Trabajar en VMware vSphere

Esta sección describe operaciones que son específicas para entornos de VMware vSphere.

Replicación de equipos virtuales

La replicación solo está disponible para los equipos virtuales VMware ESXi.

Es el proceso de crear una copia exacta (réplica) de un equipo virtual y mantener luego la réplica sincronizada con el equipo original. Al replicar un equipo virtual crítico, siempre dispondrá de una copia del equipo en un estado "listo para comenzar".

La replicación se puede iniciar manualmente o según la planificación que especifique. La primera replicación es completa (se copia todo el equipo). Las siguientes replicaciones son incrementales y se realizan con Seguimiento de bloques modificados cuando esta opción está habilitada.

Diferencias entre la replicación y la copia de seguridad

A diferencia de las copias de seguridad, las réplicas solo conservan el último estado del equipo virtual. Una réplica consume espacio del almacén de datos, mientras que las copias de seguridad se pueden guardar en un almacenamiento más económico.

Sin embargo, encender una réplica es mucho más rápido que realizar una recuperación y más veloz que ejecutar un equipo virtual desde una copia de seguridad. Cuando se enciende, la réplica funciona más rápido que un equipo virtual que se ejecuta desde una copia de seguridad y no carga el Agente para VMware.

Ejemplos de uso

- **Replicar equipos virtuales en un sitio remoto**.
  La replicación permite hacer frente a los errores parciales o completos que surgen en centros de datos mediante la clonación de los equipos virtuales de un sitio primario a otro secundario. El sitio secundario suele encontrarse en una instalación remota que tiene poca probabilidad de verse afectada por factores medioambientales o de infraestructura, entre otros, que podrían provocar fallos en el sitio primario.
- **Replicar equipos virtuales dentro de un solo sitio (de un servidor/almacén de datos a otro)**.
  La replicación in situ se puede usar en escenarios de alta disponibilidad y recuperación ante desastres.

Lo que se puede hacer con una réplica

- **Realizar pruebas en una réplica**

  La réplica se encenderá para la realización de las pruebas. Use vSphere Client u otras herramientas para comprobar si la réplica funciona correctamente. La replicación se suspende mientras se están realizando pruebas.
- **Conmutar por error a una réplica**

  La conmutación por error es una transición de la carga de trabajo del equipo virtual original a su réplica. La replicación se suspende mientras la conmutación por error está en marcha.
- **Hacer una copia de seguridad de la réplica**

  Tanto la copia de seguridad como la replicación requieren el acceso a los discos virtuales, por lo que afectan al rendimiento del servidor donde se ejecuta el equipo virtual. Si quiere disponer de la réplica de un equipo virtual y, además, de las copias de seguridad, pero no quiere someter el servidor de producción a una carga extra, replique el equipo en otro servidor y configure la replicación de las copias de seguridad.

Restricciones

Los siguientes tipos de equipos virtuales no se pueden replicar:

- Equipos tolerantes a errores que se ejecutan en ESXi 5.5 y versiones anteriores.
- Equipos que se ejecutan desde copias de seguridad.
- Réplicas de equipos virtuales.

Creación de un plan de replicación

Se debe crear un plan de replicación individual para cada equipo. No se puede aplicar un plan existente a otros equipos.

Para crear un plan de replicación

1. Seleccione un equipo virtual que quiera replicar.
2. Haga clic en **Replicación**.

   El software muestra una nueva plantilla de plan de replicación.
3. [Opcional] Para modificar el nombre del plan de replicación, haga clic en el nombre predeterminado.
4. Haga clic en **Equipo de destino** y luego haga lo siguiente:
   a. Seleccione si desea crear una réplica nueva o utilizar una réplica existente del equipo original.
   b. Seleccione el servidor ESXi y especifique el nombre de la réplica nueva o seleccione una réplica existente.

      El nombre predeterminado de una réplica nueva es **[Nombre del equipo original]_replica**.
   c. Haga clic en **Aceptar**.

5. [Solo al replicar en un equipo nuevo] Haga clic en **Almacén de datos** y luego seleccione el almacén de datos para el equipo virtual.
6. [Opcional] Haga clic en **Planificación** para cambiar la planificación de la replicación.

   De forma predeterminada, la replicación se realiza a diario de lunes a viernes. Puede seleccionar la hora a la que la replicación se ejecutará.

   Si quiere cambiar la frecuencia con que se realiza la replicación, mueva el control deslizante y especifique la planificación.

   También puede hacer lo siguiente:
   - Fije el rango de fechas en el que la planificación tendrá efecto. Seleccione la casilla de verificación **Ejecutar el plan en un rango de fechas** y especifique el rango de fechas.
   - Deshabilite la planificación. En este caso, la replicación se puede iniciar manualmente.
7. [Opcional] Haga clic en el ícono de engranaje para modificar las opciones de replicación.
8. Haga clic en **Aplicar**.
9. [Opcional] Para ejecutar el plan manualmente, haga clic en **Ejecutar ahora** en el panel del plan.

Al ejecutar un plan de replicación, la réplica del equipo virtual aparece en la lista **Todos los dispositivos** con el icono siguiente: 

Realización de pruebas en una réplica

Para preparar una réplica para la realización de pruebas

1. Seleccione la réplica que desea someter a prueba.
2. Haga clic en **Probar réplica**.
3. Haga clic en **Iniciar pruebas**.
4. Seleccione si desea conectar la réplica encendida a una red. De forma predeterminada, la réplica no se conectará a ninguna red.
5. [Opcional] Si elige conectar la réplica a la red, desactive la casilla de verificación **Detener equipo virtual original** para detener el equipo original antes de encender la réplica.
6. Haga clic en **Iniciar**.

Para detener las pruebas de una réplica

1. Seleccione una réplica en la que se estén realizando pruebas.
2. Haga clic en **Probar réplica**.
3. Haga clic en **Detener pruebas**.
4. Confirme su decisión.

Conmutación por error en una réplica

Para conmutar por error un equipo en una réplica

1. Seleccione la réplica donde quiera realizar la conmutación por error.
2. Haga clic en **Acciones de réplica**.
3. Haga clic en **Conmutación por error**.
4. Seleccione si desea conectar la réplica encendida a una red. De forma predeterminada, la réplica se conectará a la misma red que el equipo original.
5. [Opcional] Si elige conectar la réplica a la red, desactive la casilla de verificación **Detener equipo virtual original** para mantener conectado el equipo original.
6. Haga clic en **Iniciar**.

Mientras la réplica está en un estado de conmutación por error, puede elegir una de las siguientes acciones:

- **Detener conmutación por error**

  Detenga la conmutación por error si el equipo original se ha arreglado. La réplica se apagará. Se reanudará la replicación.
- **Ejecutar conmutación por error permanente en la réplica**

  Esta operación instantánea elimina la marca "réplica" del equipo virtual para que ya no se pueda realizar ninguna replicación. Si quiere reanudar la replicación, edite el plan de replicación para seleccionar este equipo como origen.
- **Conmutación por recuperación**

  Realice una conmutación por recuperación si ejecutó una conmutación por error en el sitio que no está destinado a las operaciones continuas. La réplica se recuperará en el equipo original o en un equipo virtual nuevo. Cuando se completa la recuperación en el equipo original, se enciende y la replicación se reanuda. Si elige recuperar en un equipo nuevo, edite el plan de replicación para seleccionar este equipo como origen.

Detención de una conmutación por error

Para detener conmutación por error

1. Seleccione una réplica en estado de conmutación por error.
2. Haga clic en **Acciones de réplica**.
3. Haga clic en **Detener conmutación por error**.
4. Confirme su decisión.

Ejecución de una conmutación por error permanente

Para ejecutar una conmutación por error permanente

1. Seleccione una réplica en estado de conmutación por error.
2. Haga clic en **Acciones de réplica**.
3. Haga clic en **Conmutación por error permanente**.
4. [Opcional] Cambie el nombre del equipo virtual.

5. [Opcional] Active la casilla de verificación **Detener equipo virtual original**.
6. Haga clic en **Iniciar**.

Conmutación por recuperación

Para conmutar por recuperación desde una réplica

1. Seleccione una réplica en estado de conmutación por error.
2. Haga clic en **Acciones de réplica**.
3. Haga clic en **Conmutación por recuperación desde la réplica**.
   El software selecciona automáticamente el equipo original como equipo de destino.
4. [Opcional] Haga clic en **Equipo de destino** y luego haga lo siguiente:
   a. Seleccione si desea realizar la conmutación por recuperación en un equipo nuevo o existente.
   b. Seleccione el servidor ESXi y especifique el nombre del equipo nuevo o seleccione un equipo existente.
   c. Haga clic en **Aceptar**.
5. [Opcional] Al realizar una conmutación por recuperación en un equipo nuevo, también puede hacer lo siguiente:
   - Haga clic en **Almacén de datos** para seleccionar el almacén de datos para el equipo virtual.
   - Haga clic en **Configuración de VM** para cambiar el tamaño de la memoria, el número de procesadores y las conexiones de red del equipo virtual.
6. [Opcional] Haga clic en **Opciones de recuperación** para modificar las opciones de conmutación por recuperación.
7. Haga clic en **Iniciar recuperación**.
8. Confirme su decisión.

Opciones de replicación

Para modificar las opciones de replicación, haga clic en el icono del engranaje que se encuentra al lado del nombre del plan de replicación y, a continuación, haga clic en **Opciones de replicación**.

Seguimiento de bloques modificados (CBT)

Esta opción se parece a la opción de copia de seguridad "Seguimiento de bloques modificados (CBT)".

Aprovisionamiento del disco

Esta opción define los ajustes de aprovisionamiento del disco para la réplica.

El valor predeterminado es el siguiente: **Aprovisionamiento fino**.

Los valores disponibles son los siguientes: **Aprovisionamiento fino**, **Aprovisionamiento grueso**, **Mantener la configuración original**.

Manejo de errores

Esta opción se parece a la opción de copia de seguridad "Manejo de errores".

Comandos previos/posteriores

Esta opción se parece a la opción de copia de seguridad "Comandos previos/posteriores".

Volume Shadow Copy Service VSS para equipos virtuales

Esta opción se parece a la opción de copia de seguridad "Volume Shadow Copy Service VSS para equipos virtuales".

Opciones de recuperación tras error

Para modificar las opciones de conmutación por recuperación, haga clic en **Opciones de recuperación** al configurar la conmutación por recuperación.

Manejo de errores

Esta opción se parece a la opción de recuperación "Manejo de errores".

Rendimiento

Esta opción se parece a la opción de recuperación "Rendimiento".

Comandos previos/posteriores

Esta opción se parece a la opción de recuperación "Comandos previos/posteriores".

Gestión de energía de VM

Esta opción se parece a la opción de recuperación "Gestión de energía del equipo virtual".

Recopilación de una réplica inicial

Para acelerar la replicación en una ubicación remota y ahorrar ancho de banda en la red, puede realizar recopilación de réplicas.

Importante
Para realizar la recopilación de réplicas, Agente para VMware (dispositivo virtual) debe ejecutarse en el ESXi de destino.

Para recopilar una réplica inicial

1. Realice uno de los siguientes procedimientos:
   - Si el equipo virtual original puede desconectarse, hágalo y luego vaya directamente al paso 4.
   - Si el equipo virtual original no se puede desconectar, continúe en el paso siguiente.

2. Cree un plan de replicación.

   Al crear el plan, en **Equipo de destino**, seleccione **Réplica nueva** y el ESXi que aloja el equipo original.
3. Ejecute el plan una vez.

   Se crea una réplica en el ESXi original.
4. Exporte los archivos del equipo virtual (o de la réplica) a un disco duro externo.
   a. Conecte el disco duro externo al equipo donde se ejecuta vSphere Client.
   b. Conecte vSphere Client al vCenter\ESXi original.
   c. Seleccione la réplica recién creada en el inventario.
   d. Haga clic en **Archivo** > **Exportar** > **Exportar plantilla de OVF**.
   e. En **Directorio**, especifique la carpeta del disco rígido externo.
   f. Haga clic en **Aceptar**.
5. Transfiera el disco duro a la ubicación remota.
6. Importe la réplica al ESXi de destino.
   a. Conecte el disco duro externo al equipo donde se ejecuta vSphere Client.
   b. Conecte vSphere Client al vCenter\ESXi de destino.
   c. Haga clic en **Archivo** > **Implementar plantilla de OVF**.
   d. En **Implementar desde un archivo o URL**, especifique la plantilla que exportó en el paso 4.
   e. Complete el procedimiento de importación.
7. Edite el plan de replicación que creó en el paso 2. En **Equipo de destino**, seleccione **Réplica existente** y, a continuación, seleccione la réplica importada.

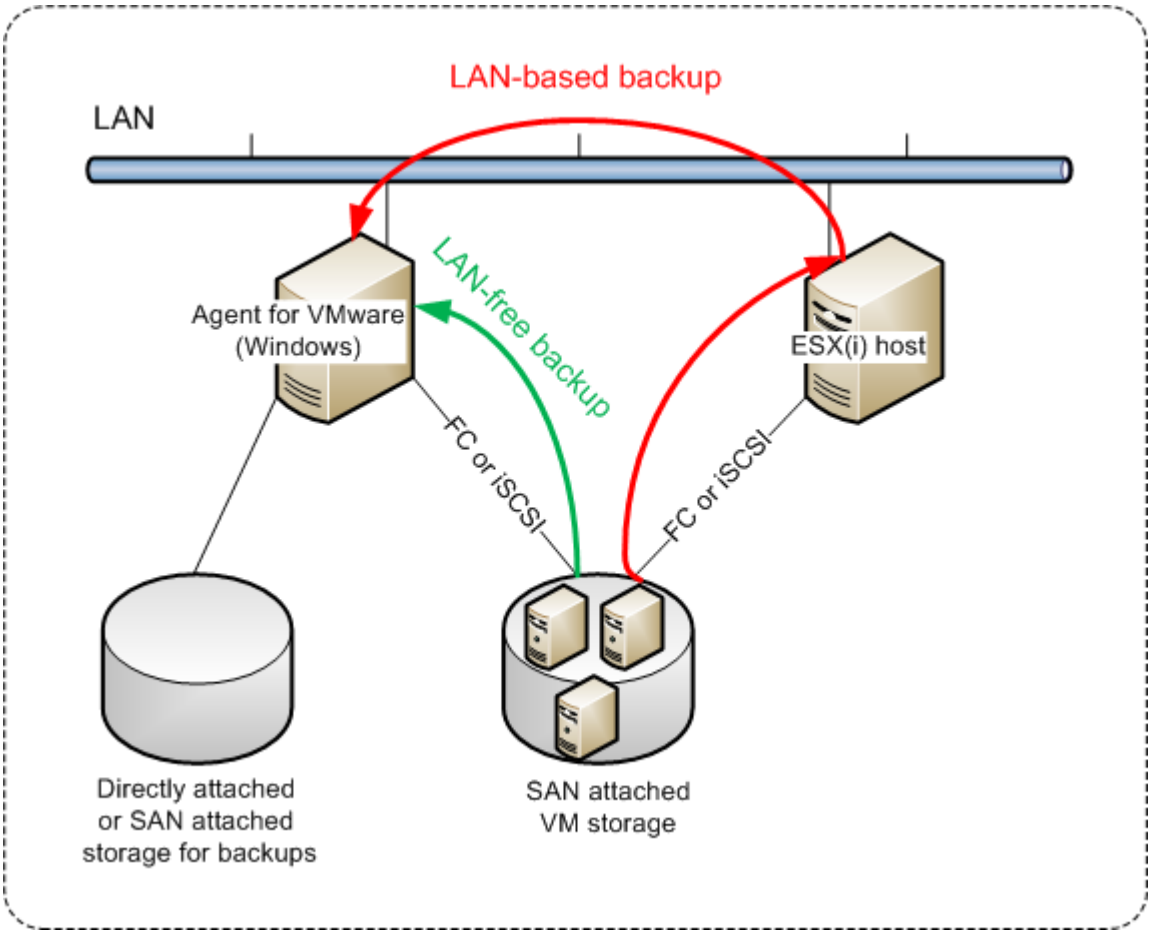
Como resultado, el software continuará actualizando la réplica. Todas las replicaciones serán incrementales.

Copia de seguridad sin LAN

Si sus servidores ESXi de producción están tan cargados que no es recomendable la ejecución de los dispositivos virtuales, considere instalar Agente para VMware (Windows) en un equipo físico fuera de la infraestructura de ESXi.

Si su ESXi usa un almacenamiento conectado a SAN, instale el agente en un equipo conectado al mismo SAN. El agente realizará la copia de seguridad de los equipos virtuales directamente desde el almacenamiento en vez de mediante el servidor ESXi y LAN. Esta capacidad se llama copia de seguridad sin LAN.

El diagrama a continuación ilustra una copia de seguridad basada en LAN y sin LAN. El acceso sin LAN a los equipos virtuales está disponible si posee canal de fibra (FC) o red de área de almacenamiento iSCSI. Para eliminar completamente la transferencia de los datos incluidos en la copia de seguridad a través de la LAN, almacene las copias de seguridad en un disco local del equipo del agente o en un almacenamiento SAN conectado.



Para permitir que el agente acceda al almacén de datos directamente

1. Instale el Agente para VMware en un equipo que ejecute Windows y esté conectado a vCenter Server.
2. Conecte el número de unidad lógica (LUN) que aloja el almacén de datos en el equipo. Considere el siguiente escenario:
   - Use el mismo protocolo (iSCSI o FC) que se utiliza para la conexión del almacén de datos con el ESXi.
   - *No debe* iniciar el LUN y, además, debe mostrarse como disco "desconectado" en **Gestión del disco**. Si Windows inicia el LUN, este puede resultar dañado o ilegible en VMware vSphere. Para evitar la inicialización de LUN, la **directiva SAN** se establecerá automáticamente en **Todos los que están fuera de línea** durante la instalación del Agente para VMware (Windows).

Como resultado, el agente utilizará el modo de transporte SAN para acceder a los discos virtuales, es decir, leerá los sectores LUN sin procesar en iSCSI/FC sin reconocer el sistema de archivos VMFS, que Windows no detecta.

Limitaciones

- En vSphere 6.0 y versiones posteriores, el agente no puede utilizar el modo de transporte de SAN si algunos de los discos de equipo virtual están ubicados en un Volumen Virtual de VMware (VVol) y otros no. Las copias de seguridad de dichos equipos virtuales fallarán.
- Los equipos virtuales cifrados, presentados en VMware vSphere 6.5, se incluirán en la copia de seguridad mediante LAN, incluso si configura el modo de transporte SAN para el agente. El agente recurrirá al transporte NBD, pues VMware no es compatible con el transporte SAN para realizar copias de seguridad de discos virtuales cifrados.

Ejemplo

Si está utilizando un SAN de iSCSI, configure el iniciador de iSCSI en el equipo que ejecute Windows y en el que esté instalado Agente para VMware.

Para configurar la directiva SAN

1. Inicie sesión como administrador, ejecute el símbolo del sistema, escriba `diskpart` y, a continuación, pulse **Intro**.
2. Escriba `san`, y, a continuación, pulse **Intro**. Asegúrese de que se muestra la **Directiva SAN: Se muestran Todos los que están fuera de línea**.
3. Si se establece otro valor para la directiva SAN:
   a. Escriba `san policy=offlineall`.
   b. Pulse **Intro**.
   c. Para comprobar que la configuración se haya aplicado correctamente, siga el paso 2.
   d. Reinicie el equipo.

Para configurar un iniciador iSCSI

1. Vaya al **Panel de control** > **Herramientas administrativas** > **Iniciador de iSCSI**.

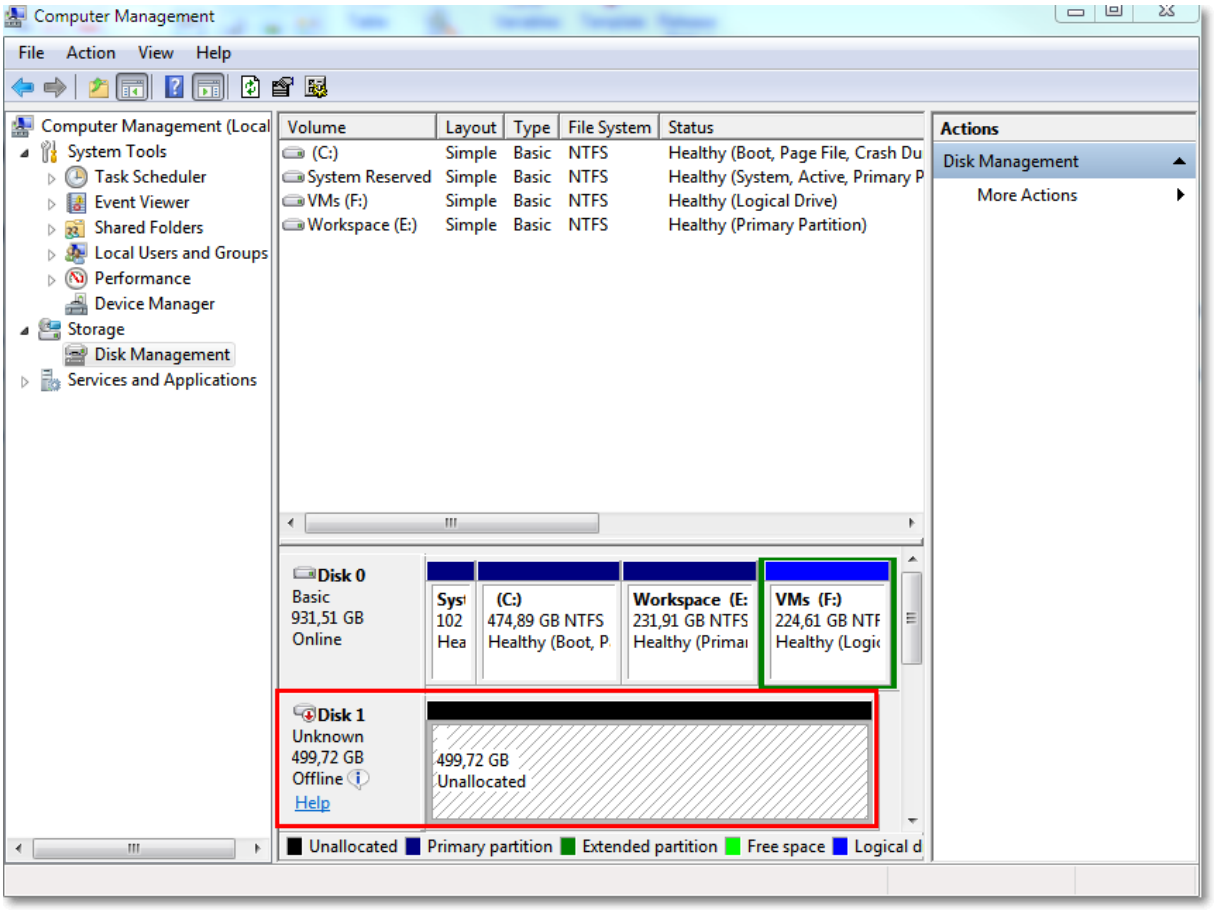
   Nota
   Para encontrar el applet **Herramientas administrativas**, es posible que necesite cambiar la vista del **Panel de control** a una diferente de **Inicio** o **Categoría**. También puede utilizar la búsqueda.

2. Si es la primera vez que ejecuta el iniciador de iSCSI, confirme que desea iniciar el servicio del iniciador de iSCSI de Microsoft.
3. En la pestaña **Destinos**, escriba el nombre de dominio completo (FQDN) o la dirección IP del dispositivo SAN de destino y, después, haga clic en **Conexión rápida**.
4. Seleccione el LUN que aloja el almacén de datos y, a continuación, haga clic en **Conectar**.
   Si no se muestra el LUN, asegúrese de que la división en zonas en el objetivo de iSCSI permite al equipo que está ejecutando el agente acceder el LUN. Debe añadir el equipo a la lista de

iniciadores de iSCSI permitidos en este destino.

5. Haga clic en **Aceptar**.

El SAN o LUN listo debería aparecer en **Gestión del disco**, tal y como se muestra en la captura de pantalla de abajo.



Uso de instantáneas de hardware SAN

Si su VMware vSphere utiliza un sistema de almacenamiento de red de área de almacenamiento (SAN) como almacén de datos, puede habilitar Agente para VMware (Windows) para utilizar instantáneas de hardware SAN al realizar una copia de seguridad.

Importante
Solo admite el almacenamiento en NetApp SAN.

¿Por qué utilizar instantáneas de hardware SAN?

El Agente para VMware necesita una instantánea de equipo virtual para crear una copia de seguridad consistente. Como el agente lee el contenido de la unidad de disco virtual de la instantánea, esta debe conservarse todo el tiempo que dure el proceso de copia de seguridad.

De forma predeterminada, el agente utiliza instantáneas de VMware nativas creadas por el servidor ESXi. Mientras se conserva la instantánea, los archivos de unidad de disco virtual se encuentran en

estado de solo lectura y el servidor escribe todos los cambios realizados en los discos en archivos delta independientes. Una vez que finaliza el proceso de copia de seguridad, el servidor elimina la instantánea, es decir, combina los archivos delta con los archivos de unidad de disco virtual.

Tanto el mantenimiento como la eliminación de la instantánea afectan al rendimiento del equipo virtual. Con unidades de disco virtuales grandes y rápidos cambios de datos, estas operaciones tardan mucho tiempo y puede degradarse el rendimiento. En casos extremos, cuando se realiza la copia de seguridad de varios equipos simultáneamente, los archivos delta crecientes prácticamente llenan el almacén de datos y hacen que todos los equipos virtuales se apaguen.

Puede reducir la utilización de recursos del hipervisor trasladando las instantáneas a la red SAN. En este caso, la secuencia de las operaciones es la siguiente:

1. El ESXi toma una instantánea de VMware al inicio del proceso de copia de seguridad para poner las unidades de disco virtuales en un estado consistente.
2. La red SAN crea una instantánea de hardware del volumen o LUN que contiene el equipo virtual y su instantánea de VMware. Esta operación normalmente tarda unos segundos.
3. El ESXi elimina la instantánea de VMware. Agente para VMware lee el contenido de la unidad de disco virtual de la instantánea de hardware SAN.

Como la instantánea de VMware solo se conserva durante unos segundos, se minimiza la degradación del rendimiento del equipo virtual.

¿Qué necesito para usar las instantáneas de hardware SAN?

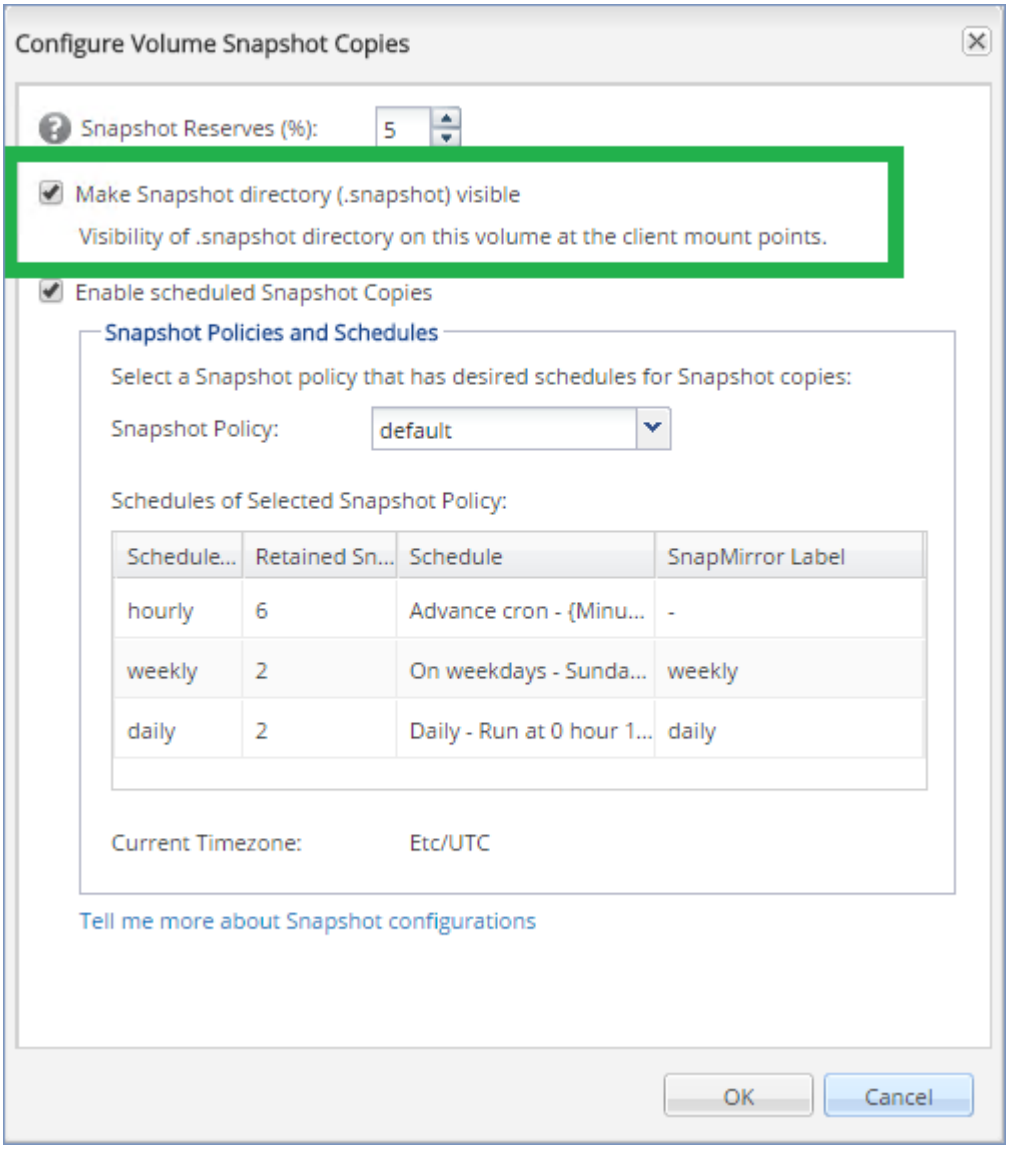
Si desea utilizar las instantáneas de hardware SAN al realizar copias de seguridad de equipos virtuales, asegúrese de que se cumplan todas las condiciones siguientes:

- El almacenamiento SAN de NetApp cumple los requisitos descritos en "Requisitos de almacenamiento NetApp SAN".
- El equipo que ejecuta Agente para VMware (Windows) está configurado como se describe en "Configurar el equipo que ejecuta Agente para VMware".
- El almacenamiento SAN está registrado en el servidor de gestión.
- [Si hay Agentes para VMware que no participaron en el anterior registro] Los equipos virtuales que residen en el almacenamiento SAN se asignan a los agentes habilitados para SAN, como se describe en "Enlace de equipos virtuales".
- La opción de copia de seguridad "Instantáneas de hardware SAN" está habilitada en las opciones de plan de protección.

Requisitos de almacenamiento NetApp SAN

- El almacenamiento SAN debe utilizarse como un almacén de datos NFS o iSCSI.
- El SAN debe ejecutar Data ONTAP 8.1 o posterior en el modo **ONTAP de datos en clúster (cDOT)**. El modo **7-mode** no es compatible.
- En el NetApp OnCommand System Manager, la casilla de verificación **Instantánea copia el directorio visible** > **Configurar** > **Make Snapshot (.snapshot)** debe estar seleccionada para el

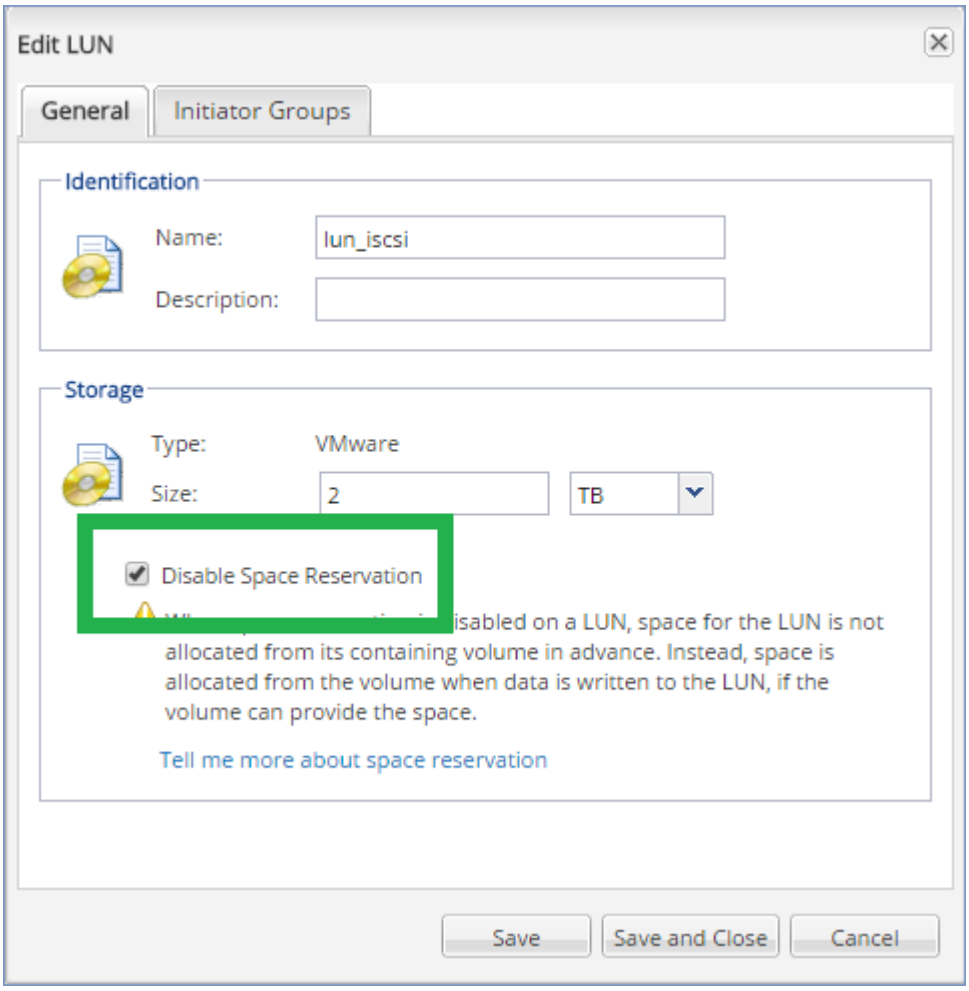
volumen en donde se ubica el almacén de datos.



- [Para almacenes de datos NFS] El acceso a recursos compartidos NFS desde los clientes Windows NFSv3 debe estar habilitado en el Equipo Virtual de Almacenamiento (SVM) que se haya especificado al crear el almacén de datos. El acceso puede habilitarse mediante el siguiente comando:

  ```
  vserver nfs modify -vserver [SVM name] -v3-ms-dos-client enable
  ```

  Para obtener más información, consulte el documento Mejores prácticas de NetApp: https://kb.netapp.com/support/s/article/ka21A0000000k89QAA/top-windows-nfsv3-0-issues-workarounds-and-best-practices
- [Para almacenes de datos iSCSI] En el NetApp OnCommand System Manager, debe estar seleccionada la casilla de verificación **Disable Space Reservation** para el iSCSI LUN en donde se ubica el almacén de datos.



Configuración del equipo con Agent para VMware

Dependiendo de si se utiliza el almacenamiento SAN como almacén de datos NFS o iSCSI, consulte la sección correspondiente a continuación.

Configuración del iniciador iSCSI

Asegúrese de que todo lo que aparece a continuación sea correcto:

- Se ha instalado el iniciador iSCSI de Microsoft.
- El tipo de inicio de servicio de iniciador iSCSI de Microsoft se ha configurado en **Automático** o **Manual**. Esto se puede realizar en el complemento **Servicios**.
- El iniciador iSCSI se ha configurado como se indica en la sección de ejemplos de "Copia de seguridad sin LAN".

Configuración del cliente NFS

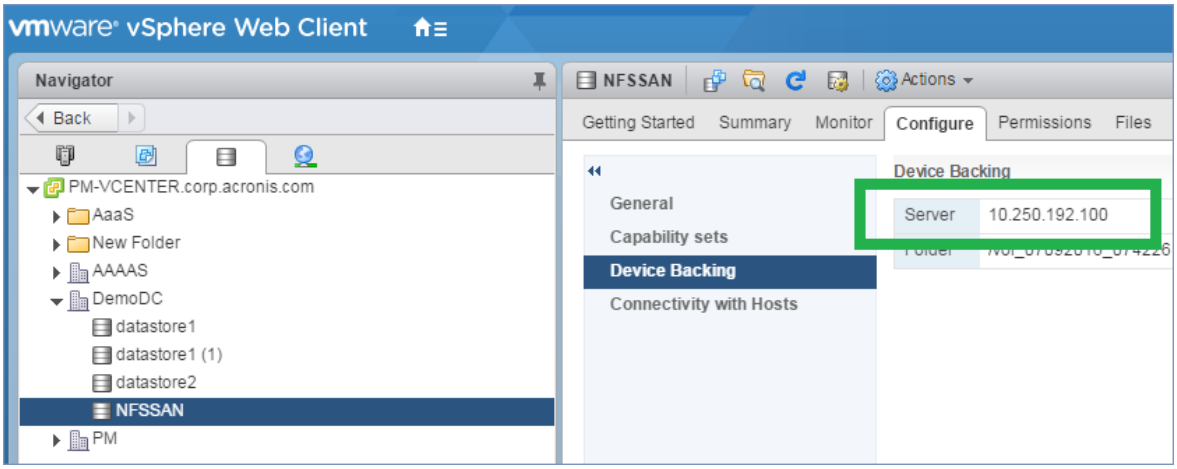
Asegúrese de que todo lo que aparece a continuación sea correcto:

- Se ha instalado **Servicios para NFS** de Microsoft (en Windows Server 2008) o **Cliente para NFS** (en Windows Server 2012 y posterior).

- El cliente NFS se ha configurado para acceso anónimo. Esto se puede realizar de la siguiente manera:
  a. Abra el Editor del registro.
  b. Busque la siguiente clave del registro: **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ClientForNFS\CurrentVersion\Default**
  c. En esta clave, cree un nuevo valor **DWORD** llamado **AnonymousUID** y configure su valor en 0.
  d. En la misma clave, cree un nuevo valor **DWORD** llamado **AnonymousGID** y configure su valor en 0.
  e. Reinicie el equipo.

Registro del almacenamiento SAN en el servidor de gestión

1. Haga clic en **Configuración**> **Almacenamiento SAN**.
2. Haga clic en **Agregar almacenamiento**.
3. [Opcional] En **Nombre**, cambie el nombre del almacenamiento.
   Este nombre se mostrará en la pestaña **Almacenamiento SAN**.
4. En **Nombre o dirección IP del servidor**, especifique el Equipo virtual de almacenamiento (SVM, también conocido como filtrador), que se especificó durante la creación del almacén de datos.
   Para encontrar la información requerida del cliente web VMware vSphere, seleccione el almacén de datos y, a continuación, haga clic en **Configurar** > **Copia de seguridad del dispositivo**. El nombre o dirección IP del servidor se muestra en el campo **Servidor**.



5. En **Nombre de usuario** y **Contraseña**, especifique las credenciales del administrador SVM.

   Importante
   La cuenta indicada debe ser un administrador local en el SVM, más que un administrador de gestión del sistema NetApp completo.

   Puede especificar un usuario nuevo o crearlo. Para crear un usuario nuevo, en el NetApp OnCommand System Manager, vaya a **Configuración** > **Seguridad** > **Usuarios** y, a continuación, cree un usuario nuevo.

6. Seleccione uno o más Agent for VMware (Windows), a los que se les concederá el permiso de lectura para el dispositivo SAN.
7. Haga clic en **Agregar**.

Utilización de un almacenamiento conectado localmente

Puede conectar un disco adicional a Agent for VMware (Virtual Appliance) para que el agente pueda realizar la copia de seguridad en este almacenamiento conectado localmente. Este enfoque elimina el tráfico de red entre el agente y la ubicación de copia de seguridad.

Un dispositivo virtual que se ejecute en el mismo servidor o clúster que los equipos virtuales de los que se ha realizado la copia de seguridad tiene acceso directo a los almacenes de datos donde residan los equipos. Esto significa que el dispositivo puede adjuntar los discos de los que se ha realizado la copia de seguridad mediante el transporte HotAdd y, por tanto, la transferencia de datos de la copia de seguridad se dirige desde un disco local a otro. Si el almacén de datos está conectado como **Disco/LUN** en lugar de **NFS**, la copia de seguridad no dependerá en ningún momento de LAN. En el caso de un almacén de datos NFS, habrá tráfico de red entre el almacén de datos y el servidor.

Utilizar un almacenamiento conectado localmente presume que el agente siempre realiza la copia de seguridad de los mismos equipos. Si múltiples agentes trabajan con vSphere y uno o más de ellos utiliza almacenamientos conectados localmente, necesita enlazar manualmente cada agente a los equipos de los que tiene que realizar la copia de seguridad. De lo contrario, si el servidor de gestión redistribuye los equipos entre los agentes, las copias de seguridad de un equipo pueden dispersarse en varios almacenamientos.

Puede añadir el almacenamiento a un agente ya en funcionamiento o cuando implemente el agente desde una plantilla OVF.

Para conectar un almacenamiento a un agente que ya está trabajando

1. En el inventario de VMware vSphere, haga clic con el botón derecho en Agent for VMware (Virtual Appliance).
2. Añada el disco al editar los ajustes del equipo virtual. El tamaño del disco deben ser de al menos 10 GB.

   Advertencia.
   Tenga cuidado al añadir un disco ya existente. Una vez creado el almacenamiento, todos los datos incluidos previamente en este disco se perderán.

3. Vaya a la consola del dispositivo virtual. El enlace **Crear almacenamiento** estará disponible en la parte inferior de la pantalla. Si no lo está, haga clic en **Actualizar**.
4. Haga clic en el enlace **Crear almacenamiento**, seleccione el disco y especifique una etiqueta para el mismo. La longitud de la etiqueta está limitada a 16 caracteres debido a las restricciones del sistema de archivos.

Para seleccionar un almacenamiento conectado localmente como el destino de la copia de seguridad

Al crear un plan de protección, en **Dónde realizar copias de seguridad**, seleccione **Carpetas locales** y, a continuación, escriba la letra correspondiente al almacenamiento conectado localmente, por ejemplo, **D:**.

Enlace de equipos virtuales

Esta sección le proporciona información general sobre cómo el servidor de gestión organiza la operación de múltiples agentes en VMware vCenter.

El algoritmo de distribución especificado a continuación funciona para dispositivos virtuales y agentes instalados en Windows.

Algoritmo de distribución

Los equipos virtuales están distribuidos uniformemente entre Agentes para VMware. Por uniformemente queremos decir que cada agente gestiona un número igual de equipos. La cantidad de espacio de almacenamiento ocupado por un equipo virtual no se cuenta.

Sin embargo, al escoger un agente para un equipo, el software intenta optimizar el rendimiento general del sistema. En particular, el software tiene en cuenta la ubicación del agente y el equipo virtual. Es preferible un agente alojado en el mismo servidor. Si no hay ningún agente en el mismo servidor, se prefiere un agente del mismo clúster.

Una vez que el equipo virtual se ha asignado a un agente, todas las copias de seguridad del equipo se delegarán a este agente.

Redistribución

La redistribución se realiza cada vez que se rompe el equilibrio establecido o, más precisamente, cuando el desequilibrio de cargas entre los agentes llega al 20 por ciento. Esto sucede cuando un equipo o un agente se añade o retira, o un equipo se migra a un servidor o clúster diferente, o si enlaza manualmente un equipo a un agente. Si ocurre esto, el servidor de gestión redistribuye los equipos utilizando el mismo algoritmo.

Por ejemplo, se da cuenta que necesita más agentes para ayudar al rendimiento y para implementar dispositivos virtuales adicionales en el clúster. El servidor de gestión asignará los equipos más adecuados al nuevo agente. La carga de los agentes anteriores se reducirá.

Cuando retira un agente del servidor de gestión, los equipos asignados al agente se distribuyen entre los agentes restantes. Sin embargo, esto no sucederá si un agente se daña o elimina manualmente de vSphere. La redistribución comenzará solo después de eliminar dicho agente de la interfaz web.

Visualización del resultado de distribución

Puede ver el resultado de la distribución automática:

- en la columna **Agente** para cada equipo virtual en la sección **Todos los dispositivos**
- en la sección **Equipos virtuales asignados** del panel **Detalles** cuando un agente está seleccionado en la sección **Configuración** > **Agentes**

Enlace manual

El enlace de Agente para VMware le permite excluir un equipo virtual de este proceso de distribución al especificar el agente que siempre debe realizar la copia de seguridad de este equipo. Se continuará manteniendo el equilibrio general, pero este equipo concreto se puede pasar a un agente diferente solo si el agente original se elimina.

Para enlazar un equipo con un agente:

1. Seleccione el equipo.
2. Haga clic en **Detalles**.
   En la sección **Agente asignado**, el software muestra el agente que actualmente gestiona el equipo seleccionado.
3. Haga clic en **Cambiar**.
4. Seleccione **Manual**.
5. Seleccione el agente al que desea enlazar el equipo.
6. Haga clic en **Guardar**.

Para desenlazar un equipo de un agente:

1. Seleccione el equipo.
2. Haga clic en **Detalles**.
   En la sección **Agente asignado**, el software muestra el agente que actualmente gestiona el equipo seleccionado.
3. Haga clic en **Cambiar**.
4. Seleccione **Automático**.
5. Haga clic en **Guardar**.

Deshabilitar la asignación automática para un agente

Puede deshabilitar la asignación automática para Agente para VMware para excluirla del proceso de distribución especificando la lista de equipos de los que debe realizar la copia de seguridad este agente. Se mantendrá el equilibrio general entre otros agentes.

La asignación automática no se puede deshabilitar para un agente si no hay otros agentes registrados o si una asignación automática está deshabilitada para el resto de agentes.

Para deshabilitar la asignación automática para un agente

1. Haga clic en **Ajustes** > **Agentes**.
2. Seleccione Agente para VMware para el cual desea deshabilitar la asignación automática.

3. Haga clic en **Detalles**.
4. Deshabilite el conmutador **Asignación automática**.

Ejemplos de uso

- El enlace manual es práctico si desea que Agente para VMware (Windows) realice la copia de seguridad de un equipo (muy grande) en particular a través del canal de fibra, mientras que los dispositivos virtuales realicen la copia de seguridad de los demás equipos.
- El enlace manual es necesario si se utilizan instantáneas de hardware SAN. Enlace Agente para VMware (Windows) para el cual las instantáneas de hardware SAN están configuradas con los equipos que residen en el almacén de datos SAN.
- Es necesario enlazar los VM a un agente si el agente tiene un almacenamiento conectado localmente.
- Deshabilitando la asignación automática es posible asegurarse de que previsiblemente la copia de seguridad de un equipo virtual se realiza según la planificación especificada. El agente que solo realiza la copia de seguridad de un VM no puede estar ocupado con la copia de seguridad de otros VM cuando llega la hora planificada.
- Deshabilitar la asignación automática es útil si existen varios servidores ESXi que están geográficamente separados. Si se deshabilita la asignación automática y luego se enlazan los VM de cada servidor al agente que se ejecuta en el mismo servidor, se puede garantizar que el agente nunca realizará copias de seguridad de ningún equipo que se ejecute en servidores ESXi remotos, lo que ahorra tráfico en la red.

Compatibilidad con migración VM

En este apartado se describe lo que puede ocurrir cuando equipos virtuales migran dentro de un entorno de vSphere, incluido cuando migran entre hosts ESXi que forman parte de un clúster vSphere.

vMotion

vMotion mueve la configuración y el estado de una equipo virtual a otro servidor mientras el disco del equipo continua estando en la misma ubicación en almacenamiento compartido.

- vMotion, de Agent for VMware (dispositivo virtual), no es compatible y está deshabilitado.
- El vMotion de un equipo virtual está deshabilitado durante la realización de una copia de seguridad. Las copias de seguridad continuarán ejecutándose cuando finalice la migración.

Storage vMotion

Storage vMotion mueve discos de equipos virtuales de un almacén de datos a otro.

- Storage vMotion de Agent for VMware (dispositivo virtual) no es compatible y está deshabilitado.
- El Storage vMotion de un equipo virtual está deshabilitado durante la realización de una copia de seguridad. Las copias de seguridad continuarán ejecutándose tras la migración.

Gestión de entornos de virtualización

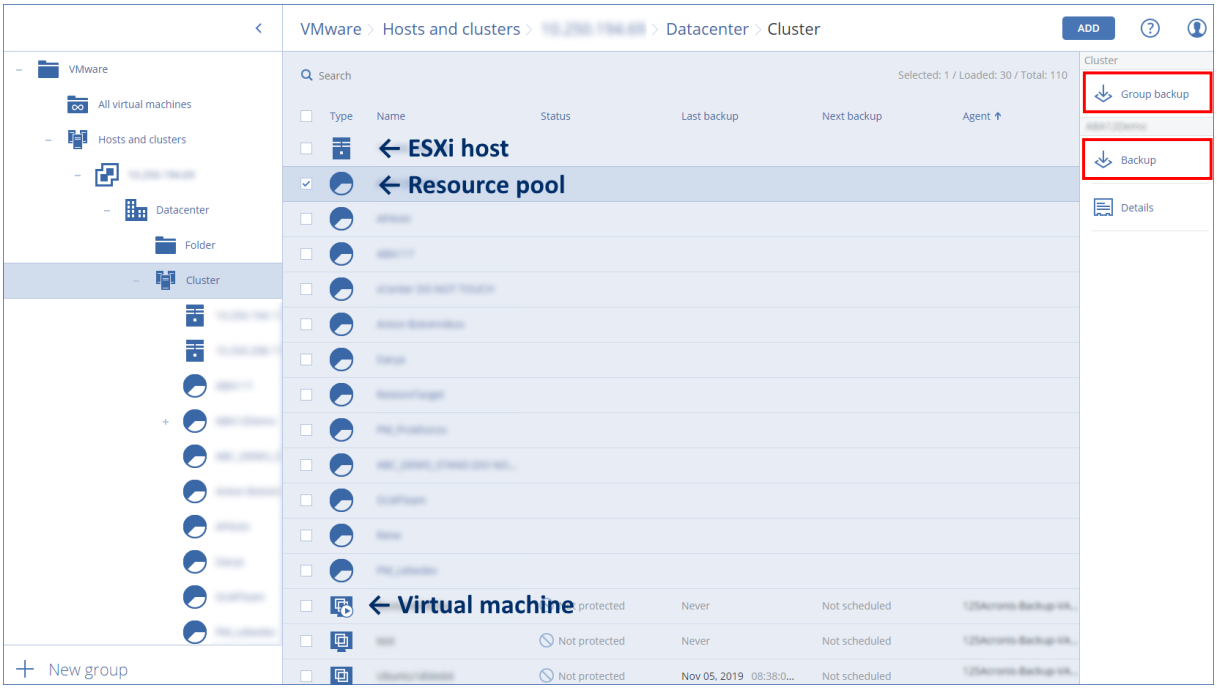
Puede visualizar los entornos de vSphere, Hyper-V y Virtuozzo en su presentación nativa. Cuando el agente correspondiente esté instalado y registrado, aparecerá la pestaña **VMware**, **Hyper-V** o **Virtuozzo** en **Dispositivos**.

En la pestaña **VMware**, puede realizar una copia de seguridad de los siguientes objetos de la infraestructura vSphere:

- Centro de datos
- Carpeta
- Clúster
- Servidor ESXi
- Grupo de recursos

Todos estos objetos de infraestructura funcionan como objeto del grupo para equipos virtuales. Cuando aplique un plan de protección a cualquiera de estos objetos de grupo, se realizará una copia de seguridad de todos los equipos virtuales incluidos en él. Puede realizar una copia de seguridad de los equipos de los grupos seleccionados al hacer clic en **Copia de seguridad**, o bien de los equipos del grupo principal en el que se incluyen los grupos seleccionados al hacer clic en **Copia de seguridad de grupo**.

Por ejemplo, ha seleccionado el clúster y, a continuación, ha seleccionado el grupo de recursos que incluye. Si hace clic en **Copia de seguridad**, se realizará una copia de seguridad de todos los equipos virtuales incluidos en el grupo de recursos seleccionado. Si hace clic en **Copia de seguridad de grupo**, se realizará una copia de seguridad de todos los equipos virtuales incluidos en el clúster.



Puede cambiar las credenciales de acceso a vCenter Server o al servidor ESXi independiente sin tener que reinstalar el agente.

Para modificar las credenciales de acceso a vCenter Server o al servidor ESXi

1. En **Dispositivos**, haga clic en **VMware**.
2. Haga clic en **Servidores y clústeres**.
3. En la lista de **Servidores y clústeres** (situada a la derecha del árbol de **Servidores y clústeres**), seleccione vCenter Server o el servidor ESXi independiente que se especificó durante la instalación del Agente para VMware.
4. Haga clic en **Detalles**.
5. En **Credenciales**, haga clic en el nombre de usuario.
6. Especifique las nuevas credenciales de acceso y, a continuación, haga clic en **Aceptar**.

Visualización del estado de la copia de seguridad en vSphere Client

Puede ver el estado de la copia de seguridad y el momento en el que se llevó a cabo la última copia de seguridad de un equipo virtual en vSphere Client.

Esta información aparece en el resumen del equipo virtual (**Resumen** > **Atributos personalizados**/**Anotaciones**/**Notas**, según el tipo de cliente y la versión de vSphere). También puede habilitar las columnas **Última copia de seguridad** y **Estado de la copia de seguridad** en la pestaña **Equipos virtuales** para cualquier host, centro de datos, carpeta, pool de recursos o todo el vCenter Server.

Para proporcionar estos atributos, el Agente para VMware debe tener los siguientes privilegios, además de los descritos en "Agente para VMware: privilegios necesarios":

- **Global** > **Gestionar atributos personalizados**
- **Global** > **Establecer atributos personalizados**

Agente para VMware: privilegios necesarios

Esta sección describe los privilegios necesarios para realizar operaciones con equipos virtuales ESXi y, además, para la implementación de dispositivos virtuales.

Nota
Las API de vStorage deben estar instaladas en el host ESXi para habilitar las copias de seguridad de máquinas virtuales. Consulte https://kb.acronis.com/content/14931.

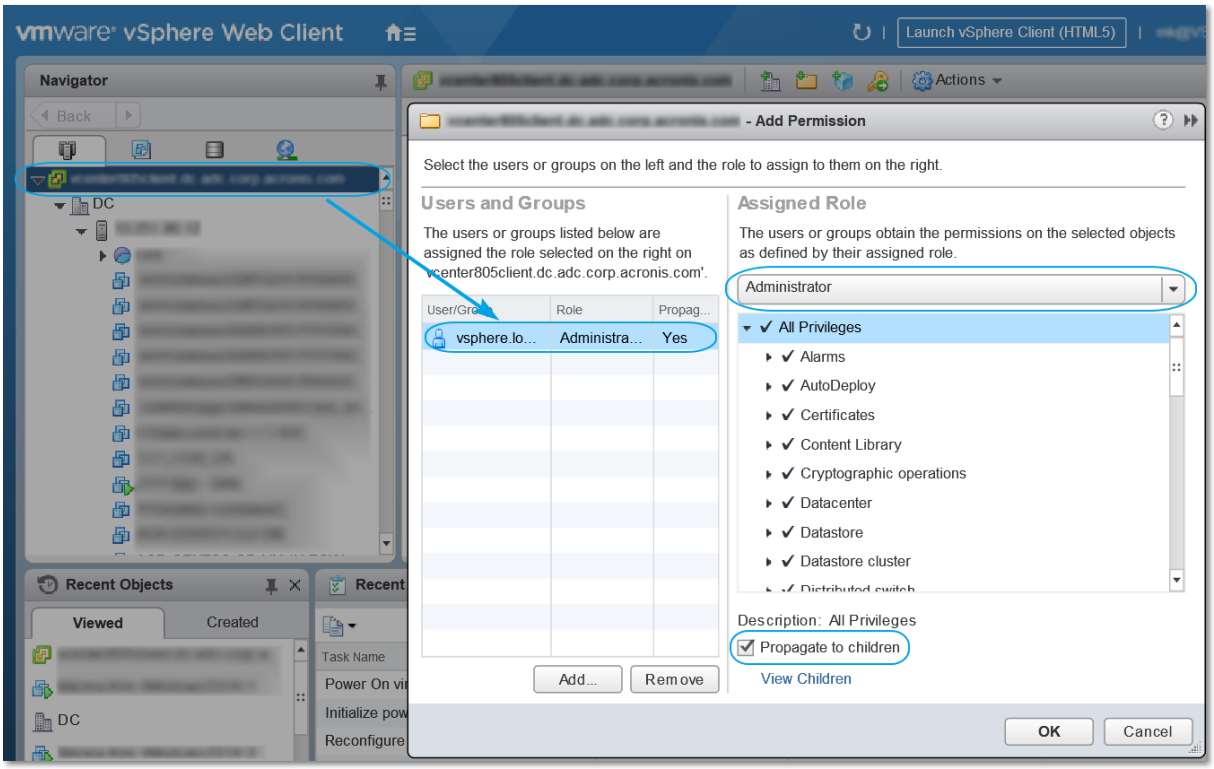
Para llevar a cabo cualquier operación con objetos de vCenter, como equipos virtuales, servidores ESXi, clústeres o vCenter, entre otros, Agente para VMware se autentica en el servidor vCenter o ESXi mediante las credenciales de vSphere proporcionadas por el usuario. La cuenta de vSphere, que usa el Agente para VMware para establecer la conexión con vSphere, debe contar con los

privilegios necesarios en todos los niveles de la infraestructura de vSphere, empezando desde el nivel de vCenter.

Indique la cuenta de vSphere con los privilegios necesarios durante la instalación o configuración de Agente para VMware. Si necesita cambiar la cuenta en un momento posterior, consulte la sección "Gestionar entornos de virtualización".

Para asignar los permisos a un usuario de vSphere en el nivel de vCenter, lleve a cabo los siguientes pasos:

1. Inicie sesión en el cliente web de vSphere.
2. Haga clic en vCenter y, a continuación, en **Añadir permiso**.
3. Seleccione o añada un nuevo usuario con el rol requerido (el rol debe incluir todos los permisos necesarios de la tabla que aparece a continuación).
4. Seleccione la opción **Propagar a secundarios**.



Objeto	Privilegio	Operación				
		Copia de seguridad de un equipo virtual	Recuperación en un nuevo equipo virtual	Recuperación en un equipo virtual existente	Ejecutar VM desde la copia de seguridad	Implementación de un dispositivo virtual
Operaciones	**Agregar disco**	+*				

criptográficas (primeros pasos con vSphere 6.5)						
	Acceso directo	+*				
Almacén de datos	**Asignar espacio**		+	+	+	+
	Examinar almacén de datos				+	+
	Configurar los almacenes de datos	+	+	+	+	+
	Operaciones con archivos de bajo nivel				+	+
Global	**Licencias**	+	+	+	+	
	Deshabilitar métodos	+	+	+		
	Habilitar métodos	+	+	+		
	Gestionar atributos personalizados	+	+	+		
	Establecer atributo personalizado	+	+	+		
Servidor > **Configuración**	**Configuración de autoarranque de VM**					+
	Configuración de partición de almacenamiento				+	
Servidor >	**Modificar**					+

Inventario	**clúster**					
Servidor > **Operaciones locales**	**Crear VM**				+	+
	Eliminar VM				+	+
	Reconfigurar VM				+	+
Red	**Asignar red**		+	+	+	+
Recurso	**Asignar equipo virtual a pool de recursos**		+	+	+	+
	Importar					+
Equipo virtual > **Configuración**	**Añadir disco existente**	+	+		+	
	Añadir disco nuevo		+	+	+	+
	Añadir o quitar dispositivo		+		+	+
	Avanzado	+	+	+		+
	Cambiar recuento de CPU		+			
	Seguimiento de cambios de disco	+		+		
	Disco arrendado	+		+		
	Memoria		+			
	Quitar disco	+	+	+	+	
	Cambiar nombre		+			
	Establecer anotación				+	

	Configuración		+	+	+	
Equipo virtual >Operaciones de huésped	**Ejecución de programa de operación de huésped**	+**				+
	Consultas de operación de huésped	+**				+
	Modificaciones de operaciones de huésped	+**				
Equipo virtual > Interacción	**Adquirir vale de control de huésped** (en vSphere 4.1 y 5.0)				+	+
	Configurar dispositivo de CD		+	+		
	Interacción de consola					+
	Gestión del sistema operativo huésped por VIX API (en vSphere 5.1 y versiones posteriores)				+	+
	Apagar			+	+	+
	Encender		+	+	+	+
Equipo virtual > Inventario	**Crear desde existente**		+	+	+	
	Crear nuevo		+	+	+	+
	Mover					+
	Registrar				+	

	Quitar		+	+	+	+
	Anular el registro				+	
Equipo virtual > **Aprovisionamiento**	**Permitir acceso a disco**		+	+	+	
	Permitir acceso a disco de solo lectura	+		+		
	Permitir descarga de equipo virtual	+	+	+	+	
Equipo virtual > **Estado** **Máquina virtual** > **Administración de instantáneas** (vSphere 6.5 y versiones posteriores)	**Crear instantánea**	+		+	+	+
	Eliminar instantánea	+		+	+	+
vApp	**Agregar equipo virtual**				+	

* Este privilegio solo es obligatorio para realizar copias de seguridad de equipos cifrados.

** Este privilegio solo es obligatorio para copias de seguridad compatibles con aplicaciones.

Copia de seguridad de equipos Hyper-V en clúster

En un clúster Hyper-V, los equipos virtuales pueden migrarse entre los nodos del clúster. Siga estas recomendaciones para configurar una copia de seguridad correcta de equipos Hyper-V en clúster:

1. Un equipo debe estar disponible para la copia de seguridad sin importar a qué nodo se migra. Para garantizar que el Agente para Hyper-V tenga acceso a un equipo en cualquier nodo, ejecute el servicio de agente en una cuenta de usuario del dominio que posea privilegios administrativos en cada uno de los nodos de clúster.

Le recomendamos que especifique dicha cuenta para el servicio del agente durante la instalación de Agente para Hyper-V.

2. Instale Agente para Hyper-V en cada nodo del clúster.
3. Registre todos los agentes en el servidor de gestión.

Alta disponibilidad de un equipo recuperado

Cuando recupera discos con copias de seguridad en un equipo virtual Hyper-V *existente*, la propiedad de alta disponibilidad del equipo se mantiene como está.

Cuando recupera discos con copias de seguridad en un equipo virtual Hyper-V *nuevo* o realiza una conversión a un equipo virtual Hyper-V dentro de un plan de protección, el equipo no tiene alta disponibilidad. Se considera un equipo de reserva y normalmente está apagado. Si necesita usar el equipo en el entorno de producción, puede configurarlo para que tenga alta disponibilidad desde el complemento **Administración del clúster de conmutación por error**.

Limitar el número total de equipos virtuales que se incluyen en la copia de seguridad al mismo tiempo

En la opción de copia de seguridad **Programación**, puede limitar el número de máquinas virtuales por plan de protección de las que se ha hecho una copia de seguridad simultáneamente.

Cuando un agente ejecuta varios planes al mismo tiempo, el número de máquinas respaldadas simultáneamente aumenta. Múltiples copias de seguridad ejecutadas por el mismo agente pueden afectar al rendimiento de la copia de seguridad y sobrecargar el host y el almacenamiento del equipo virtual. Por ello, puede configurar otra limitación, a nivel del agente.

Pasos para limitar las copias de seguridad simultáneas en el nivel del agente

Agente para VMware (Windows)

1. En el equipo con el agente, cree un nuevo documento de texto y ábralo en un editor de texto.
2. Copie y pegue las siguientes líneas en el archivo.

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_
MACHINE\SOFTWARE\Acronis\MMS\Configuration\ManagedMachine\SimultaneousBackupsLimits]
"MaxNumberOfSimultaneousBackups"=dword:00000001
```

3. Reemplace `00000001` por el valor hexadecimal del límite que desee establecer.
   Por ejemplo, `00000001` es 1 y `0000000A` es 10.
4. Guarde el documento como **limit.reg**.
5. Ejecute el archivo como administrador.
6. Confirme que desea editar el registro de Windows.

7. Reinicie el agente:
   a. En el menú **Inicio**, haga clic en **Ejecutar**.
   b. Escriba **cmd** y, a continuación, haga clic en **Aceptar**.
   c. En la línea de comandos, ejecute los siguientes comandos:

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

Agente para Hyper-V

1. En el equipo con el agente, cree un nuevo documento de texto y ábralo en un editor de texto.
2. Copie y pegue las siguientes líneas en el archivo.

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_
MACHINE\SOFTWARE\Acronis\MMS\Configuration\ManagedMachine\SimultaneousBackupsLimits]
"MaxNumberOfSimultaneousBackups"=dword:00000001
```

3. Reemplace `00000001` por el valor hexadecimal del límite que desee establecer.
   Por ejemplo, `00000001` es 1 y `0000000A` es 10.
4. Guarde el documento como **limit.reg**.
5. Ejecute el archivo como administrador.
6. Confirme que desea editar el registro de Windows.
7. Reinicie el agente:
   a. En el menú **Inicio**, haga clic en **Ejecutar**.
   b. Escriba **cmd** y, a continuación, haga clic en **Aceptar**.
   c. En la línea de comandos, ejecute los siguientes comandos:

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

Dispositivos virtuales

Este procedimiento se aplica al Agente para VMware (dispositivo virtual), el Agente para Scale Computing, el Agente para Virtuozzo Hybrid Infrastructure y el Agente para oVirt.

1. En la consola del dispositivo virtual, presione CTRL+SHIFT+F2 para abrir la interfaz de línea de comandos.
2. Abra el archivo `/etc/Acronis/MMS.config` en un editor de texto.
3. Busque la siguiente sección:

```
<key name="SimultaneousBackupsLimits">
    <value name="MaxNumberOfSimultaneousBackups" type="Tdword">"10"</value>
</key>
```

4. Reemplace `10` por el número máximo de copias de seguridad paralelas que desee establecer.
5. Guarde el archivo.
6. Reinicie el agente con el comando `reboot`.

Dispositivo VMware All-in-One (OVF)

1. Inicie sesión como usuario raíz en el dispositivo VMware All-in-One .
   Utilice la misma contraseña que para acceder a la consola web de Cyber Protect.
2. Abra el archivo `/etc/Acronis/MMS.config` en un editor de texto.
3. Busque la siguiente sección:

   ```
   <key name="SimultaneousBackupsLimits">
       <value name="MaxNumberOfSimultaneousBackups" type="Tdword">"10"</value>
   </key>
   ```

4. Reemplace `10` por el número máximo de copias de seguridad paralelas que desee establecer.
5. Guarde el archivo.
6. Reinicie el agente con el siguiente comando:

   ```
   sudo service acronis_mms restart
   ```

Agente para Virtuozzo

El Agente para Virtuozzo se incluye con el Agente para Linux.

1. Inicie sesión como usuario raíz en el equipo con el agente.
   Utilice la contraseña que usa para acceder a la consola web de Cyber Protect.
2. Abra el archivo `/etc/Acronis/MMS.config` en un editor de texto.
3. Busque la siguiente sección:

   ```
   <key name="SimultaneousBackupsLimits">
       <value name="MaxNumberOfSimultaneousBackups" type="Tdword">"10"</value>
   </key>
   ```

4. Reemplace `10` por el número máximo de copias de seguridad paralelas que desee establecer.
5. Guarde el archivo.
6. Ejecute el siguiente comando para reiniciar el agente:

   ```
   sudo service acronis_mms restart
   ```

Migración de equipos

Puede realizar la migración de un equipo recuperando su copia de seguridad en un equipo no original.

La siguiente tabla resume las opciones de migración disponibles.

Tipo de equipo incluido en la copia de seguridad	Destinos de recuperación disponibles							
	Equipo físico	**Equipo virtual ESXi**	**Equipo virtual Hyper-V**	**Equipo virtual Virtuozzo***	**Contenedor Virtuozzo***	**Equipo virtual Virtuozzo Hybrid Infrastructure***	**Equipo virtual de Scale Computing HC3**	**Equipo virtual RHV/oVirt***
Equipo físico	+	+	+	-	-	+	+	+
Equipo virtual VMware ESXi	+	+	+	-	-	+	+	+
Equipo virtual Hyper-V	+	+	+	-	-	+	+	+
Equipo virtual Virtuozzo*	+	+	+	+	-	+	+	+
Contenedor Virtuozzo*	-	-	-	-	+	-	-	-
Equipo virtual Virtuozzo Hybrid Infrastructure*	+	+	+	-	-	+	+	+
Equipo virtual de Scale Computing HC3	+	+	+	-	-	+	+	+
Equipo virtual de Red Hat Virtualization/oVirt*	+	+	+	-	-	+	+	+

* Solo disponible con el despliegue en la nube.

Para obtener instrucciones sobre cómo realizar la migración, consulte las siguientes secciones:

- Físico a virtual (P2V) – "Recuperación de un equipo físico en una máquina virtual" (p. 366)
- Virtual a virtual (V2V) – "Recuperación de una máquina virtual" (p. 369)
- Virtual a físico (V2P) – "Recuperación de una máquina virtual" (p. 369) o "Recuperar discos y volúmenes usando dispositivos de arranque" (p. 372)

Aunque es posible realizar la migración V2P en la interfaz web, se recomienda usar dispositivos de inicio en determinados casos. A veces, es posible que desee usar los dispositivos para migrar a ESXi o Hyper-V.

Los dispositivos le permiten hacer lo siguiente:

- Realice la migración P2V y V2P de un equipo Linux que contenga volúmenes lógicos (LVM). Use Agente para Linux o un dispositivo de arranque para crear la copia de seguridad y el dispositivo de arranque para la recuperación.
- Proporcionar los controladores del hardware específico que sea fundamental para la capacidad de arranque del sistema.

Equipos virtuales Windows Azure y Amazon EC2

Para realizar una copia de seguridad de un equipo virtual Windows Azure o Amazon EC2, instale un agente de protección en el equipo. La copia de seguridad y la recuperación son iguales que con un equipo físico. No obstante, el equipo se cuenta como virtual al definir las cuotas del número de equipos en una implementación en la cloud.

La diferencia con respecto a un equipo físico es que los equipos virtuales Windows Azure y Amazon EC2 no se pueden iniciar desde dispositivos de arranque. Si necesita realizar una recuperación a un equipo virtual nuevo Windows Azure o Amazon EC2, siga el procedimiento siguiente.

Para recuperar un equipo como un equipo virtual Windows Azure o Amazon EC2

1. Cree un equipo virtual nuevo desde una imagen/plantilla en Windows Azure o Amazon EC2. El equipo nuevo debe tener la misma configuración de disco que el equipo que desea recuperar.
2. Instale Agente para Windows o Agente para Linux en el equipo nuevo.
3. Recupere el equipo del que se ha realizado la copia de seguridad, como se describe en "Equipo físico". Al configurar la recuperación, seleccione el equipo nuevo como el equipo de destino.

Requisitos de red

Los agentes instalados en los equipos incluidos en la copia de seguridad deben poder comunicarse con el servidor de gestión a través de la red.

Implementación local

- Si tanto los agentes como el servidor de gestión están instalados en la nube de Azure/EC2, todos los equipos ya estarán ubicados en la misma red. No se necesitan realizar acciones adicionales.

- Si el servidor de gestión está ubicado fuera de la nube de Azure/EC2, los equipos en la nube no tendrán acceso de red a la red local donde está instalado el servidor de gestión. Para permitir que los agentes instalados en esos equipos puedan comunicarse con el servidor de gestión, se debe crear una conexión de red privada virtual (VPN) entre la red local (en instalaciones) y la red de nube (Azure/EC2). Para obtener instrucciones acerca de cómo crear la conexión VPN, consulte los artículos siguientes:

  Amazon EC2: http://docs.aws.amazon.com/es_es/AmazonVPC/latest/UserGuide/VPC_VPN.html

  Windows Azure: https://docs.microsoft.com/es-es/azure/vpn-gateway/vpn-gateway-howto-site-to-site-resource-manager-portal

Implementación en la nube

En una implementación en la nube, el servidor de gestión se ubica en uno de los centros de datos de Acronis y, por tanto, los agentes pueden acceder a él. No se necesitan realizar acciones adicionales.

Protección de SAP HANA

Puede consultar información sobre la protección de SAP HANA en otro documento disponible en https://dl.managed-protection.com/u/pdf/AcronisCyberProtect_15_SAP_HANA_whitepaper_es-ES.pdf.

Protección antimalware y web

Con la protección antimalware de Cyber Protect obtendrá los siguientes beneficios:

- Protección de calidad en todas las fases: proactivas, activas y reactivas.
- Cuatro tecnologías antimalware diferentes incluidas para proporcionar lo mejor de la protección de varias capas.
- Gestión de Microsoft Security Essentials y del antivirus Windows Defender.

Protección antivirus y antimalware

El módulo de protección antivirus y antimalware le permite proteger a sus equipos Windows y macOS de todas las amenazas de malware recientes. Tenga en cuenta que la funcionalidad Active Protection que forma parte de la protección antimalware no es compatible con los equipos macOS. Consulte la lista completa de características antimalware compatibles: Funciones compatibles con el sistema operativo.

Acronis Cyber Protect es compatible con el centro de protección de Windows y viene registrado en él.

Si su equipo ya está protegido con una solución antivirus de terceros en el momento en que se aplica en el equipo el módulo de protección antimalware y antivirus, el sistema generará una alerta y detendrá la protección en tiempo real para evitar posibles problemas relacionados con el rendimiento y la compatibilidad. Tendrá que deshabilitar o desinstalar la solución antivirus de terceros para habilitar una protección antimalware y antivirus Acronis Cyber Protect que funcione perfectamente.

Tiene disponibles las siguientes capacidades antimalware:

- Detección de malware en archivos en los modos de protección en tiempo real y bajo demanda (para Windows y macOS)
- Detección de comportamientos maliciosos en los procesos (para Windows)
- Bloqueo de acceso a URL maliciosas (para Windows)
- Puesta en cuarentena de archivos peligrosos
- Inclusión de aplicaciones corporativas de confianza en la lista blanca

Con el módulo de protección antivirus y antimalware se pueden llevar a cabo dos tipos de análisis:

- Análisis de la protección en tiempo real
- Análisis de malware bajo demanda

Análisis de la protección en tiempo real

La protección en tiempo real comprueba todos los archivos que se van a ejecutar o abrir en un equipo para evitar las amenazas de malware.

Puede escoger uno de los siguientes tipos de análisis:

- La detección en acceso es aquella en la que el programa antimalware se ejecuta en segundo plano, y analiza de forma activa y constante su equipo en busca de virus y otras amenazas maliciosas. Además, se lleva a cabo siempre que el sistema esté encendido. En ambos casos, el malware se detectará cuando se ejecute un archivo y durante distintas operaciones con el mismo, por ejemplo, al abrirlo para su lectura o modificación.
- La detección en ejecución significa que los archivos ejecutables solo se escanean en el momento de su ejecución para garantizar que estén limpios y que no causarán ningún daño al equipo o a los datos. No se detectará la copia de un archivo infectado.

Análisis de malware bajo demanda

El análisis antimalware se lleva a cabo según una planificación.

Puede comprobar los resultados del análisis antimalware en **Panel de control** > **Información general** > widget Elementos afectados recientemente.

Ajustes de la protección antivirus y antimalware

Para obtener más información sobre cómo crear un plan de protección con el módulo de protección antimalware y antivirus, consulte "Creación de un plan de protección".

Se pueden establecer los siguientes ajustes en el módulo de protección antivirus y antimalware.

Active Protection

Active Protection protege el sistema del ransomware y del malware de minado de criptomonedas. El ransomware cifra los archivos y pide un rescate para obtener la clave de encriptación. El malware de criptominado lleva a cabo cálculos matemáticos en segundo plano. De esta manera, roba potencia de procesamiento y tráfico de red.

En las ediciones Cyber Backup de Acronis Cyber Protect, Active Protection es un módulo independiente del plan de protección. Por lo tanto, se puede configurar de forma independiente y aplicar a distintos dispositivos o grupos de dispositivos. En las ediciones Protect de Acronis Cyber Protect, Active Protection es parte del módulo de protección antivirus y antimalware.

Active Protection está disponible para los equipos que ejecutan los siguientes sistemas operativos:

- Sistemas operativos de escritorio: Windows 7 Service Pack 1 y posteriores
  En equipos que ejecutan Windows 7, asegúrese de que está instalada la actualización para Windows 7 (KB2533623).
- Sistemas operativos de servidor: Windows Server 2008 R2 y posterior.

El Agente para Windows debe instalarse en el equipo.

Cómo funciona

Active Protection controla los procesos que se ejecutan en el equipo protegido. Si el proceso de un tercero intenta cifrar algún archivo o minar criptomonedas, Active Protection genera una alerta y lleva a cabo otras acciones, si así se ha especificado en la configuración.

Además, Active Protection evita los cambios no autorizados en los procesos propios del software de copia de seguridad, los archivos de registro, los archivos ejecutables y de configuración y las copias de seguridad que se encuentran en las carpetas locales.

Para identificar los procesos maliciosos, Active Protection utiliza la heurística basada en el comportamiento. Active Protection compara la cadena de acciones realizadas por un proceso con las cadenas de eventos registradas en la base de datos de patrones de conducta maliciosos. Este enfoque permite a Active Protection detectar malware nuevo identificando su comportamiento típico.

Configuración predeterminada: **Habilitado**.

Configuración de Active Protection

En **Acción sobre la detección**, seleccione la acción que el software deberá realizar al detectar una actividad de ransomware y, a continuación, haga clic en **Realizado**.

Puede seleccionar una de las siguientes opciones:

- **Solo notificar**
  El software generará una alerta sobre el proceso.
- **Detener el proceso**
  El software generará una alerta y detendrá el proceso.
- **Revertir usando la caché**
  El software generará una alerta, detendrá el proceso y revertirá los cambios de los archivos usando la caché de servicios.

Configuración predeterminada: **Revertir usando la caché**.

Protección de carpetas de red

La opción **Proteger carpetas de red asignadas como dispositivos locales** define si la protección antimalware y antivirus protege las carpetas de la red que están asignadas como dispositivos locales de los procesos maliciosos locales.

Esta opción se aplica a carpetas compartidas por protocolos SMB o NFS.

Si un archivo se encontraba al principio en un dispositivo asignado, no se puede guardar en la ubicación original cuando se extraiga de la caché mediante la acción **Revertir usando la caché**. En su lugar, se guardará en la carpeta especificada en la configuración de esta opción. La carpeta predeterminada es **C:\ProgramData\Acronis\Restored Network Files**. Si esta carpeta no existe,

se creará. Si quiere cambiar la ruta, especifique una carpeta local. No se admiten carpetas de red, ni siquiera las de dispositivos asignados.

Configuración predeterminada: **Habilitado**.

Protección del servidor

Esta opción define si la protección antimalware y antivirus protege las carpetas de la red que comparte de conexiones entrantes externas de otros servidores de la red que puedan suponer amenazas.

Configuración predeterminada: **Deshabilitado**.

Configuración de confianza y conexiones bloqueadas

En la pestaña **De confianza**, puede especificar las conexiones que tienen permitido modificar cualquier dato. Debe definir el nombre de usuario y la dirección IP.

En la pestaña **Bloqueado**, puede especificar las conexiones que no podrán modificar ningún dato. Debe definir el nombre de usuario y la dirección IP.

Autoprotección

Autoprotección evita los cambios no autorizados en los procesos propios del software, los archivos de registro, los archivos ejecutables y de configuración, Secure Zone y las copias de seguridad que se encuentran en las carpetas locales. No recomendamos deshabilitar esta función.

Configuración predeterminada: **Habilitado**.

Permitir que procesos específicos modifiquen las copias de seguridad

La opción **Permitir que procesos específicos modifiquen las copias de seguridad** es efectiva cuando está habilitada la opción **Autoprotección**.

Se aplica a los archivos cuyas extensiones son .tibx, .tib o .tia y que se encuentran en carpetas locales.

Con esta opción, puede especificar los procesos que se siguen para modificar los archivos incluidos en la copia de seguridad, aunque estén protegidos por la autoprotección. Esto es útil, por ejemplo, si elimina archivos de copia de seguridad o los traslada a una ubicación diferente con una secuencia de comandos.

Si esta opción está deshabilitada, solo los procesos firmados por el proveedor del software de la copia de seguridad pueden modificar los archivos incluidos en ella. Así, el software puede aplicar reglas de retención y eliminar copias de seguridad cuando un usuario lo solicite desde la interfaz web. Otros procesos no podrán llevar a cabo modificaciones en ellas, sin importar si son sospechosos o no.

Si esta opción está habilitada, puede permitir que otros procesos modifiquen las copias de seguridad. Especifique la ruta completa al ejecutable del proceso, empezando por la letra de unidad de disco.

Configuración predeterminada: **Deshabilitado**.

Detección del proceso de criptominería

Esta opción define si la protección antivirus y antimalware detecta posibles casos de malware de criptominado.

El malware de criptominado afecta al rendimiento de aplicaciones de utilidad, aumenta las facturas de la electricidad, puede provocar que el sistema falle e, incluso, dañar el hardware debido a su explotación. Le recomendamos que añada el malware de criptominería a la lista de procesos **peligrosos** para evitar que se ejecute.

Configuración predeterminada: **Habilitado**.

Configuración de detección de procesos de criptominería

Seleccione la acción que el software deberá realizar al detectar una actividad de criptominería y, a continuación, haga clic en **Realizado**. Puede seleccionar una de las siguientes opciones:

- **Solo notificar**
  El software genera una alerta del proceso sospechoso de actividad de criptominería.
- **Detener el proceso**
  El software genera una alerta y detiene el proceso sospechoso de actividad de criptominería.

Configuración predeterminada: **Detener el proceso**.

Cuarentena

La carpeta Cuarentena sirve para conservar los archivos sospechosos (posiblemente infectados) o potencialmente peligrosos en un lugar aislado.

Eliminar archivos en cuarentena después de: define el periodo en días tras el que se eliminarán los archivos que están puestos en cuarentena.

Configuración predeterminada: **30 días**.

Detección del comportamiento

Acronis Cyber Protect protege su sistema con heurística del comportamiento para identificar procesos maliciosos: compara la cadena de acciones realizadas por un proceso con las cadenas de acciones registradas en la base de datos de patrones de conducta maliciosos. De esta forma, el nuevo malware se detecta por su comportamiento típico.

Configuración predeterminada: **Habilitado**.

Configuración de la detección del comportamiento

En **Acción sobre la detección**, seleccione la acción que el software deberá realizar al detectar una actividad de malware y, a continuación, haga clic en **Realizado**.

Puede seleccionar una de las siguientes opciones:

- **Solo notificar**
  El software generará una alerta del proceso sospechoso de actividad de malware.
- **Detener el proceso**
  El software generará una alerta y detendrá el proceso sospechoso de actividad de malware.
- **Cuarentena**
  El software generará una alerta, detiene el proceso y traslada el archivo ejecutable a la carpeta de cuarentena.

Configuración predeterminada: **Cuarentena**.

Protección en tiempo real

La **protección en tiempo real** comprueba de forma constante el sistema de su equipo en busca de virus y otras amenazas mientras el sistema esté encendido.

Configuración predeterminada: **Habilitado**.

Configuración de la acción sobre la detección para la protección en tiempo real

En **Acción sobre la detección**, seleccione la acción que el software deberá realizar al detectar un virus u otra amenaza maliciosa y, a continuación, haga clic en **Realizado**.

Puede seleccionar una de las siguientes opciones:

- **Bloquear y notificar**
  El software bloquea el proceso y genera una alerta del proceso sospechoso de actividades de malware.
- **Cuarentena**
  El software genera una alerta, detiene el proceso y traslada el archivo ejecutable a la carpeta de cuarentena.

Configuración predeterminada: **Cuarentena**.

Configuración del modo de análisis para la protección en tiempo real

En el **Modo de análisis**, seleccione la acción que el software deberá realizar al detectar un virus u otra amenaza maliciosa y, a continuación, haga clic en **Realizado**.

Puede seleccionar una de las siguientes opciones:

- **Análisis en acceso**: supervisa todas las actividades del sistema y analiza automáticamente los archivos cuando se accede a ellos para su lectura o escritura, o cuando se inicia un programa.

- **Análisis en ejecución**: escanea de forma automática archivos ejecutables únicamente cuando se inician para garantizar que estén limpios y que no causarán ningún daño al equipo o a los datos.

Configuración predeterminada: **En acceso inteligente**.

Planificar análisis

Puede definir la planificación según la cual se comprobará si hay malware en su equipo. Para ello, habilite la configuración **Planificar análisis**.

Acción sobre la detección:

- **Cuarentena**
  El software genera una alerta y traslada el archivo ejecutable a la carpeta de cuarentena.
- **Solo notificar**
  El software genera una alerta del proceso sospechoso de ser malware.

Configuración predeterminada: **Cuarentena**.

Tipo de análisis:

- **Completo**
  El análisis completo tarda mucho tiempo en terminar en comparación con el análisis rápido porque se comprueban todos los archivos.
- **Rápido**
  El análisis rápido solo comprueba las zonas comunes en las que suele residir el malware en el equipo.
- **Personalizado**
  El análisis personalizado comprueba los archivos y las carpetas que seleccionó el administrador para el plan de protección.

Puede planificar los tres análisis, **Rápido**, **Completo** y **Personalizado**, dentro de un único plan de protección.

Configuración predeterminada:

- Se ha programado el escaneado **Rápido** y **Completo**.
- El análisis **Personalizado** está deshabilitado de forma predeterminada.

Planifique la ejecución de tareas con los siguientes eventos:

- **Planificar por tiempo**: la tarea se ejecutará según el tiempo especificado.
- **Cuando el usuario inicia sesión en el sistema**: de forma predeterminada, el inicio de sesión de cualquier usuario iniciará la tarea. Puede modificar esta configuración para que únicamente una cuenta de usuario concreta pueda activar la tarea.
- **Cuando el usuario cierra sesión en el sistema**: de forma predeterminada, cuando cualquier usuario cierre sesión se iniciará la tarea. Puede modificar esta configuración para que únicamente una cuenta de usuario concreta pueda activar la tarea.

Nota
La tarea no se ejecutará al apagarse el sistema. Apagar y cerrar sesión son dos acciones diferentes de la configuración de la programación.

- **Al iniciarse el sistema**: la tarea se ejecutará cuando el sistema operativo se inicie.
- **Al apagarse el sistema**: la tarea se ejecutará cuando el sistema operativo se apague.

Configuración predeterminada: **Planificar por hora**.

Tipo de planificación:

- **Mensualmente** : seleccione los meses y las semanas o días del mes en los que se ejecutará la tarea.
- **Diariamente** : seleccione los días de la semana en los que se ejecutará la tarea.
- **Cada hora**: seleccione los días de la semana, el número de repeticiones y el intervalo de tiempo en los que se ejecutará la tarea.

Configuración predeterminada: **Diariamente**.

Iniciar a las : seleccione la hora exacta a la que se ejecutará la tarea.

Ejecutar dentro de un intervalo de fechas: Establezca un rango en el que la planificación configurada sea efectiva.

Condiciones de inicio: defina todas las condiciones que se deben cumplir de forma simultánea para que se ejecute la tarea.

Las condiciones de inicio para el análisis antimalware son similares a las de inicio del módulo de copia de seguridad que se describen en "Condiciones de inicio" (p. 289). Puede definir las siguientes condiciones de inicio adicionales:

- **Distribuir las horas de inicio de la tarea en un período de tiempo**: esta opción le permite establecer el plazo de tiempo de la tarea para evitar cuellos de botella en la red. Puede especificar el retraso en horas o minutos. Por ejemplo, si la hora de inicio predeterminada son las 10:00 y el retraso es de 60 minutos, la tarea empezará entre las 10:00 y las 11:00.
- **Si el equipo está apagado, ejecutar las tareas perdidas al iniciar el equipo**
- **Evitar el modo de suspensión o hibernación durante la ejecución de una tarea**: esta opción solo se aplica en equipos que ejecuten Windows.
- **Si no se cumplen las condiciones de inicio, ejecutar la tarea de todos modos después de**: especifique el periodo tras el que se ejecutará la tarea, sin importar el resto de las condiciones de inicio.

Analizar únicamente archivos nuevos y modificados: solo se analizarán los archivos que se hayan creado recientemente y los que se hayan modificado.

Configuración predeterminada: **Habilitado**.

Al planificar un **Análisis completo**, tiene dos opciones adicionales:

- **Analizar archivos del archivo comprimido**
  Configuración predeterminada: **Habilitado**.
  - **Máxima profundidad de recursión**
    Número de niveles de archivos incrustados que se pueden analizar. Por ejemplo, documento MIME > archivo zip > archivo comprimido de Office > contenido del documento.
    Configuración predeterminada: **16**.
  - **Tamaño máx.**
    Tamaño máximo de los archivos de un archivo comprimido que se vaya a escanear.
    Configuración predeterminada: **Ilimitada**.
- **Analizar unidades extraíbles**
  Configuración predeterminada: **Deshabilitado**.
  - **Unidades de red asignadas (remotas)**
  - **Dispositivos de almacenamiento USB** (como unidades flash y discos duros externos)
  - **CD/DVD**

Exclusiones

Para minimizar los recursos usados por el análisis heurístico y para eliminar los llamados falsos positivos, cuando un programa de confianza se considera ransomware, puede definir la configuración siguiente:

En la pestaña **De confianza**, puede especificar:

- Los procesos que nunca se considerarán malware. Los procesos firmados por Microsoft siempre son de confianza.
- Las carpetas en las que no se controlarán los cambios de archivos.
- Los archivos y las carpetas en las que no se realizarán los análisis planificados.

En la pestaña **Bloqueado**, puede especificar:

- Los procesos que se bloquearán siempre. Estos procesos no podrán iniciarse mientras Active Protection esté habilitado en el equipo.
- Las carpetas en las que se bloqueará cualquier proceso.

Especifique la ruta completa al ejecutable del proceso, empezando por la letra de unidad de disco. Por ejemplo: `C:\Windows\Temp\er76s7sdkh.exe`.

Para especificar carpetas, puede utilizar los caracteres comodín * y ?. El asterisco (*) sustituye a cero o más caracteres. El signo de pregunta (?) sustituye exactamente un carácter. No pueden usarse variables de entorno, como `%AppData%`.

Configuración predeterminada: no se define ninguna exclusión de forma predeterminada.

Filtrado de URL

Consulte Filtrado de URL para obtener una descripción detallada.

Active Protection

En las ediciones Cyber Backup de Acronis Cyber Protect, Active Protection es un módulo independiente del plan de protección. Este módulo tiene la siguiente configuración:

- Acción sobre la detección
- Autoprotección
- Protección de carpetas de red
- Protección del servidor
- Detección del proceso de criptominería
- Exclusiones

En las ediciones Protect de Acronis Cyber Protect, Active Protection es parte del módulo de protección antivirus y antimalware.

Active Protection está disponible para los equipos que ejecutan los siguientes sistemas operativos:

- Sistemas operativos de escritorio: Windows 7 Service Pack 1 y posteriores
  En equipos que ejecutan Windows 7, asegúrese de que está instalada la actualización para Windows 7 (KB2533623).
- Sistemas operativos de servidor: Windows Server 2008 R2 y posterior.

El Agente para Windows debe instalarse en el equipo.

Para obtener más información sobre Active Protection y su configuración, consulte "Ajustes de la protección antivirus y antimalware" (p. 573).

Antivirus Windows Defender

El antivirus Windows Defender es un componente antimalware integrado de Microsoft Windows que se empezó a ofrecer en Windows 8.

Con el módulo Antivirus Windows Defender, puede configurar la directiva de seguridad del antivirus Windows Defender y realizar un seguimiento de su estado a través de la consola web de Cyber Protect.

Este módulo se aplica a equipos en los que esté instalado el antivirus Windows Defender.

Planificar análisis

Especifique la planificación para el análisis planificado.

Modo de análisis:

- **Completa**: comprobación completa de todos los archivos y las carpetas, además de los elementos analizados en el análisis rápido. Se necesitan más recursos del equipo que los

empleados para el análisis rápido.

- **Rápido**: comprobación rápida de los procesos y las carpetas de la memoria en los que se suele encontrar malware. Se requieren menos recursos del equipo.

Defina el día de la semana y la hora en que se llevará a cabo el análisis.

Análisis rápido diario: sirve para definir el momento en que tendrá lugar el análisis diario rápido.

Puede establecer las siguientes opciones en función de sus necesidades:

Iniciar el análisis planificado cuando el equipo está encendido, pero no en uso

Buscar las definiciones de virus y software espía más recientes antes de ejecutar un análisis planificado

Limitar el uso de la CPU durante el análisis a

Para obtener más información sobre la configuración de la planificación del antivirus Windows Defender, consulte https://docs.microsoft.com/en-us/sccm/protect/deploy-use/endpoint-antimalware-policies#scheduled-scans-settings.

Acciones predeterminadas

Defina las acciones predeterminadas que se van a llevar a cabo para las amenazas detectadas con distintos niveles de gravedad:

- **Limpiar**: limpiar el malware detectado en un equipo.
- **Cuarentena**: poner en cuarentena el malware detectado en la carpeta Cuarentena, pero no eliminarlo.
- **Eliminar**: eliminar el malware detectado de un equipo.
- **Permitir**: no eliminar ni poner en cuarentena el malware detectado.
- **Definido por el usuario**: se pedirá a un usuario que especifique la acción que se va llevar a cabo con el malware detectado.
- **Sin acción**: no se llevará a cabo ninguna acción.
- **Bloquear**: bloquear el malware detectado.

Para obtener más información sobre la configuración de las acciones por defecto del antivirus Windows Defender, consulte https://docs.microsoft.com/en-us/sccm/protect/deploy-use/endpoint-antimalware-policies#default-actions-settings.

Protección en tiempo real

Habilite la **protección en tiempo real** para detectar malware e impedir que se instale o se ejecute en los equipos.

Analizar todas las descargas: si esta opción está seleccionada, se analizan todos los adjuntos y archivos descargados.

Habilitar supervisión del comportamiento: si esta opción está seleccionada, se habilitará la supervisión del comportamiento.

Analizar archivos de red: si esta opción está seleccionada, se analizarán los archivos de red.

Permitir análisis completo de los dispositivos de red asignados: si esta opción está seleccionada, se analizarán por completo los dispositivos de red asignados.

Permitir análisis del correo electrónico: si esta opción está habilitada, el motor analizará los archivos del correo y de los buzones de correo en función de su formato específico con el fin de analizar los archivos adjuntos y el cuerpo de los correos.

Para obtener más información sobre la configuración de la protección en tiempo real del antivirus Windows Defender, consulte https://docs.microsoft.com/en-us/sccm/protect/deploy-use/endpoint-antimalware-policies#real-time-protection-settings.

Avanzado

Especifique la configuración de análisis avanzado:

- **Analizar archivos del archivo comprimido**: incluye archivos comprimidos como archivos .zip o .rar en el análisis.
- **Analizar unidades extraíbles**: analiza unidades extraíbles durante los análisis completos.
- **Crear un punto de restauración del sistema**: hay ocasiones en las que una entrada de registro o un archivo importante se elimina como "falso positivo". Con esta opción podrá restaurar el sistema desde un punto de recuperación.
- **Eliminar archivos en cuarentena después de**: define el periodo tras el que se eliminarán los archivos que están puestos en cuarentena.
- **Enviar muestras de archivos automáticamente cuando se requiere un análisis más detallado:**
  - **Indicar siempre**: se le pedirá su confirmación antes de enviar un archivo.
  - **Enviar muestras seguras automáticamente**: se enviarán automáticamente la mayoría de las muestras, excepto los archivos que puedan contener información personal. Esos archivos requerirán una confirmación adicional.
  - **Enviar todas las muestras automáticamente**: se enviarán todas las muestras automáticamente.
- **Deshabilitar interfaz del antivirus Windows Defender**: si se selecciona esta opción, no estará disponible la interfaz de usuario del antivirus Windows defender para un usuario. Puede gestionar las directivas del antivirus Windows Defender a través de la consola web de Cyber Protect.
- **MAPS (Microsoft Active Protection Service)**: comunidad en línea que la ayuda a decidir cómo responder a posibles amenazas.
  - **No quiero unirme a MAPS**: no se enviará ninguna información a Microsoft sobre el software que se haya detectado.

- **Afiliación básica**: se enviará información básica a Microsoft sobre el software que se haya detectado.
- **Afiliación avanzada**: se enviará información más detallada a Microsoft sobre el software que se haya detectado.

  Para obtener más información, consulte https://www.microsoft.com/security/blog/2015/01/14/maps-in-the-cloud-how-can-it-help-your-enterprise.

Para obtener más información sobre la configuración avanzada del antivirus Windows Defender, consulte https://docs.microsoft.com/en-us/sccm/protect/deploy-use/endpoint-antimalware-policies#advanced-settings.

Exclusiones

Puede definir que se excluyan del análisis los siguientes archivos y carpetas:

- **Procesos**: cuando añade un proceso, cualquier archivo en que el proceso lea o escriba quedará excluido del análisis. Tiene que definir una ruta completa al archivo ejecutable del proceso.
- **Archivos y carpetas**: los archivos y las carpetas especificados excederán del análisis. Tiene que definir una ruta completa a una carpeta o un archivo, o bien definir la extensión del archivo.

Para obtener más información sobre la configuración de exclusiones del antivirus Windows Defender, consulte https://docs.microsoft.com/en-us/sccm/protect/deploy-use/endpoint-antimalware-policies#exclusion-settings.

Microsoft Security Essentials

Microsoft Security Essentials es un componente antimalware integrado de Microsoft Windows que se empezó a ofrecer con Windows en versiones superiores a la 8.

Con el módulo Antivirus Microsoft Security Essentials, puede configurar la directiva de seguridad de Microsoft Security Essentials y realizar un seguimiento de su estado a través de la consola web de Cyber Protect.

Este módulo se aplica a equipos en los que esté instalado Microsoft Security Essentials.

La configuración de Microsoft Security Essentials es prácticamente la misma que la del antivirus Microsoft Windows Defender. Sin embargo, no cuenta con ajustes relacionados con la protección en tiempo real ni se pueden definir exclusiones a través de la consola web Cyber Protect.

Filtrado de URL

El malware lo suelen distribuir sitios infectados o maliciosos mediante el método de infección conocido como Drive-by download. El filtrado de URL le permite proteger los equipos de amenazas como el malware o la suplantación de identidad que procedan de Internet. Puede bloquear el acceso a los sitios web en los que pueda haber contenido malicioso.

Con el filtrado de URL también puede controlar el uso de los sitios web para que cumplan con las regulaciones externas y las directivas internas de la empresa. Puede configurar diferentes políticas de acceso para más de 40 categorías de sitio web.

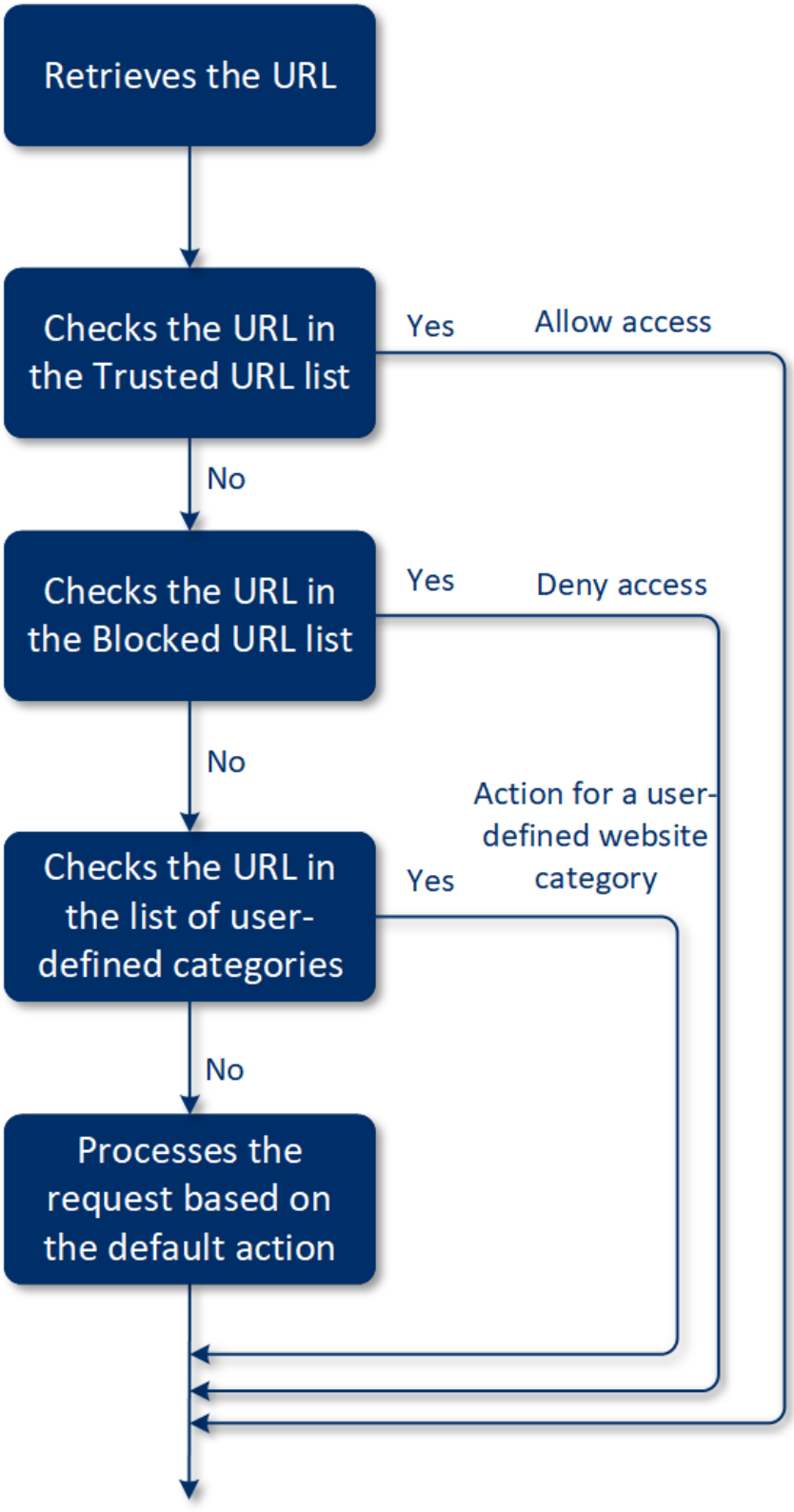
Actualmente las conexiones HTTP y HTTPS de los equipos Windows las comprueba el agente de protección.

La característica Filtrado de URL requiere una conexión a Internet para funcionar.

Nota
Pueden surgir conflictos si se utiliza el filtrado de URL al mismo tiempo que soluciones antivirus de terceros que también utilicen funciones de filtrado de URL. Puede determinar el estado de otras soluciones antivirus instaladas mediante el Centro de seguridad de Windows.
Si se produce un problema de compatibilidad o rendimiento, desinstale la solución de terceros o deshabilite el módulo de filtrado de URL en sus planes de protección.

Cómo funciona

Un usuario sigue un enlace o introduce una URL en la barra de direcciones de un navegador. El interceptor obtiene la URL y la envía al agente de protección. El agente de protección analiza la URL, comprueba la base de datos y devuelve un veredicto al interceptor. Si la URL está prohibida, el interceptor bloquea el acceso a la misma y notifica al usuario que no se le permite ver este contenido.



Pasos para configurar el filtrado de URL

1. Cree un plan de protección con el módulo Filtrado de URL habilitado.
2. Configure los ajustes del filtrado de URL (consulte la información que aparece a continuación).

3. Asigne el plan de protección a los equipos que desee.

Para comprobar que direcciones URL se han bloqueado, vaya a **Panel de control** > **Alertas**.

Ajustes del filtrado de URL

Para el módulo de filtrado de URL se pueden configurar los siguientes ajustes:

Acceso a sitio web malicioso

Especifique qué acción se llevará a cabo cuando un usuario intente abrir un sitio web malicioso:

- **Bloquear** : Se bloqueará el acceso al sitio web malicioso y se generará una alerta.
- **Preguntar siempre al usuario**: Se le preguntará al usuario si continuar al sitio web o volver.

Categorías que se pueden filtrar

Hay 44 categorías de sitio web cuya política de acceso puede configurar: De forma predeterminada, se permite el acceso a los sitios web de todas las categorías.

	Categoría del sitio web	Descripción
1	**Publicidad**	En esta categoría se incluyen aquellos dominios cuyo objetivo principal es ofrecer anuncios.
2	**Tableros de mensajes**	En esta categoría se incluyen los foros, los grupos de discusión y los sitios web de pregunta-respuesta. Esta categoría no cubre las secciones específicas de los sitios web empresariales donde los clientes hacen preguntas.
3	**Sitios web personales**	En esta categoría se incluyen los sitios web personales y todos los tipos de blogs: individuales, de varias personas e incluso de empresas. Un blog es un diario publicado en la World Wide Web. Consta de entradas (“publicaciones”) que normalmente se muestran en orden cronológico inverso, de modo que las más recientes aparecen primero.
4	**Sitios web empresariales/corporativos**	Esta categoría es amplia porque abarca los sitios web corporativos que no suelen pertenecer a ninguna otra categoría.
5	**Software**	En esta categoría se incluyen aquellos sitios web en los que se ofrece software, normalmente de código abierto, gratuito o shareware. También puede cubrir algunas tiendas de software en línea.
6	**Medicamentos**	En esta categoría se incluyen los sitios web relacionados con los medicamentos, el alcohol o los cigarros en los que se habla del uso o la venta de medicamentos (legales) o parafernalia médica, alcohol o productos con tabaco.

		Tenga en cuenta que las drogas ilegales quedan cubiertas en la categoría Drogas.
7	**Formación**	En esta categoría se incluyen aquellos sitios web que pertenecen a instituciones educativas oficiales, incluidos aquellos que no pertenecen al dominio .edu. También incluye los sitios web educativos, como las enciclopedias.
8	**Entretenimiento**	En esta categoría se incluyen aquellos sitios web que proporcionan información relacionada con actividades artísticas y museos, además de sitios web en los que se analiza o puntúa contenido como películas, música o arte.
9	**Uso compartido de archivos**	Esta categoría cubre los sitios web de compartición de archivos, donde un usuario puede cargar archivos y compartirlos con otros. También cubre los sitios web para compartir torrents, así como los rastreadores de torrents.
10	**Finanzas**	Esta categoría incluye todos los sitios web propiedad de bancos que proporcionan acceso en línea. También cubre algunas unidades de crédito y otras instituciones financieras. Sin embargo, las entidades bancarias locales podrían no estar cubiertas.
11	**Apuestas**	En esta categoría se incluyen los sitios web de apuestas. Son los del tipo "casino en línea " o "lotería en línea", que normalmente requieren un pago anticipado para que el usuario pueda apostar dinero en juegos de azar en línea como la ruleta, el póquer, el blackjack, etcétera. Algunos son legítimos, lo que significa que existe una posibilidad de ganar: otros son fraudulentos y no existe dicha posibilidad. También detecta los sitios web de "consejos y trucos para apostar", donde se describen modos de ganar dinero con los sitios web de juegos de azar y loterías en línea.
12	**Juegos**	En esta categoría se incluyen los sitios web que ofrecen juegos en línea, normalmente basados en applets Adobe Flash o Java. Para la detección, no importa si el juego es gratuito o si requiere una suscripción, pero los sitios web de estilo casino se integran en la categoría Apuestas. Esta categoría no cubre lo siguiente: • Sitios web oficiales de empresas que desarrollan videojuegos (salvo que produzcan juegos en línea) • Sitios web donde se conversa sobre juegos • Sitios web donde se pueden descargar juegos que no son en línea (algunos de los cuales se cubren en la categoría Ilegal) • Juegos que requieren que el usuario descargue y ejecute un archivo ejecutable, como World of Warcraft; es posible

		prevenirlos de distintas formas, como un cortafuegos
13	**Gobierno**	En esta categoría se incluyen los sitios web del Gobierno, incluidas las instituciones oficiales, las embajadas y los ministerios.
14	**Hackeo**	En esta categoría se incluyen los sitios web que proporcionan herramientas de hackeo, artículos y plataformas de discusión para los hackers. También cubre los sitios web que ofrecen "exploits" para plataformas comunes que facilitan el hackeo de cuentas de Facebook o Gmail.
15	**Actividades ilegales**	Esta categoría es amplia e incluye todo lo relacionado con el odio, la violencia y el racismo, y está pensada para bloquear las siguientes categorías de sitio web: • Sitios web pertenecientes a organizaciones terroristas • Sitios web con contenido racista o xenófobo • Sitios web donde se habla de deportes violentos, o que promueven la violencia
16	**Salud y bienestar**	En esta categoría se incluyen aquellos sitios web que están asociados a instituciones médicas, sitios web relacionados con la prevención de enfermedades y su tratamiento, y sitios web que ofrecen información o productos para perder peso, dietas, esteroides, anabolizantes y productos para estimular la hormona del crecimiento, así como aquellos sitios web que proporcionan información sobre cirugía plástica.
17	**Aficiones**	En esta categoría se incluyen aquellos sitios web que ofrecen recursos sobre actividades normalmente de ocio, como el coleccionismo, las manualidades y el ciclismo.
18	**Alojamiento web**	En esta categoría se incluyen los sitios web gratuitos y comerciales que alojan servicios con los que los usuarios y las organizaciones privadas pueden crear únicas páginas web.
19	**Descargas ilegales**	En esta categoría se incluyen los sitios web relacionados con la piratería de software, como los siguientes: • Sitios web de rastreadores P2P (BitTorrent, emule, DC++) conocidos por ayudar a distribuir contenido con derechos de autor sin el consentimiento de los poseedores de estos derechos • Sitios web y tableros de discusión de warez (software comercial pirateado) • Sitios web que proporcionan a los usuarios cracks, generadores de claves y números de serie para facilitar el uso ilegal del software

		Algunos de estos sitios web también pueden detectarse como pornografía o alcohol/tabaco, ya que a menudo utilizan publicidad de esta clase para obtener ingresos.
20	**Mensajería instantánea**	En esta categoría se incluyen los sitios web para chatear y de mensajería instantánea con los que los usuarios pueden hablar en tiempo real. También detecta yahoo.com y gmail.com, pues ambos contienen un servicio integrado de mensajería instantánea.
21	**Empleo**	En esta categoría se incluyen los sitios web que ofrecen bolsas de empleo, anuncios clasificados relacionados con el empleo y oportunidades de trabajo, además de agregadores de esos servicios. No cubre las agencias de reclutamiento ni las páginas de "empleos" en los sitios web oficiales de las empresas.
22	**Contenido para adultos**	En esta categoría se incluye el contenido que el creador de un sitio web ha etiquetado como dirigido a un público adulto. Cubre una amplia gama de sitios web, desde el libro Kama Sutra y las páginas de educación sexual hasta la pornografía más explícita.
23	**Drogas**	En esta categoría se incluyen los sitios web en los que se comparte información sobre drogas ilegales y recreativas. Esta categoría también cubre los sitios web sobre el desarrollo y cultivo de drogas.
24	**Noticias**	En esta categoría se incluyen los sitios web que ofrecen noticias en vídeo y texto. Intenta cubrir los sitios web de noticias tanto globales como locales, aunque algunos sitios web locales de pequeño tamaño pueden no quedar incluidos.
25	**Citas en línea**	En esta categoría se incluyen los sitios web de citas en línea, de pago y gratuitos, en los que los usuarios pueden buscar a otras personas según ciertos criterios. También pueden publicar sus perfiles para permitir que otras personas los busquen. Este categoría incluye los sitios web de citas tanto de pago como gratuitos. Como la mayoría de las redes sociales populares pueden utilizarse como sitios de citas en línea, determinados sitios populares, como Facebook, también se detectan dentro de esta categoría. Se recomienda utilizar esta categoría junto con la categoría Redes sociales.
26	**Pagos en línea**	En esta categoría se incluyen los sitios web que ofrecen pagos o transferencias de dinero en línea. Detecta sitios web de pago populares como PayPal o Moneybookers. También detecta de forma heurística las páginas web que, en sitios de otra naturaleza, solicitan información de tarjetas de crédito, lo que

		permite detectar tiendas en línea ocultas, desconocidas o ilegales.
27	**Uso compartido de fotos**	En esta categoría se incluyen los sitios web para compartir fotos cuyo objetivo principal es que los usuarios suban y compartan imágenes.
28	**Tiendas en línea**	En esta categoría se incluyen las tiendas en línea conocidas. Un sitio web se considera una tienda en línea si vende en línea bienes o servicios.
29	**Pornografía**	En esta categoría se incluyen los sitios web en los que hay contenido erótico y pornografía. Incluye tanto los sitios gratuitos como los de pago. Cubre los sitios web que ofrecen imágenes, historias y vídeos, y también detecta contenido pornográfico en sitios web con contenidos mixtos.
30	**Portales**	En esta categoría se incluyen los sitios web que reúnen información de varios recursos y dominios, y que normalmente ofrecen funciones como motores de búsqueda, correo electrónico, noticias e información sobre entretenimiento.
31	**Radio**	En esta categoría se incluyen los sitios web que ofrecen servicios de reproducción de música en Internet, desde emisoras de radio en línea hasta sitios web que proporcionan contenido de audio bajo demanda, ya sea de pago o gratuito.
32	**Religión**	En esta categoría se incluyen los sitios web que promueven la religión o las sectas religiosas. También cubre los foros de discusión relacionados con una o más religiones.
33	**Motores de búsqueda**	En esta categoría se incluyen los sitios web de motores de búsqueda, como Google, Yahoo y Bing.
34	**Redes sociales**	En esta categoría se incluyen los sitios web de redes sociales, como MySpace.com, Facebook.com, Bebo.com, etc. Sin embargo, las redes sociales especializadas, como YouTube.com, se encuadran en la categoría Vídeo/Foto.
35	**Deportes**	En esta categoría se incluyen los sitios web que ofrecen información, noticias y tutoriales deportivos.
36	**Suicidio**	En esta categoría se incluyen los sitios web que promueven, ofrecen o defienden el suicidio. No cubre las clínicas de prevención del suicidio.
37	**Prensa amarilla**	Esta categoría se ha diseñado principalmente para los sitios web de porno suave y cotilleo sobre famosos. Muchos sitios web de noticias sensacionalistas pueden tener subcategorías aquí integradas. La detección de esta categoría también se basa en un mecanismo heurístico.

38	**Pérdida de tiempo**	En esta categoría se incluyen aquellos sitios web en los que las personas suelen pasar mucho tiempo. Pueden incluirse sitios web de otras categorías, como las redes sociales o el entretenimiento.
39	**Viajes**	En esta categoría se incluyen aquellos sitios web que ofrecen ofertas de viajes y equipamiento para viajar, además de reseñas y puntuaciones sobre destinos de viajes.
40	**Vídeos**	En esta categoría se incluyen aquellos sitios web en los que se alojan vídeos o fotos, ya sean subidos por los usuarios u ofrecidos por distintos proveedores de contenidos. Se incluyen sitios web como YouTube, Metacafe o Google Video, y sitios de fotos como Picasa o Flickr. También detecta vídeos incrustados en otros sitios web o blogs.
41	**Dibujos animados violentos**	En esta categoría se incluyen aquellos sitios web en los que se habla, se comparten y se proporcionan dibujos animados violentos o manga que pueden ser inapropiados para menores por su violencia, lenguaje explícito o contenido sexual. Esta categoría no cubre los sitios web que ofrecen dibujos animados generalistas como "Tom y Jerry".
42	**Armas**	En esta categoría se incluyen los sitios web de venta, intercambio, fabricación o uso de armas. También cubre los recursos de caza y el uso de armas BB y de aire comprimido, así como las armas cuerpo a cuerpo.
43	**Correo electrónico**	En esta categoría se incluyen aquellos sitios web que proporcionan funcionalidades de correo electrónico en forma de aplicación web.
44	**Proxy web**	En esta categoría se incluyen aquellos sitios web que ofrecen servicios de proxy web. Se trata de sitios web del tipo “navegador dentro de un navegador” en los que el usuario abre una página web, introduce la URL solicitada en un formulario y hace clic en “Enviar”. A continuación, el sitio de proxy web descarga la página y la muestra dentro del navegador del usuario. Estas son las razones por las que se detectan estos sitios (y por las que podría ser necesario bloquearlos): • Para navegar de forma anónima. Como las solicitudes al servidor web de destino se realizan desde el servidor web del proxy, solo la dirección IP de dicho servidor es visible. Si el administrador del servidor de destino rastrea al usuario, el rastro termina en el proxy web, que puede o no mantener registros que permitan localizar al usuario original.

		• Para falsificar la ubicación. La dirección IP de los usuarios se utiliza a menudo para segmentar los servicios según la ubicación de origen (algunos sitios gubernamentales solo están disponibles desde direcciones IP locales); el uso de estos servicios puede ayudar al usuario a camuflar su auténtica ubicación. • Para acceder a contenido prohibido. Si se utiliza un simple filtro de URL, solo se verán las URL del proxy web y no los servidores reales que el usuario visita. • Para evitar la supervisión de las empresas. Una directiva de empresa puede requerir que se supervise el uso que los empleados hacen de Internet. Como se accede a todo el contenido a través de un proxy web, un usuario podría evadir esta supervisión, que no obtendrá información correcta. Como el SDK analiza la página HTML (si se proporciona) y no solo las URL, en algunas categorías, el SDK podrá seguir detectando el contenido. Sin embargo, con el simple uso del SDK no pueden evitarse algunas de las razones.

Si habilita la casilla de verificación **Mostrar todas las notificaciones de las URL bloqueadas por categorías**, se mostrarán en la bandeja las notificaciones de URL bloqueadas organizadas por categorías. Si un sitio web tiene varios subdominios, también se generan notificaciones para ellos, por lo que el número de estas puede ser elevado.

Exclusiones

Las direcciones URL que se sabe que son seguras se pueden añadir a la lista de direcciones URL de confianza. Las direcciones URL que suponen una amenaza se pueden añadir a la lista de direcciones URL bloqueadas.

Pasos para añadir una URL a una lista

1. En el módulo filtrado de URL de un plan de protección, haga clic en **Exclusiones**.
2. Seleccione la lista deseada: **De confianza** o **Bloqueadas**.
3. Haga clic en **Agregar**.
4. Especifique la URL o la dirección IP y haga clic en la marca de verificación.

Ejemplos de exclusiones URL:

- Si añade xyz.com como de confianza o de no confianza, todas las direcciones del dominio xyz.com se tratarán como de confianza o de no confianza según donde quiera añadirlas.
- Si desea añadir un subdominio específico, puede añadir **mail.xyz.com** como de confianza o de no confianza. Esto no provocará que todas las direcciones **xyz.com** sean de confianza o de no confianza.

- Si desea añadir IPv4 a la lista de confianza o de no confianza, debe utilizar el siguiente formato para que sea válido: **20.53.203.50**.
- Si desea añadir varias exclusiones URL al mismo tiempo, asegúrese de añadir cada entrada a una nueva línea:

  acronis.com

  mail.xyz.com

  20.53.203.50

Cuarentena

Cuarentena es una carpeta especial que se encuentra aislada en el disco duro de un equipo. En ella se colocan los archivos sospechosos detectados por la protección antivirus y antimalware para evitar que las amenazas se expandan todavía más.

Gracias a esta opción, puede revisar los archivos sospechosos y potencialmente peligrosos de todos los equipos, y decidir si se deben eliminar o restaurar. Los archivos que estén en cuarentena se borran automáticamente si el equipo se elimina del sistema.

¿Cómo llegan los archivos a la carpeta de cuarentena?

1. Configure el plan de protección y defina la acción predeterminada para los archivos infectados, es decir, ponerlos en cuarentena.
2. Durante el análisis en acceso o planificado, el sistema detecta archivos maliciosos y los coloca en la carpeta segura Cuarentena.
3. El sistema actualiza la lista de elementos en cuarentena de cada equipo.
4. Los archivos se borran automáticamente de la carpeta Cuarentena cuando pasa el periodo de tiempo definido en la configuración **Eliminar archivos en cuarentena después de** del plan de protección.

Gestión de los archivos que están en cuarentena

Para gestionar los archivos que están en cuarentena, vaya a **Protección antimalware** > **Cuarentena**. Ahí encontrará una lista con los archivos que están en cuarentena de todos los equipos.

Nombre	Descripción
Archivo	Nombre del archivo.
Fecha de puesta en cuarentena	Fecha y hora en que el archivo se puso en cuarentena.
Dispositivo	Dispositivo en que se encuentra el archivo

	infectado.
Nombre de la amenaza	El nombre de la amenaza.
Plan de protección	Plan de protección según el que el archivo sospechoso se puso en cuarentena.

Con los archivos que están en cuarentena, puede llevar a cabo dos acciones:

- **Eliminar**: eliminar permanentemente un archivo en cuarentena de todos los equipos.
- **Restaurar**: restaurar un archivo en cuarentena a su ubicación original sin ninguna modificación. Si ya hay un archivo con el mismo nombre en la ubicación original, se sobrescribirá con el archivo restaurado.

Ubicación de la carpeta Cuarentena en los equipos

La ubicación predeterminada para los archivos que están en cuarentena es la siguiente:

Para un equipo Windows: `%ProgramData%\%product_name%\Quarantine`

Para un equipo Mac o Linux: `/usr/local/share/%product_name%/quarantine`

Lista blanca corporativa

Importante
La lista blanca corporativa requiere que Scan Service esté instalado en el servidor de gestión.

Alguna solución antivirus podría identificar aplicaciones específicas corporativas legítimas como sospechosas. Para evitar esos falsos positivos, las aplicaciones de confianza se añaden de forma manual a la lista blanca, y eso supone perder bastante tiempo.

Cyber Protect puede automatizar este proceso: el módulo de protección antimalware y antivirus analiza las copias de seguridad con el fin de añadir las aplicaciones a la lista blanca y prevenir las detecciones de falsos positivos. Además, la lista blanca en el nivel de la empresa mejora el rendimiento posterior de los análisis.

La lista blanca se puede activar y desactivar. Cuando está desactivada, sus archivos añadidos se ocultan temporalmente.

Inclusión automática de aplicaciones en la lista blanca

1. Ejecutar un análisis en la nube de las copias de seguridad en al menos dos equipos. Para hacerlo, utilice los "Análisis de planes de copia de seguridad" (p. 404).
2. En la configuración de las listas blancas, habilite el conmutador **Generación automática de listas blancas**.

Inclusión manual de aplicaciones en la lista blanca

Cuando el conmutador **Generación automática de listas blancas** esté deshabilitado, podrá añadir archivos a la lista blanca de forma manual.

1. En la consola web de Cyber Protect, vaya a **Protección Antimalware** > **Lista blanca**.
2. Haga clic en **Añadir archivo**.
3. Especifique la ruta del archivo y haga clic en **Añadir**.

Añadir archivos en cuarentena a la lista blanca

Puede añadir archivos en cuarentena a la lista blanca.

1. En la consola web de Cyber Protect, vaya a **Protección Antimalware** > **Cuarentena**.
2. Seleccione un archivo en cuarentena y haga clic en **Añadir a la lista blanca**.

Configuración de la lista blanca

Cuando habilite el conmutador **Generación automática de listas blancas**, debe especificar uno de los siguientes niveles de protección heurística:

- **Bajo**
  Las aplicaciones empresariales se añadirán a la lista blanca solo después de un tiempo significativo y varias comprobaciones. Tales aplicaciones ofrecen mayor confianza. Sin embargo, este enfoque aumenta la posibilidad de que se detecten falsos positivos. Los criterios para considerar que un archivo está limpio y es de confianza son muy elevados.
- **Predeterminado**
  Las aplicaciones empresariales se añadirán a la lista blanca en función del nivel de protección recomendado para reducir la detección de posibles falsos positivos. Los criterios para considerar que un archivo está limpio y es de confianza son intermedios.
- **Alto**
  Las aplicaciones empresariales se añadirán a la lista blanca más rápido para reducir la detección de posibles falsos positivos. Sin embargo, así no se garantiza que el software esté limpio y más adelante podría reconocerse como sospechoso o malware. Los criterios para considerar que un archivo está limpio y es de confianza son bajos.

Visualización de detalles sobre elementos de la lista blanca

Puede hacer clic en un elemento para ver más información sobre este y analizarlo en línea.

Si tiene dudas sobre un elemento que añadió, puede comprobarlo en el analizador de VirusTotal. Al hacer clic en **Comprobar en VirusTotal**, el sitio analiza archivos y URL sospechosos para detectar tipos de malware mediante el hash del archivo del elemento que añadió. Puede ver el hash en la cadena **Hash del archivo (MD5)**.

El valor **Equipos** representa el número de equipos en los que se ha encontrado ese hash durante el análisis de copias de seguridad. Este valor se completa solo si un elemento proviene del análisis de copias de seguridad o de la cuarentena. El campo se queda vacío si se ha añadido el archivo manualmente a la lista blanca.

Análisis antimalware de copias de seguridad

Para evitar la recuperación de archivos infectados, configure un plan de escaneado de copias de seguridad y asegúrese de que no contienen malware.

El análisis antimalware de las copias de seguridad está disponible si el componente Scan Service está instalado con el servidor de administración Cyber Protect. Para obtener más información, consulte "Scan Service" (p. 112).

Los planes de escaneo de copias de seguridad son compatibles con las copias de seguridad de **equipo completo** y **disco/volumen** de equipos Windows. Solo se analizan los volúmenes con el sistema de archivos NTFS y particionado GPT o MBR.

Los siguientes almacenamientos de copias de seguridad son compatibles:

- Almacenamiento en la cloud
- Carpeta de red
- Carpeta local
  Solo los agentes instalados en la misma carga de trabajo pueden acceder a las copias de seguridad en una carpeta local.

Nota
Por motivos de seguridad y rendimiento, le recomendamos utilizar un equipo designado para fines de análisis. Este equipo deberá tener acceso a todas las copias de seguridad que se analizan.

Las copias de seguridad que seleccione para llevar a cabo el análisis pueden encontrarse en uno de los siguientes estados:

- No analizado
- Sin malware
- Malware detectado

Para comprobar el estado, en la consola web de Cyber Protect, vaya a **Almacenamiento de copias de seguridad** > **Ubicaciones** y, a continuación, compruebe la columna **Estado**. El widget **Detalles del análisis de copias de seguridad** de la pestaña **Panel de control** > **Descripción general** también proporciona información sobre este estado.

Limitaciones

- No se analizan los puntos de recuperación con copias de seguridad de Protección continua de datos (CDP). Solo se analizan los puntos de recuperación no CDP del conjunto de copias de

seguridad seleccionado. Para obtener más información sobre Protección continua de datos, consulte "Protección continua de datos (CDP)" (p. 268).

- Cuando se realiza una recuperación segura de una copia de seguridad de **equipo completo**, los datos del punto de recuperación CDP no se recuperan automáticamente. Para recuperar estos datos, ejecute una recuperación de **Archivos/carpetas**.

Protección de aplicaciones de colaboración y comunicación

Zoom, Cisco Webex Meetings y Microsoft Teams son aplicaciones de comunicación, videoconferencia y conferencia web muy extendidas. Cyber Protect le permite proteger sus herramientas de colaboración.

La configuración de protección para Zoom, Cisco Webex Meetings y Microsoft Teams es similar. En el ejemplo siguiente, veremos la configuración correspondiente a Zoom.

Pasos para configurar la protección de Zoom

1. Instale un agente de protección en el equipo donde está instalada la aplicación de colaboración.
2. Inicie sesión en la consola web de Cyber Protect y aplique un plan de protección que tenga habilitado alguno de los módulos siguientes:
   - **Protección antimalware y antivirus** (con las opciones **Autoprotección** y **Active Protection** habilitadas): si tiene una de las ediciones de Cyber Protect.
   - **Active Protection** (con la opción **Autoprotección** habilitada): si tiene una de las ediciones de Cyber Backup.
3. [Opcional] Para instalar las actualizaciones automáticamente, configure el módulo **Gestión de correcciones** en el plan de protección.

Como resultado, su aplicación Zoom quedará bajo una protección que incluye las actividades siguientes:

- Instalación automática de actualizaciones del cliente de Zoom
- Protección de los procesos de Zoom frente a inyecciones de código
- Prevención de operaciones sospechosas por parte de los procesos de Zoom
- Protección del archivo de "servidores" para que no se añadan dominios relacionados con Zoom

Evaluación de vulnerabilidades y gestión de parches

La **evaluación de vulnerabilidades** es un proceso que consiste en identificar, cuantificar y priorizar las vulnerabilidades encontradas en el sistema. Al utilizar el módulo de evaluación de vulnerabilidades en un plan de protección, podrá analizar los equipos en busca de vulnerabilidades y asegurarse de que todos los sistemas operativos y las aplicaciones instaladas estén actualizados y funcionen correctamente.

El análisis de evaluación de vulnerabilidades es compatible con equipos con los siguientes sistemas operativos:

- Windows. Para obtener más información, consulte "Productos de Microsoft y de terceros compatibles" (p. 601).
- Equipos Linux (CentOS 7/Virtuozzo/Acronis Cyber Infrastructure). Para obtener más información, consulte "Productos de Linux compatibles" (p. 602).

Utilice la función de **gestión de parches** (PM) para gestionar los parches (actualizaciones) de las aplicaciones y los sistemas operativos instalados en sus equipos y mantener actualizados sus sistemas. Con el módulo de gestión de parches, podrá aprobar manual o automáticamente la instalación de actualizaciones en sus equipos.

La gestión de parches es compatible con equipos con Windows. Para obtener más información, consulte "Productos de Microsoft y de terceros compatibles" (p. 601).

Evaluación de vulnerabilidades

El proceso de evaluación de vulnerabilidades está formado por los siguientes pasos:

1. Cree un plan de protección con el módulo de evaluación de vulnerabilidades habilitado, especifique los ajustes de la evaluación de vulnerabilidades y asigne el plan a los equipos.
2. El sistema, si está planificado o se le pide, envía un comando a los agentes de protección para que se ejecute el análisis de la evaluación de vulnerabilidades.
3. Los agentes reciben el comando, empiezan a analizar equipos en busca de vulnerabilidades y generan la actividad de análisis.
4. Cuando haya terminado la evaluación de vulnerabilidades, los agentes generan los resultados y los envían al servicio de supervisión.
5. El servicio de supervisión procesa los datos de los agentes y muestra los resultados en los widgets de evaluación de vulnerabilidades y en una lista de vulnerabilidades encontradas.
6. Con esta información, puede decidir cuáles de las vulnerabilidades halladas deben arreglarse.

Puede comprobar los resultados del análisis de la evaluación de vulnerabilidades en **Panel de control** > **Información general** > widgets **Vulnerabilidades/Vulnerabilidades existentes**.

Productos de Microsoft y de terceros compatibles

Los siguientes productos de Microsoft y de terceros para sistemas operativos Windows son compatibles con la evaluación de vulnerabilidades.

Productos de Microsoft compatibles

Sistemas operativos de escritorio

- Windows 7 (Enterprise, Professional y Ultimate)
- Windows 8
- Windows 8.1
- Windows 10

Sistemas operativos de servidor

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2

Microsoft Office y componentes relacionados

- Microsoft Office 2019 (x64, x86)
- Microsoft Office 2016 (x64, x86)
- Microsoft Office 2013 (x64, x86)
- Microsoft Office 2010 (x64, x86)

Componentes de Windows

- Internet Explorer
- Microsoft Edge
- Windows Media Player
- .NET Framework
- Visual Studio y aplicaciones
- Componentes del sistema operativo

Aplicaciones del servidor

- Microsoft SQL Server 2008 R2
- Microsoft SQL Server 2012
- Microsoft SQL Server 2014
- Microsoft SQL Server 2016
- Microsoft SQL Server 2017
- Microsoft SQL Server 2019
- Microsoft Exchange Server 2013
- Microsoft Sharepoint Server 2016
- Microsoft Sharepoint Server 2016

Productos de terceros compatibles con Windows

Cyber Protect es compatible con la evaluación de vulnerabilidades y la instalación de parches de una amplia gama de aplicaciones de terceros, incluyendo herramientas de colaboración y clientes VPN, que son de vital importancia en escenarios de trabajo remotos.

Para ver la lista completa de los productos de terceros compatibles para Windows, consulte https://kb.acronis.com/content/62853.

Productos de Linux compatibles

Distribuciones Linux y versiones de este sistema operativo que son compatibles con la evaluación de vulnerabilidades:

- Virtuozzo 7.0.11
- Virtuozzo 7.0.10 (320)
- Virtuozzo 7.0.9 (539)
- Virtuozzo 7.0.8 (524)
- CentOS 7.x
- Acronis Ciberinfraestructura 3.x
- Acronis Almacenamiento 2.4.0
- Acronis Almacenamiento 2.2.0

Configuración de la evaluación de vulnerabilidades

Para obtener más información sobre cómo crear un plan de protección con el módulo de evaluación de vulnerabilidades, consulte "Creación de un plan de protección" (p. 247). El análisis de la evaluación de vulnerabilidades se puede llevar a cabo cuando esté planificado o cuando se desee (mediante la acción **Ejecutar ahora** de un plan de protección).

Puede especificar los ajustes siguientes en el módulo de evaluación de vulnerabilidades.

Qué analizar

Seleccione los productos de software que quiera analizar para detectar vulnerabilidades:

- Equipos Windows:
  - **Productos de Microsoft**
  - **Productos de terceros para Windows**
    Para obtener más información sobre los productos de terceros compatibles para Windows, consulte https://kb.acronis.com/content/62853.
- Equipos Linux:
  - **Analizar paquetes de Linux**

Planificación

Defina la planificación que se deberá seguir para llevar a cabo el análisis de la evaluación de vulnerabilidades en los equipos seleccionados:

Planifique la ejecución de tareas con los siguientes eventos:

- **Planificar por tiempo**: la tarea se ejecutará según el tiempo especificado.
- **Cuando el usuario inicia sesión en el sistema**: de forma predeterminada, el inicio de sesión de cualquier usuario iniciará la tarea. Puede modificar esta configuración para que únicamente una cuenta de usuario concreta pueda activar la tarea.
- **Cuando el usuario cierra sesión en el sistema**: de forma predeterminada, cuando cualquier usuario cierre sesión se iniciará la tarea. Puede modificar esta configuración para que únicamente una cuenta de usuario concreta pueda activar la tarea.

  Nota
  La tarea no se ejecutará al apagarse el sistema. Apagar y cerrar sesión son dos acciones diferentes de la configuración de la programación.

- **Al iniciarse el sistema**: la tarea se ejecutará cuando el sistema operativo se inicie.
- **Al apagarse el sistema**: la tarea se ejecutará cuando el sistema operativo se apague.

Configuración predeterminada: **Planificar por hora**.

Tipo de planificación:

- **Mensualmente** : seleccione los meses y las semanas o días del mes en los que se ejecutará la tarea.
- **Diariamente** : seleccione los días de la semana en los que se ejecutará la tarea.
- **Cada hora**: seleccione los días de la semana, el número de repeticiones y el intervalo de tiempo en los que se ejecutará la tarea.

Configuración predeterminada: **Diariamente**.

Iniciar a las : seleccione la hora exacta a la que se ejecutará la tarea.

Ejecutar dentro de un intervalo de fechas: Establezca un rango en el que la planificación configurada sea efectiva.

Condiciones de inicio: defina todas las condiciones que se deben cumplir de forma simultánea para que se ejecute la tarea.

Las condiciones de inicio para el análisis antimalware son similares a las de inicio del módulo de copia de seguridad que se describen en "Condiciones de inicio" (p. 289). Puede definir las siguientes condiciones de inicio adicionales:

- **Distribuir las horas de inicio de la tarea en un período de tiempo**: esta opción le permite establecer el plazo de tiempo de la tarea para evitar cuellos de botella en la red. Puede especificar el retraso en horas o minutos. Por ejemplo, si la hora de inicio predeterminada son las 10:00 y el retraso es de 60 minutos, la tarea empezará entre las 10:00 y las 11:00.
- **Si el equipo está apagado, ejecutar las tareas perdidas al iniciar el equipo**
- **Evitar el modo de suspensión o hibernación durante la ejecución de una tarea**: esta opción solo se aplica en equipos que ejecuten Windows.
- **Si no se cumplen las condiciones de inicio, ejecutar la tarea de todos modos después de**: especifique el periodo tras el que se ejecutará la tarea, sin importar el resto de las condiciones de inicio.

Nota
En Linux, las condiciones de inicio no están admitidas.

Evaluación de vulnerabilidades para equipos Windows

Puede analizar equipos Windows y productos de terceros para Windows para buscar vulnerabilidades.

1. En la consola web de Cyber Protect, cree un plan de protección y habilite el módulo de **evaluación de vulnerabilidades**.
2. Especifique la configuración de la evaluación de vulnerabilidades:
   - **Qué analizar**: seleccione **Microsoft**, **productos de terceros para Windows** o ambos.
   - **Planificación** : define la planificación para ejecutar la evaluación de vulnerabilidades.
     Para obtener más información sobre las opciones de **Planificación**, consulte "Configuración de la evaluación de vulnerabilidades" (p. 602).
3. Asigne el plan a los equipos Windows.

Después de un análisis de evaluación de vulnerabilidades, verá una lista de vulnerabilidades halladas. Puede procesar la información y decidir cuáles de las vulnerabilidades halladas deben arreglarse.

Para comprobar los resultados de la evaluación de vulnerabilidades, consulte **Panel de control** > **Información general** > widgets **Vulnerabilidades/Vulnerabilidades existentes**.

Evaluación de vulnerabilidades para equipos Linux

Puede escanear equipos Linux en busca de vulnerabilidades a nivel de aplicación y núcleo.

Para configurar la evaluación de vulnerabilidades en equipos Linux

1. En la consola web de Cyber Protect, cree un plan de protección y habilite el módulo de **evaluación de vulnerabilidades**.
2. Especifique la configuración de la evaluación de vulnerabilidades:
   - **Qué analizar**: seleccione **Analizar paquetes de Linux**.
   - **Planificación** : define la planificación para ejecutar la evaluación de vulnerabilidades.
     Para obtener más información sobre las opciones de **Planificación**, consulte "Configuración de la evaluación de vulnerabilidades" (p. 602).
3. Asigne el plan a los equipos de Linux.

Después de un análisis de evaluación de vulnerabilidades, verá una lista de vulnerabilidades halladas. Puede procesar la información y decidir cuáles de las vulnerabilidades halladas deben arreglarse.

Para comprobar los resultados de la evaluación de vulnerabilidades, consulte **Panel de control** > **Información general** > widgets **Vulnerabilidades/Vulnerabilidades existentes**.

Gestión de vulnerabilidades encontradas

Si la evaluación de vulnerabilidades se ha llevado a cabo al menos una vez y se detecta alguna vulnerabilidad, las podrá encontrar en **Gestión del software** > **Vulnerabilidades**. En la lista de vulnerabilidades se muestran tanto aquellas para las que hay disponibles parches como las que no tienen ningún parche sugerido. Puede usar el filtro para mostrar únicamente las vulnerabilidades con parches disponibles.

Nombre	Descripción
Nombre	Nombre de la vulnerabilidad.
Productos afectados	Productos de software en los que se han encontrado vulnerabilidades.
Equipos	Número de equipos afectados.
Gravedad	La gravedad de la vulnerabilidad encontrada. Se pueden asignar los siguientes niveles según el sistema Common Vulnerability Scoring System (CVSS): • **Crítico**: 9-10 CVSS • **Alto**: 7-9 CVSS • **Medio**: 3-7 CVSS • **Bajo**: 0-3 CVSS

	• **Ninguno**
Parches	Número de parches adecuado.
Fecha de publicación	La fecha y la hora en las que se publicó la vulnerabilidad en Vulnerabilidades y exposiciones comunes (CVE).
Fecha de la detección	Fecha en la que se detectó por primera vez una vulnerabilidad existente en equipos.

Si hace clic en su nombre en la lista, encontrará la descripción de una vulnerabilidad encontrada.

Pasos para iniciar el proceso de resolución de vulnerabilidades

1. En la consola web de Cyber Protect, vaya a **Gestión del software** > **Vulnerabilidades**.
2. Seleccione las vulnerabilidades en la lista y, a continuación, haga clic en **Instalar parches**. Se abrirá el asistente de solución de vulnerabilidades.
3. Seleccione los parches a instalar. Haga clic en **Siguiente**.
4. Seleccione los equipos en los cuales desea instalar parches.
5. Seleccione si desea reiniciar el equipo después de la instalación del parche:
   - **No**: los equipos no se reiniciarán nunca después de la instalación de un parche.
   - **Si es necesario**: el reinicio tendrá lugar únicamente si es necesario para aplicar las actualizaciones.
   - **Sí**: siempre se reiniciará el equipo tras la instalación de los parches. Sin embargo, puede indicar una demora.

   No reiniciar hasta que la copia de seguridad haya finalizado: si un proceso de copia de seguridad se está ejecutando, se retrasará el reinicio de la máquina hasta que finalice la copia de seguridad.
6. Haga clic en **Instalar parches**.

Como resultado, los parches seleccionados se instalan en los equipos indicados.

Gestión de parches

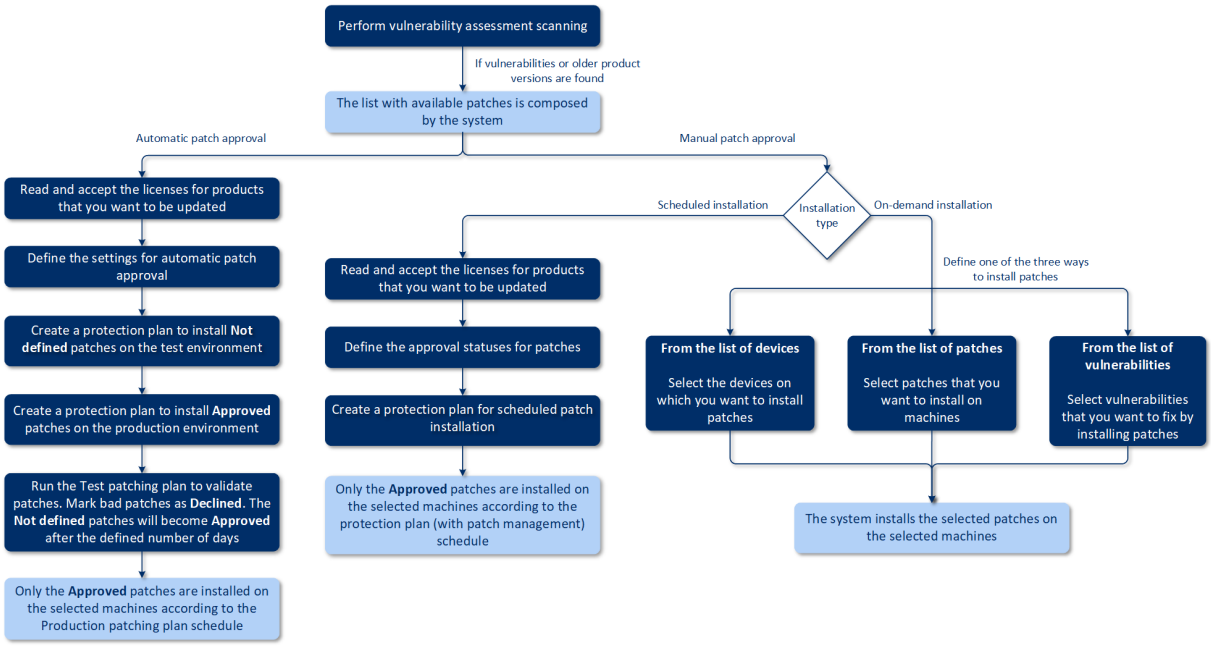
Utilice la funcionalidad de gestión de parches para:

- Instalar actualizaciones a nivel de aplicación y sistema operativo
- Aprobar la instalación manual o automática de parches
- Instalar parches cuando se desee o según una planificación
- Definir de forma precisa qué parches aplicar según distintos criterios: gravedad, categoría y estado de aprobación
- Llevar a cabo copias de seguridad previas a las actualizaciones por si no se realizan correctamente
- Definir la opción de reinicio que se va aplicar después de la instalación de parches

Cyber Protect presenta tecnología de par a par con el fin de minimizar el tráfico del ancho de banda de red. Puede elegir uno o varios agentes dedicados que descargarán actualizaciones de Internet y las distribuirán ente otros agentes en la red. Además, todos los agentes compartirán actualizaciones con el resto como agentes del mismo nivel.

Cómo funciona

Puede configurar si desea que los parches se aprueben de forma manual o automática. En el esquema que aparece continuación puede ver los flujos de trabajo de las aprobaciones de parches tanto manuales como automáticas.



1. En primer lugar, tiene que llevar a cabo al menos un análisis de la evaluación de vulnerabilidades usando el plan de protección con el módulo **Evaluación de vulnerabilidades** habilitado. Cuando se lleva a cabo el análisis, el sistema forma las listas de vulnerabilidades encontradas y de parches disponibles.
2. A continuación puede configurar la aprobación de parches automática o usar el enfoque de aprobación de parches manual.
3. Defina cómo desea que se instalen los parches: según una planificación o bajo demanda. La instalación de parches bajo demanda se puede llevar a cabo de tres maneras según sus preferencias:
   - Vaya a la lista de parches (**Gestión del software** > **Parches**) e instale los parches necesarios.
   - Vaya a la lista de vulnerabilidades (**Gestión del software** > **Vulnerabilidades**) e inicie el proceso de resolución que incluye, además, la instalación de parches.
   - Vaya a la lista de dispositivos (**Dispositivos** > **Todos los dispositivos**), seleccione los equipos concretos que quiera actualizar y en los que desee instalar los parches.

Puede revisar los resultados de la instalación de parches en el widget **Panel de control** > **Información general** > **Historial de instalación de parches**.

Configuración de la gestión de parches

Para obtener más información sobre cómo crear un plan de protección con el módulo de gestión de parches, consulte "Creación de un plan de protección". Al usar el plan de protección, puede especificar qué actualizaciones de productos Microsoft y otros productos de terceros para Windows quiere instalar automáticamente en los equipos definidos.

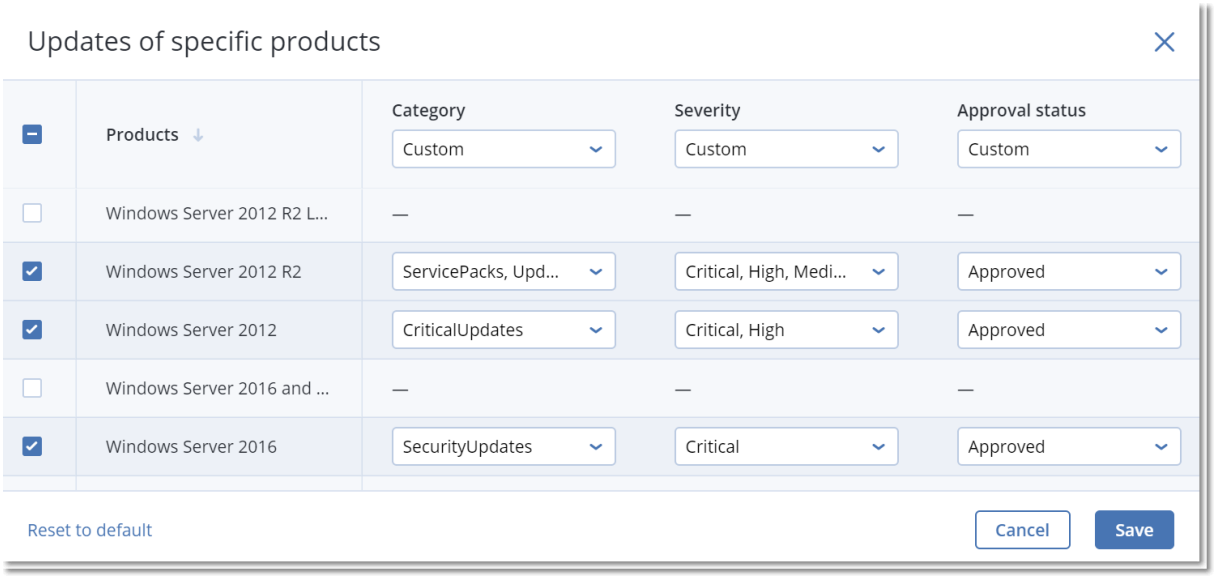
Para el módulo de gestión de parches se pueden establecer los siguientes ajustes:

Productos de Microsoft

Para instalar las actualizaciones de Microsoft en los equipos seleccionados, habilite la opción **Actualizar productos de Microsoft**.

Seleccionar qué actualizaciones desea que se instalen:

- **Todas las actualizaciones**
- **Solo actualizaciones de seguridad y críticas**
- **Actualizaciones de productos específicos**: puede definir configuraciones predeterminadas para productos diferentes. Si desea actualizar productos específicos, puede definir qué actualizaciones quiere instalar para cada producto según su categoría, gravedad o estado de aprobación.

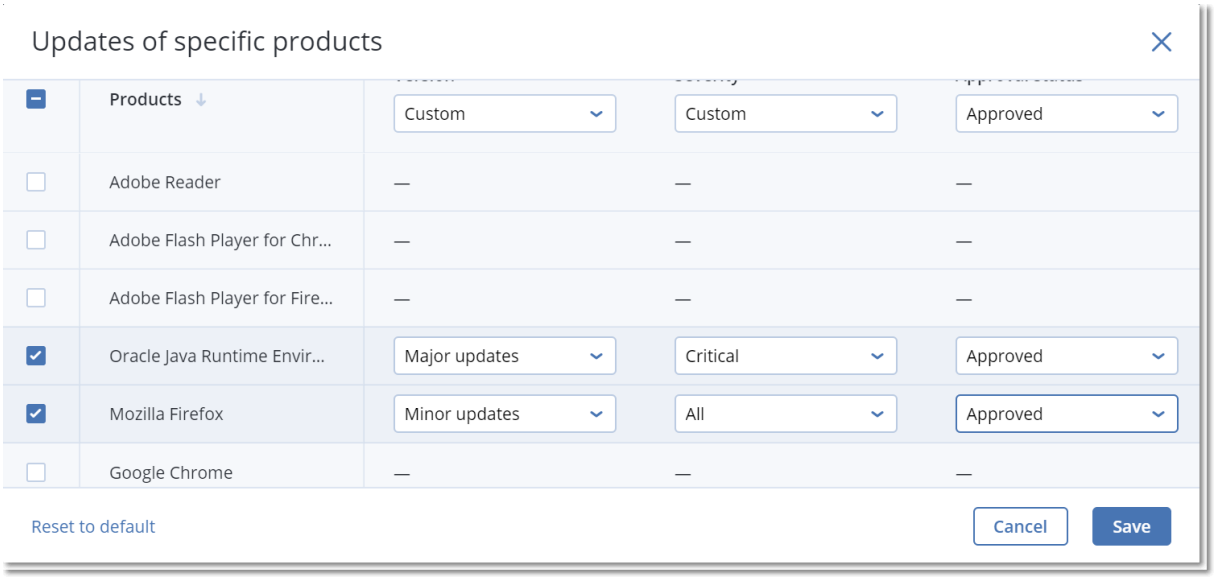


Productos de terceros a Windows

Para instalar las actualizaciones de terceros para Windows en los equipos seleccionados, habilite la opción **Productos de terceros para Windows**.

Seleccionar qué actualizaciones desea que se instalen:

- Con la opción **Solo las actualizaciones importantes**, puede instalar la última versión disponible de la actualización.
- Con la opción **Solo las actualizaciones menores**, puede instalar la versión menor de la actualización.
- **Actualizaciones de productos específicos**: puede definir configuraciones predeterminadas para productos diferentes. Si desea actualizar productos específicos, puede definir qué actualizaciones quiere instalar para cada producto según su categoría, gravedad o estado de aprobación.



Planificación

Defina la planificación que se seguirá para instalar las actualizaciones en los equipos seleccionados.

Planifique la ejecución de tareas con los siguientes eventos:

- **Planificar por tiempo**: la tarea se ejecutará según el tiempo especificado.
- **Cuando el usuario inicia sesión en el sistema**: de forma predeterminada, el inicio de sesión de cualquier usuario iniciará la tarea. Puede modificar esta configuración para que únicamente una cuenta de usuario concreta pueda activar la tarea.
- **Cuando el usuario cierra sesión en el sistema**: de forma predeterminada, cuando cualquier usuario cierre sesión se iniciará la tarea. Puede modificar esta configuración para que únicamente una cuenta de usuario concreta pueda activar la tarea.

> **Nota**
> La tarea no se ejecutará al apagarse el sistema. Apagar y cerrar sesión son dos acciones diferentes de la configuración de la programación.

- **Al iniciarse el sistema**: la tarea se ejecutará cuando el sistema operativo se inicie.
- **Al apagarse el sistema**: la tarea se ejecutará cuando el sistema operativo se apague.

Configuración predeterminada: **Planificar por hora**.

Tipo de planificación:

- **Mensualmente** : seleccione los meses y las semanas o días del mes en los que se ejecutará la tarea.
- **Diariamente** : seleccione los días de la semana en los que se ejecutará la tarea.
- **Cada hora**: seleccione los días de la semana, el número de repeticiones y el intervalo de tiempo en los que se ejecutará la tarea.

Configuración predeterminada: **Diariamente**.

Iniciar a las : seleccione la hora exacta a la que se ejecutará la tarea.

Ejecutar dentro de un intervalo de fechas: Establezca un rango en el que la planificación configurada sea efectiva.

Condiciones de inicio: defina todas las condiciones que se deben cumplir de forma simultánea para que se ejecute la tarea.

Las condiciones de inicio para el análisis antimalware son similares a las de inicio del módulo de copia de seguridad que se describen en "Condiciones de inicio" (p. 289). Puede definir las siguientes condiciones de inicio adicionales:

- **Distribuir las horas de inicio de la tarea en un período de tiempo**: esta opción le permite establecer el plazo de tiempo de la tarea para evitar cuellos de botella en la red. Puede especificar el retraso en horas o minutos. Por ejemplo, si la hora de inicio predeterminada son las 10:00 y el retraso es de 60 minutos, la tarea empezará entre las 10:00 y las 11:00.
- **Si el equipo está apagado, ejecutar las tareas perdidas al iniciar el equipo**
- **Evitar el modo de suspensión o hibernación durante la ejecución de una tarea**: esta opción solo se aplica en equipos que ejecuten Windows.
- **Si no se cumplen las condiciones de inicio, ejecutar la tarea de todos modos después de**: especifique el periodo tras el que se ejecutará la tarea, sin importar el resto de las condiciones de inicio.

Copia de seguridad anterior a la actualización

Realizar una copia de seguridad antes de instalar actualizaciones de software: el sistema creará una copia de seguridad incremental del equipo antes de instalar cualquier actualización en él. Si anteriormente no se había creado ninguna copia de seguridad, se creará una copia de seguridad completa del equipo. De este modo, podrá volver al estado anterior en caso de fallo en la instalación del parche. Para que la opción **Copia de seguridad anterior a la actualización** funcione, los equipos correspondientes deben tener el módulo de copias de seguridad y el de gestión de parches habilitados en un plan de protección, y contar con los elementos que se van a incluir en la copia de seguridad, ya sea todo el equipo o los volúmenes de inicio del sistema de arranque. Si selecciona elementos inapropiados para la copia de seguridad, el sistema no le permitirá habilitar la opción **Copia de seguridad anterior a la actualización**.

Gestión de la lista de parches

Cuando se complete la evaluación de vulnerabilidades, encontrará los parches disponibles en **Gestión del software** > **Parches**.

Nombre	Descripción
Nombre	Nombre del parche.
Gravedad	Nivel de gravedad del parche: • **Crítico** • **Alto** • **Medio** • **Bajo** • **Ninguno**
Proveedor	Proveedor del parche.
Producto	Producto en el que se puede aplicar el parche.
Versiones instaladas	Versiones del producto que ya están instaladas.
Versión	Versión del parche.
Categoría	Categoría a la que pertenece el parche: • **Actualización crítica**: correcciones de amplia distribución para tratar problemas específicos asociados a errores críticos no relacionados con aspectos de seguridad. • **Actualización de la seguridad**: revisiones de amplia distribución para tratar problemas específicos asociados a errores de seguridad. • **Actualización de la definición**: actualizaciones aplicadas a virus u otros archivos de definiciones. • **Paquete acumulativo de actualizaciones**: conjuntos acumulativos de revisiones, actualizaciones de seguridad, actualizaciones críticas y actualizaciones que se recopilan para facilitar su implementación. Un paquete acumulativo está orientado normalmente a un área específica, como la seguridad, o a un componente de un producto, como Servicios de Internet Information Server (IIS). • **Paquete de servicio**: conjuntos acumulativos de todas las revisiones, actualizaciones de seguridad, actualizaciones críticas y actualizaciones creadas desde el lanzamiento del producto. Los paquetes de servicios también pueden contener un número limitado de

	funciones o cambios de diseño solicitados por el cliente. • **Herramienta**: utilidades o funciones que ayudan a llevar a cabo una tarea o un conjunto de tareas. • **Paquete de funciones**: lanzamientos de nuevas funciones que se suelen incluir en la última versión de los productos. • **Actualización**: correcciones que se emplean muchísimo para tratar problemas específicos asociados a errores que no son críticos ni están relacionados con aspectos de seguridad. • **Aplicación**: parches para una aplicación.
KB de Microsoft	Si el parche es para un producto de Microsoft, se proporciona el ID del artículo de la KB
Fecha de publicación	Fecha en la que se publicó el parche.
Equipos	Número de equipos afectados.
Estado de aprobación	El estado de aprobación se necesita principalmente para aquellas situaciones en las que las aprobaciones se realizan automáticamente y para poder definir qué actualizaciones se instalarán en el plan de protección según su estado. Puede para definir uno de los siguientes estados para un parche: • **Aprobado**: el parche se ha instalado al menos en un equipo y se ha validado correctamente. • **Rechazado**: el parche no es seguro y puede dañar el sistema de un equipo. • **No definido**: el estado del parche no está claro y hay que validarlo.
Acuerdo de licencia	• Lea y acepte • No acepto. Si no acepta el acuerdo de licencia, el estado del parche pasa a ser **Rechazado** y no se instalará.
Vulnerabilidades	Número de vulnerabilidades. Si hace clic en esta opción, se le redirigirá a la lista de vulnerabilidades.
Tamaño	Tamaño medio del parche.
Idioma	Idioma que admite el parche.
Sitio del proveedor	Sitio oficial del proveedor.

Aprobación automática de parches

Con la aprobación automática de parches, el proceso de instalación de actualizaciones en los equipos le resultará más sencillo. Veamos cómo funciona con este ejemplo.

Cómo funciona

Debe tener dos entornos: de prueba y de producción. El entorno de prueba se utiliza para comprobar la instalación de los parches y garantizar que no dañe nada. Cuando haya comprobado la instalación de los parches en el entorno de prueba, podrá instalar automáticamente estos parches seguros en el entorno de producción.

Configuración de la aprobación automática de parches

Pasos para configurar la aprobación automática de parches

1. Debe leer y aceptar los acuerdos de licencia de cada proveedor cuyos productos tenga pensado actualizar. De lo contrario, los parches no se podrán instalar automáticamente.
2. Establezca los ajustes de la aprobación automática.
3. Prepare el plan de protección (por ejemplo, "Instalación de parches en entornos de prueba") con el módulo **Gestión de parches** habilitado y aplíquelo a los equipos del entorno de prueba. Especifique la siguiente condición con respecto a la instalación de parches: el estado de aprobación del parche debe ser **No definido**. Este paso es necesario para validar los parches y comprobar si los equipos funcionan correctamente después de su instalación.
4. Prepare el plan de protección (por ejemplo, "Instalación de parches en entornos de producción") con el módulo **Gestión de parches** habilitado y aplíquelo a los equipos del entorno de producción. Especifique la siguiente condición con respecto a la instalación de parches: el estado del parche debe ser **Aprobado**.
5. Ejecute el plan Instalación de parches en entornos de prueba y compruebe los resultados. El estado de aprobación de los equipos que no tengan problemas se puede mantener en **No definido**, mientras que el de los que no funcionan correctamente se debe establecer en **Rechazado**.
6. Según el número de días establecidos en la opción **Aprobación automática**, los parches cuyo estado sea **No definido** pasarán a **Aprobado**.
7. Cuando se lance el plan Instalación de parches en entornos de producción, únicamente se instalarán en los equipos de producción los parches cuyo estado sea **Aprobado**.

Los pasos que debe realizar manualmente se indican a continuación.

Paso 1. Lea y acepte los acuerdos de licencia de los productos que quiera actualizar.

1. En la consola web de Cyber Protect, vaya a **Gestión del software** > **Parches**.
2. Seleccione el parche y, a continuación, lea y acepte el acuerdo de licencia.

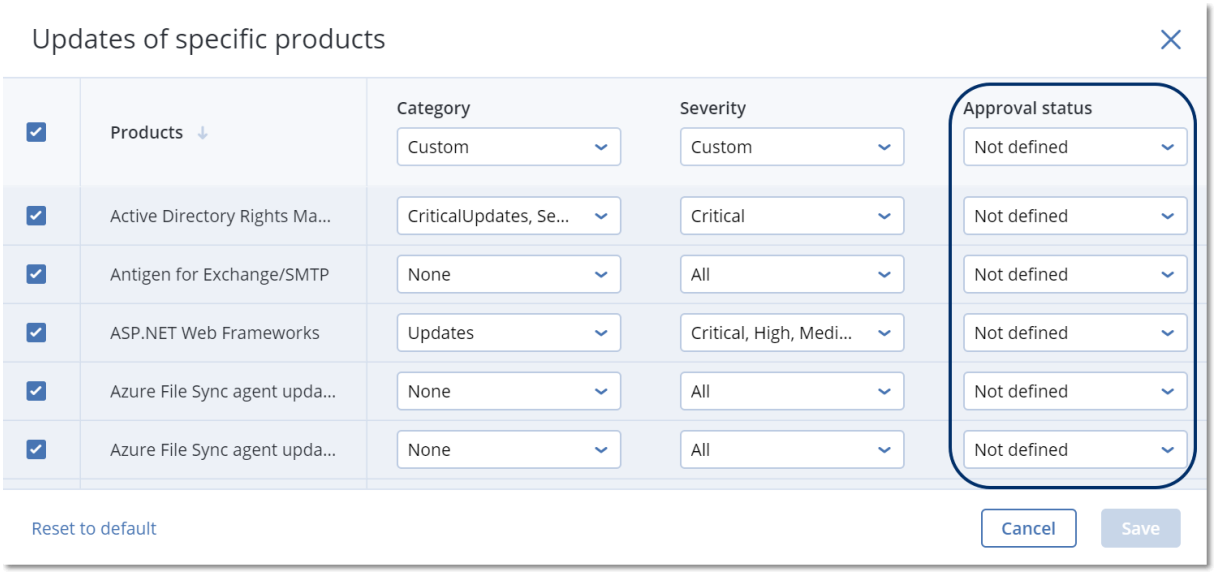
Paso 2. Establezca los ajustes de la aprobación automática.

1. En la consola web de Cyber Protect, vaya a **Gestión del software** > **Parches**.
2. Haga clic en **Configuración**.
3. Habilite la opción **Aprobación automática** y especifique el número de días. Esto significa que, cuando pase el número especificado de días desde el primer intento de instalación de los parches, los que tengan el estado **No definido** pasarán al de **Aprobado** automáticamente.
   Por ejemplo, ha especificado 10 días. Ha llevado a cabo el plan Instalación de parches en entornos de prueba para probar equipos y parches instalados. Los parches que dañaron los equipos los marcó como **Rechazados**, mientras que el resto se mantuvieron como **No definidos**. Cuando pasen 10 días, los parches cuyo estado sea **No definido** se actualizarán automáticamente al estado **Aprobado**.
4. Habilite la opción **Aceptar automáticamente los acuerdos de licencia**. Esta acción es necesaria para aceptar las licencias automáticamente durante la instalación de los parches, pues no se necesita ninguna confirmación por parte del usuario.

Paso 3. Prepare el plan de protección Instalación de parches en entornos de prueba.

1. En la consola web de Cyber Protect, vaya a **Planes** > **Protección**.
2. Haga clic en **Crear plan**.
3. Habilite el módulo **Gestión de parches**.
4. Defina qué actualizaciones desea instalar para productos de Microsoft y terceros, establezca una planificación y realice una copia de seguridad previa a la actualización. Para obtener más información sobre esa configuración, consulte "Configuración de la gestión de parches".

Importante
Defina la opción **Estado de aprobación** como **No definido** para todos aquellos productos que se vayan a actualizar. Cuando llegue el momento de actualizarlos, el agente instalará únicamente los parches cuyo estado sea **No definido** en los equipos seleccionados del entorno de prueba.

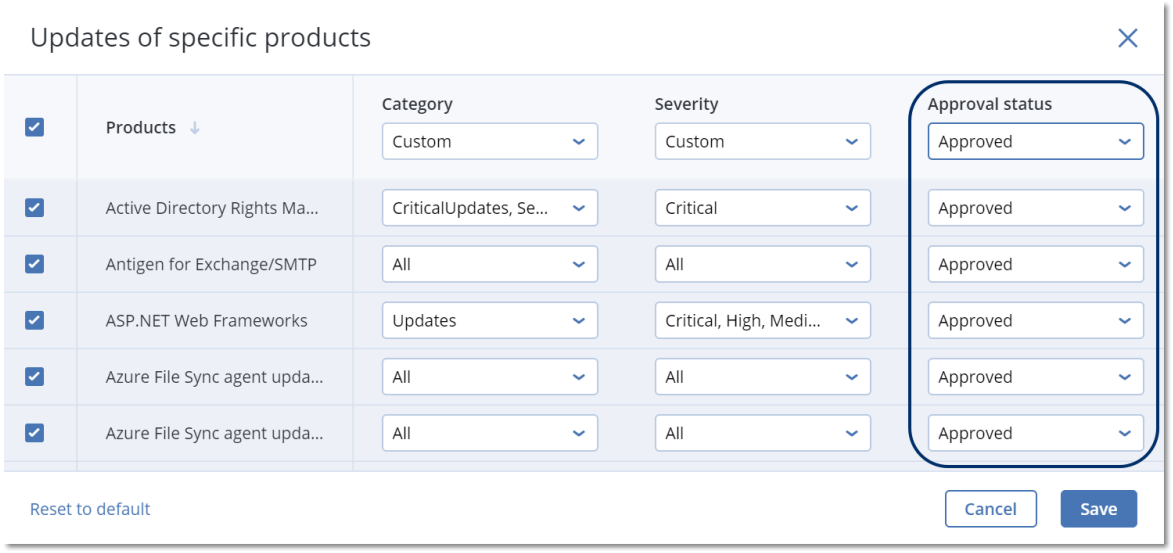


Paso 4. Prepare el plan de protección Instalación de parches en entornos de producción.

1. En la consola web de Cyber Protect, vaya a **Planes** > **Protección**.
2. Haga clic en **Crear plan**.
3. Habilite el módulo **Gestión de parches**.
4. Defina qué actualizaciones desea instalar para productos de Microsoft y terceros, establezca una planificación y realice una copia de seguridad previa a la actualización. Para obtener más información sobre esa configuración, consulte "Configuración de la gestión de parches".

Importante
Defina la opción **Estado de aprobación** como **Aprobado** para todos aquellos productos que se vayan a actualizar. Cuando llegue el momento de actualizarlos, el agente instalará únicamente los parches cuyo estado sea **Aprobado** en los equipos seleccionados del entorno de producción.

Nota



Paso 5. Ejecute el plan de protección Instalación de parches en entornos de prueba y revise los resultados.

1. Ejecute el plan de protección Instalación de parches en entornos de prueba (según la planificación o bajo demanda).
2. Luego, compruebe cuáles de los parches instalados son seguros y cuáles no.
3. Vaya a **Gestión del software** > **Parches** y establezca el **Estado de aprobación** como **Rechazado** para aquellos parches que no sean seguros.

Aprobación manual de parches

El proceso de aprobación de parches manual es el siguiente:

1. En la consola web de Cyber Protect, vaya a **Gestión del software** > **Vulnerabilidades**.
2. Seleccione los parches que quiera instalar y, a continuación, lea y acepte los acuerdos de licencia.
3. Establezca el **estado de aprobación** en **Aprobado** para los parches que apruebe para la instalación.
4. Cree un plan de protección con el módulo de gestión de parches habilitado. Puede configurar la planificación del plan o iniciarlo cuando lo desee si hace clic en **Ejecutar ahora** en la configuración del módulo de gestión de parches.

Como resultado, únicamente los parches aprobados se instalarán en los equipos indicados.

Instalación de parches bajo demanda

La instalación de parches bajo demanda se puede llevar a cabo de tres maneras según sus preferencias:

- Vaya a la lista de parches (**Gestión del software** > **Parches**) e instale los parches necesarios.
- Vaya a la lista de vulnerabilidades (**Gestión del software** > **Vulnerabilidades**) e inicie el proceso de resolución que incluye, además, la instalación de parches.
- Vaya a la lista de dispositivos (**Dispositivos** > **Todos los dispositivos**), seleccione los equipos concretos que quiera actualizar y en los que desee instalar los parches.

Centrémonos en la instalación de parches desde la lista de parches:

1. En la consola web de Cyber Protect, vaya a **Gestión del software** > **Vulnerabilidades**.
2. Acepte los acuerdos de licencia para los parches que quiera instalar.
3. Seleccione los parches que quiera instalar y haga clic en **Instalar**.
4. Seleccione los equipos en los que se deban instalar los parches.
5. Defina si se reinicia el equipo después de instalar los parches:
   - **Nunca** : los equipos no se reiniciarán nunca después de los parches.
   - **Si es necesario**: el reinicio tendrá lugar únicamente si es necesario para aplicar los parches.
   - **Siempre**: siempre se reiniciará el equipo tras la instalación de los parches. También puede especificar cuándo tendrá lugar el reinicio.

   No reiniciar hasta que la copia de seguridad haya finalizado: si el proceso de copia de seguridad se está ejecutando, se retrasará el reinicio de la máquina hasta que finalice la copia de seguridad.
6. Haga clic en **Instalar parches**.

Los parches seleccionados se instalarán en los equipos indicados.

Tiempo de los parches en la lista

Para que la lista de parches esté actualizada, vaya a **Gestión del software** > **Parches** > **Configuración** y especifique la opción **Tiempo en la lista**.

La opción **Tiempo en la lista** define el tiempo durante el cual el parche disponible detectado se conservará en la lista de parches. Normalmente el parche se elimina de la lista cuando se ha instalado correctamente en todos los equipos en los que se detectó que faltaba o cuando ha transcurrido el tiempo definido.

- **Siempre**: el parche se mantiene siempre en la lista.
- **7 días**: el parche se eliminará siete días después de su instalación.

  Por ejemplo, tiene los equipos en los que se deben instalar parches. Uno de ellos está en línea y el otro fuera de línea. El parche se ha instalado en el primer equipo. Cuando pasen siete días, el parche se eliminará, aunque no esté instalado en el segundo equipo porque estaba fuera de línea.
- **30 días**: el parche se eliminará treinta días después de su instalación.

Protección inteligente

Fuente de amenazas

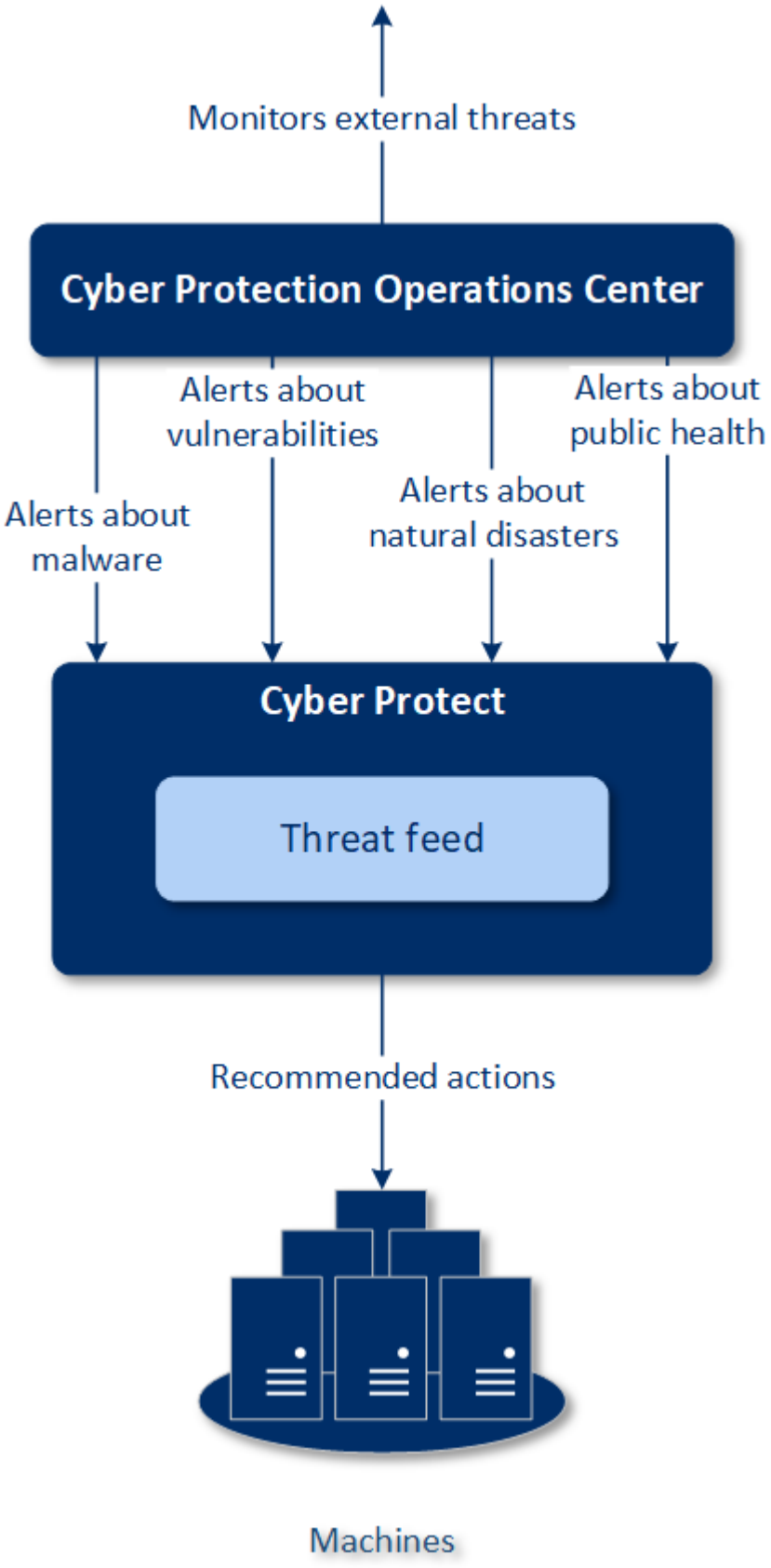
El centro de operaciones de ciberprotección (CPOC) de Acronis genera alertas de seguridad que se envían únicamente a las regiones geográficas relacionadas. Estas alertas de seguridad proporcionan información sobre malware, vulnerabilidades, desastres naturales, salud pública y otros tipos de acontecimientos globales que puedan afectar a la protección de sus datos. El registro de amenazas le informa sobre todas las posibles amenazas para que pueda evitarlas.

Una alerta de seguridad se puede resolver con las acciones específicas que indican los expertos en seguridad. Algunas alertas solo se emplean para informarle sobre las prótesis más amenazas, pero no hay acciones recomendadas disponibles.

Cómo funciona

El centro de operaciones de ciberprotección (CPOC) de Acronis supervisa las amenazas externas y genera alertas sobre amenazas relacionadas con malware, vulnerabilidades, desastres naturales y salud pública. Podrá ver todas estas alertas en la consola web de Cyber Protect, en la sección **Fuente de amenazas**. Puede realizar las acciones recomendadas respectivas en función del tipo de alerta.

El principal flujo de trabajo de la fuente de amenazas está representado en el siguiente diagrama.



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

1. En la consola web de Cyber Protect, vaya a **Panel de control** > **Fuente de amenazas** para comprobar si hay alguna alerta de seguridad existente.

2. Seleccione una alerta de la lista y revise la información proporcionada.

3. Haga clic en **Iniciar** para iniciar el asistente.

4. Habilite las acciones que quiera llevar a cabo y seleccione los equipos en los que se deben aplicar. Es posible que se sugieran las siguientes opciones:

- **Evaluación de vulnerabilidades**: su función es analizar los equipos seleccionados para la búsqueda de vulnerabilidades
- **Gestión de parches**: sirve para instalar parches en los equipos seleccionados.
- **Protección antimalware**: su función es ejecutar un análisis completo de los equipos seleccionados.
- **Copia de seguridad de equipos protegidos o no protegidos**: sirve para realizar copias de seguridad de equipos protegidos o no protegidos.

5. Haga clic en **Iniciar**.

6. En la página **Actividades**, verifique que la actividad se haya realizado correctamente.

Eliminación de todas las alertas

Las alertas de la fuente de amenazas se eliminan automáticamente después de los siguientes periodos de tiempo:

- Desastre natural: 1 semana
- Vulnerabilidad: 1 mes
- Malware: 1 mes
- Salud pública: 1 semana

Mapa de protección de datos

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

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

Cómo funciona

1. Primero, cree un plan de protección con el módulo Mapa de protección de datos habilitado.
2. A continuación, cuando se haya ejecutado el plan y sus datos se hayan detectado y analizado, obtendrá la representación visual de la protección de datos en el widget Mapa de protección de datos.
3. Otra opción es que vaya a **Dispositivos** > **Mapa de protección de datos** y busque allí información sobre los archivos que no estén protegidos por dispositivo.
4. Puede realizar acciones para proteger los archivos detectados como no protegidos en los dispositivos.

Gestión de los archivos detectados que no tienen protección

Para proteger los archivos importantes detectados como no protegidos, lleve a cabo las siguientes acciones:

1. En la consola web de Cyber Protect, vaya a **Dispositivos** > **Mapa de protección de datos**.

   En la lista de dispositivos, puede encontrar información general sobre el número de archivos sin protección, el tamaño de los archivos por dispositivo y la última detección de datos.

   Para proteger los archivos de un equipo en concreto, haga clic en el icono de puntos suspensivos (...) y luego en **Proteger todos los archivos**. Se le dirigirá a la lista de planes en la que puede crear un plan de protección con el módulo de copia de seguridad habilitado.

   Para eliminar el dispositivo concreto en el que se encuentran los archivos sin protección de la lista, haga clic en **Ocultar hasta la próxima detección de datos**.
2. Para obtener información detallada sobre los archivos sin protección de un dispositivo concreto, haga clic en el nombre del dispositivo.

   Verá una lista de archivos sin protección por extensión y ubicación. Puede filtrar esta lista por extensión de archivo.
3. Para proteger todos los archivos que no estén protegidos, haga clic en **Proteger todos los archivos**. Se le dirigirá a la lista de planes en la que puede crear un plan de protección con el módulo de copia de seguridad habilitado.

Para obtener un informe con información sobre los archivos que no están protegidos, haga clic en **Descargar informe detallado en CSV**.

Ajustes del mapa de protección de datos

Para obtener más información sobre cómo crear un plan de protección con el módulo Mapa de protección de datos, consulte "Creación de un plan de protección".

Para el módulo Mapa de protección de datos se pueden especificar los siguientes ajustes:

Planificación

Puede definir diferentes configuraciones para crear la planificación en función de la tarea que se vaya a realizar para el mapa de protección de datos.

Planifique la ejecución de tareas con los siguientes eventos:

- **Planificar por tiempo**: la tarea se ejecutará según el tiempo especificado.
- **Cuando el usuario inicia sesión en el sistema**: de forma predeterminada, el inicio de sesión de cualquier usuario iniciará la tarea. Puede modificar esta configuración para que únicamente una cuenta de usuario concreta pueda activar la tarea.
- **Cuando el usuario cierra sesión en el sistema**: de forma predeterminada, cuando cualquier usuario cierre sesión se iniciará la tarea. Puede modificar esta configuración para que únicamente una cuenta de usuario concreta pueda activar la tarea.

  Nota
  La tarea no se ejecutará al apagarse el sistema. Apagar y cerrar sesión son dos acciones diferentes de la configuración de la programación.

- **Al iniciarse el sistema**: la tarea se ejecutará cuando el sistema operativo se inicie.
- **Al apagarse el sistema**: la tarea se ejecutará cuando el sistema operativo se apague.

Configuración predeterminada: **Planificar por hora**.

Tipo de planificación:

- **Mensualmente** : seleccione los meses y las semanas o días del mes en los que se ejecutará la tarea.
- **Diariamente** : seleccione los días de la semana en los que se ejecutará la tarea.
- **Cada hora**: seleccione los días de la semana, el número de repeticiones y el intervalo de tiempo en los que se ejecutará la tarea.

Configuración predeterminada: **Diariamente**.

Iniciar a las : seleccione la hora exacta a la que se ejecutará la tarea.

Ejecutar dentro de un intervalo de fechas: Establezca un rango en el que la planificación configurada sea efectiva.

Condiciones de inicio: defina todas las condiciones que se deben cumplir de forma simultánea para que se ejecute la tarea.

Las condiciones de inicio para el análisis antimalware son similares a las de inicio del módulo de copia de seguridad que se describen en "Condiciones de inicio" (p. 289). Puede definir las siguientes condiciones de inicio adicionales:

- **Distribuir las horas de inicio de la tarea en un período de tiempo**: esta opción le permite establecer el plazo de tiempo de la tarea para evitar cuellos de botella en la red. Puede

especificar el retraso en horas o minutos. Por ejemplo, si la hora de inicio predeterminada son las 10:00 y el retraso es de 60 minutos, la tarea empezará entre las 10:00 y las 11:00.

- **Si el equipo está apagado, ejecutar las tareas perdidas al iniciar el equipo**
- **Evitar el modo de suspensión o hibernación durante la ejecución de una tarea**: esta opción solo se aplica en equipos que ejecuten Windows.
- **Si no se cumplen las condiciones de inicio, ejecutar la tarea de todos modos después de**: especifique el periodo tras el que se ejecutará la tarea, sin importar el resto de las condiciones de inicio.

Extensiones y reglas de excepción

En la pestaña **Extensiones** , puede definir la lista de extensiones de archivo que se considerarán importantes durante la detección de datos y comprobar si están protegidas. Para definir extensiones, utilice el siguiente formato:

```
.html, .7z, .docx, .zip, .pptx, .xml
```

En la pestaña **Reglas de excepción**, puede seleccionar los archivos y carpetas cuyo estado de protección no hay que comprobar durante la detección de datos.

- **Archivos y carpetas ocultos**: si esta opción está seleccionada, los archivos y carpetas ocultos se omitirán durante el análisis de los datos.
- **Archivos y carpetas del sistema**: si esta opción está seleccionada, los archivos y carpetas del sistema se omitirán durante el análisis de los datos.

Acceso a escritorio remoto

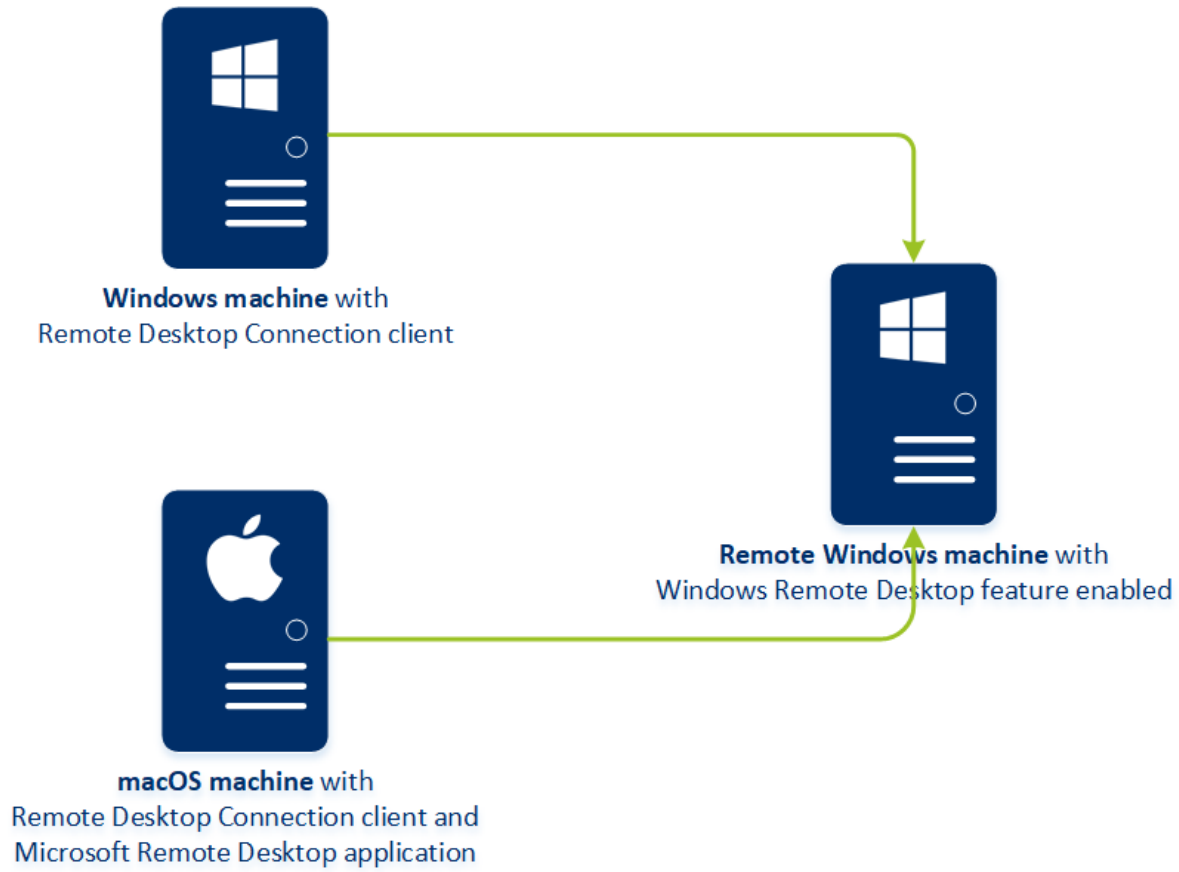
Acceso remoto (clientes RDP y HTML5)

Cyber Protect le ofrece capacidad de acceso remoto. Puede conectarse de forma remota a los equipos de sus usuarios y gestionarlos directamente desde la consola web. Así, podrá ayudar de forma sencilla a sus usuarios a resolver problemas relacionados con los equipos.

Requisitos previos:

- Se instala un agente de protección en el equipo remoto y se registra en el servidor de gestión.
- Se le ha asignado una licencia de Cyber Protect adecuada al equipo.
- El cliente de Conexión a escritorio remoto está instalado en el equipo desde el que se inicia la conexión.
- El equipo desde el que se inicia la conexión a escritorio remoto debe poder acceder al servidor de gestión con su nombre de servidor. Los ajustes DNS deben configurarse correctamente o se debe incluir el nombre del servidor de gestión en los archivos del servidor.

Se puede establecer una conexión remota desde equipos Windows y macOS.



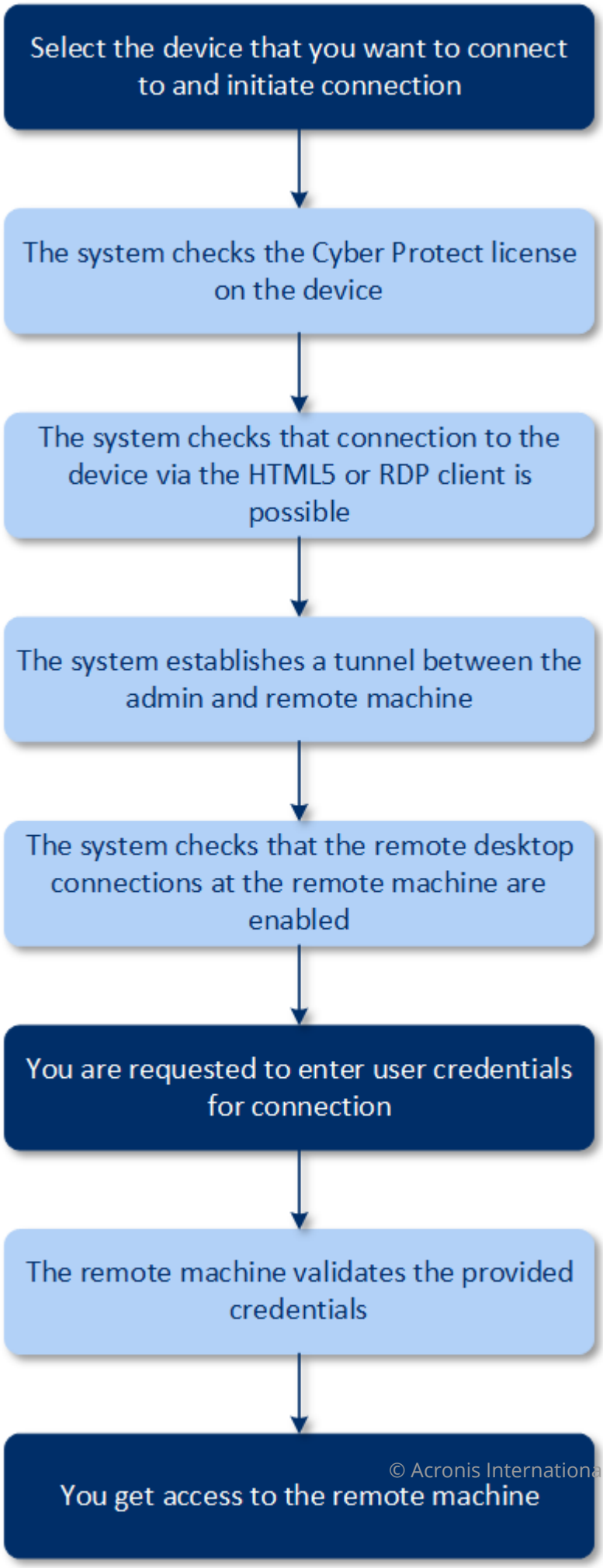
La funcionalidad de acceso remoto se puede utilizar para conexiones a equipos Windows en los que la función de escritorio remoto de Windows esté disponible. Por eso no es posible el acceso remoto a, por ejemplo, sistemas Windows 10 Home o macOS.

Para establecer una conexión con un equipo remoto desde un equipo macOS, compruebe que en este último están instaladas las siguientes aplicaciones:

- El cliente de Conexión a escritorio remoto
- La aplicación Escritorio remoto de Microsoft

Cómo funciona

Cuando intenta conectarse a un equipo remoto, el sistema comprueba primero que ese equipo tenga una licencia de Cyber Protect. A continuación, el sistema comprueba si se puede establecer la conexión mediante el cliente HTML5 o RDP. Puede iniciar una conexión a través del cliente HTML5 o RDP. El sistema establece un túnel al equipo remoto y comprueba si las conexiones a escritorios remotos están habilitadas en el equipo remoto. A continuación, introduzca las credenciales para acceder al equipo remoto tras la validación.



Cómo conectarse a un equipo remoto

Para conectarse a un equipo remoto, realice los siguientes pasos:

1. En la consola web de Cyber Protect, vaya a **Dispositivos** > **Todos los dispositivos**.
2. Haga clic en el equipo al que quiera conectarse remotamente y a continuación en **Escritorio de ciberprotección** > **Conectar mediante cliente RDP** o **Conectar mediante cliente HTML5**.

   Nota
   La conexión mediante cliente HTML5 solo está disponible si el servidor de gestión está instalado en un equipo Linux.

3. [Opcional, solo para conexiones a través del cliente RDP] Descargue e instale el cliente de conexión al escritorio remoto. Inicie la conexión con el equipo remoto.
4. Especifique el nombre de usuario y la contraseña para acceder al equipo remoto y haga clic en **Conectar**.

Como resultado, se conectará al equipo remoto y podrá gestionarlo.

Compartir una conexión remota

Los empleados que trabajan desde casa pueden necesitar acceder a sus equipos de la oficina, pero es posible que la organización no haya configurado la VPN u otras herramientas de conexión remota. Cyber Protect le permite compartir un enlace RDP con sus usuarios para proporcionarles acceso remoto a sus equipos.

Pasos para habilitar la funcionalidad de uso compartido de la conexión remota

1. En la consola web de Cyber Protect, vaya a **Configuración** > **Protección** > **Conexión remota**.
2. Seleccione la casilla de verificación **Compartir conexión de escritorio remoto**.

Como resultado, la nueva opción **Compartir conexión remota** aparecerá cuando seleccione un dispositivo en la consola web de Cyber Protect.

Pasos para compartir una conexión remota con sus usuarios

1. En la consola web de Cyber Protect, vaya a **Dispositivos** > **Todos los dispositivos**.
2. Seleccione el dispositivo al que desea que se pueda acceder de forma remota.
3. Haga clic en **Compartir conexión remota**.
4. Haga clic en **Obtener enlace**. En la ventana abierta, copie el enlace generado. Este enlace se puede compartir con un usuario que necesite acceso remoto al dispositivo. El enlace tiene una validez de 10 horas.

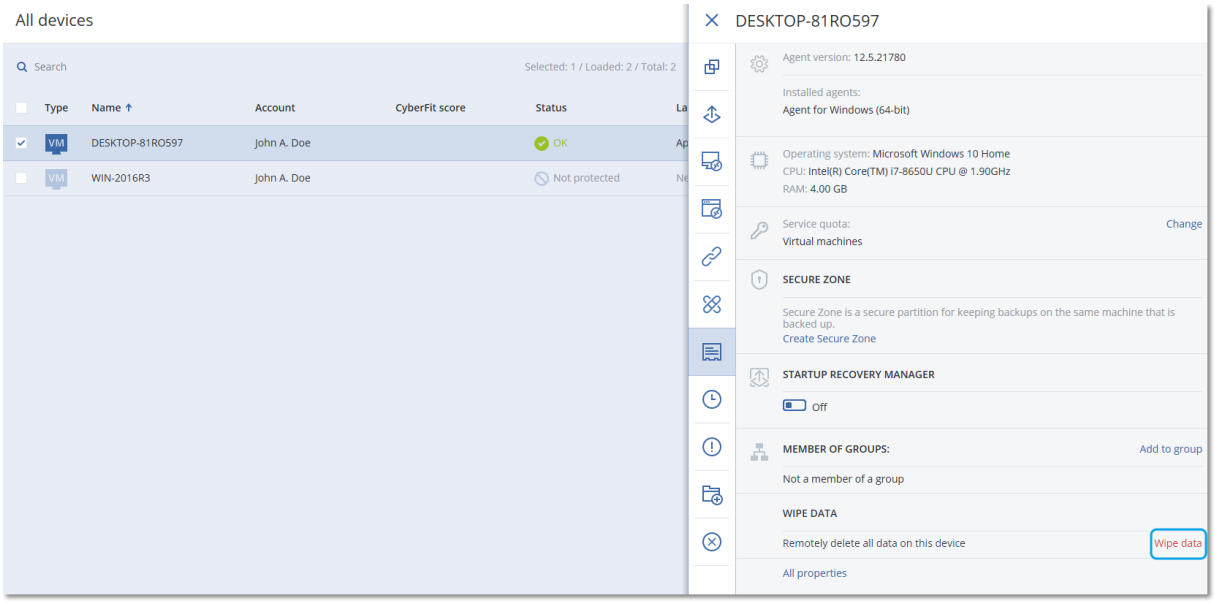
Después de obtener el enlace, puede compartirlo por correo electrónico o cualquier otro medio de comunicación. El usuario con el que comparta el enlace deberá hacer clic en él y seleccionar el tipo de conexión:

- Conectar mediante cliente RDP.
  Esta conexión solicitará que se descargue e instale el cliente de conexión remota.
- Conectar mediante cliente HTML5.
  Esta conexión no requiere la instalación de un cliente RDP en el equipo del usuario. Se redirigirá al usuario a una pantalla de inicio de sesión en la que deberá introducir las credenciales para acceder al equipo.

Borrado remoto

Borrado remoto permite a un administrador del servicio Cyber Protect y al propietario de un equipo eliminar los datos de un equipo gestionado, por ejemplo, en caso de pérdida o robo. De este modo se puede evitar el acceso no autorizado a información confidencial.

El borrado remoto solo está disponible para equipos con Windows 10. Para recibir el comando de borrado, el equipo debe estar encendido y conectado a Internet.



Pasos para borrar los datos de un equipo

1. En la consola web de Cyber Protect, vaya a **Dispositivos** > **Todos los dispositivos**.
2. Seleccione el equipo cuyos datos desea borrar.

   Nota
   Puede borrar datos de un solo equipo al mismo tiempo.

3. Haga clic en **Detalles** y, a continuación, en **Borrar datos**.
   Si el equipo que ha seleccionado está fuera de línea, la opción **Borrar datos** no es accesible.
4. Confirme su elección.
5. Introduzca las credenciales de administrador local del equipo y, a continuación, haga clic en **Borrar datos**.

   Nota
   Puede comprobar los detalles del proceso de borrado y quién lo inició desde **Panel de control** > **Actividades**.

Grupos de los dispositivos

Los grupos de dispositivos se han diseñado para gestionar cómodamente un gran número de dispositivos registrados.

Puede aplicar un plan de protección a un grupo. Cuando aparezca un nuevo dispositivo en el grupo, este pasará a estar protegido por el plan. Si se elimina un dispositivo del grupo, este dejará de estar protegido por el plan. No se puede revocar un plan que se ha aplicado a un grupo desde un miembro del grupo; únicamente se puede hacer desde el propio grupo.

Solo se pueden añadir dispositivos del mismo tipo a un grupo. Por ejemplo, en **Hyper-V** puede crear un grupo de equipos virtuales de Hyper-V. En **Equipos con agentes**, puede crear un grupo de equipos con los agentes instalados. No se puede crear un grupo en **Todos los dispositivos**.

Un único dispositivo puede ser miembro de más de un grupo.

Grupos integrados

Cuando se registre un dispositivo, este aparecerá en uno de los grupos raíz integrados de la pestaña **Dispositivos**.

No es posible modificar ni eliminar los grupos raíz. *No* puede aplicar planes a los grupos raíz.

Algunos de los grupos raíz contienen grupos subraíz integrados. Estos grupos *no* se pueden modificar ni eliminar. No obstante, *puede* aplicar planes a grupos subraíz integrados.

Grupos personalizados

La protección de todos los dispositivos de un grupo integrado con un solo plan de protección podría no ser satisfactoria por los diferentes roles de los equipos. Los datos incluidos en la copia de seguridad son específicos de cada departamento; algunos datos se han de incluir en la copia de seguridad frecuentemente, mientras que otros datos se incluyen en la copia de seguridad dos veces al año. Por lo tanto, es posible que desee crear varios planes de protección aplicables a los distintos conjuntos de equipos. En este caso, considere la creación de grupos personalizados.

Un grupo personalizado puede contener uno o más grupos anidados. Cualquier grupo personalizado puede editarse o eliminarse. Estos son los siguientes tipos de grupos personalizados:

- **Grupos estáticos**

  Los grupos estáticos contienen los equipos añadidos manualmente a ellos. El contenido del grupo estático nunca cambia a menos que añada o elimine explícitamente un equipo.

  Ejemplo: Crea un grupo personalizado para el departamento de contabilidad y añade manualmente los equipos de los contables a este grupo. Una vez aplicado el plan de protección al grupo, los equipos de los contables pasan a estar protegidos. Si se contrata un nuevo contable, deberá añadir el nuevo equipo al grupo manualmente.
- **Grupos dinámicos**

Los grupos dinámicos contienen los equipos añadidos automáticamente de conformidad con los criterios de búsqueda especificados al crear un grupo. El contenido del grupo dinámico cambia automáticamente. Los equipos permanecerán en el grupo siempre que cumpla los criterios especificados.

Ejemplo 1: Los nombres de servidor host de los equipos que pertenecen al departamento de contabilidad contienen la palabra "contabilidad". Especifique el nombre parcial del equipo como criterio de pertenencia al grupo y aplique un plan de protección a este. Si se contrata un nuevo contable, se añadirá el nuevo equipo al grupo en cuanto el mismo se registre y, por lo tanto, estará protegido automáticamente.

Ejemplo 2: El departamento de contabilidad forma una unidad organizativa de Active Directory independiente. Especifique la OU de contabilidad como criterios de pertenencia al grupo y aplique un plan de protección a este. Si se contrata un nuevo contable, se añadirá el nuevo equipo al grupo en cuanto el mismo se registre y se añada a la OU (lo que ocurra primero), por lo que estará protegido automáticamente.

Creación de un grupo estático

1. Haga clic en **Dispositivos** y, a continuación, seleccione el grupo integrado que contiene los dispositivos para los que desea crear un grupo estático.
2. Haga clic en el icono de engranaje que hay al lado del grupo en el que desea crear un grupo.
3. Haga clic en **Nuevo grupo**.
4. Escriba el nombre del grupo y, a continuación, haga clic en **Aceptar**.
   El nuevo grupo aparecerá en el árbol de grupos.

Incorporación de dispositivos en grupos estáticos

1. Haga clic en **Dispositivos** y, a continuación, seleccione uno o más dispositivos que desee añadir a un grupo.
2. Haga clic en **Añadir al grupo**.
   El software muestra un árbol de grupos a los que puede añadir el dispositivo seleccionado.
3. Si desea crear un grupo nuevo, siga los pasos siguientes. De lo contrario, omita este paso.
   a. Seleccione el grupo en el que desea crear un grupo.
   b. Haga clic en **Nuevo grupo**.
   c. Escriba el nombre del grupo y, a continuación, haga clic en **Aceptar**.
4. Seleccione el grupo al que desea añadir el dispositivo y, a continuación, haga clic en **Realizado**.

Otra forma de añadir dispositivos a un grupo estático es seleccionar el grupo y hacer clic en **Añadir dispositivos**.

Creación de un grupo dinámico

1. Haga clic en **Dispositivos** y, a continuación, seleccione el grupo que contiene los dispositivos para los que desea crear un grupo dinámico.
2. Busque los dispositivos utilizando el campo de búsqueda. Puede utilizar varios atributos y los operadores descritos a continuación.
3. Haga clic en **Guardar como** junto al campo de búsqueda.

   Nota
   Algunos atributos no se admiten para la creación de grupos. Consulte la tabla de la sección de consultas de búsqueda que aparece a continuación.

4. Escriba el nombre del grupo y, a continuación, haga clic en **Aceptar**.

Consulta de búsqueda

La tabla siguiente resume los atributos disponibles que puede usar en sus consultas de búsqueda.

Atributo	Significado	Ejemplos de consultas de búsqueda	Se admite para la creación de grupos
`name`	• Nombre de host para equipos físicos • Nombre para equipos virtuales • Nombre de la base de datos • Dirección de correo electrónico para buzones de correo	`name = 'en-00'`	Sí
`parameters.MacAddress`	Dirección MAC.	`parameters.MacAddress LIKE '00-22-4D-50-25-E5'`	Sí
`comment`	Comentario dirigido a un dispositivo. Se puede especificar automática o manualmente. Valor predeterminado: • La descripción del equipo en Windows se copia	`comment = 'important machine'` `comment = ''` (todos los equipos sin ningún comentario)	Sí

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

	automáticamente como un comentario para equipos físicos que ejecutan Windows. Este valor se sincroniza cada 15 minutos.
	• Vacío para otros dispositivos.
	
	Nota
	Si añade texto de forma manual al campo del comentario, se deshabilita la sincronización automática de la descripción de Windows. Para habilitarla de nuevo, borre el comentario que ha añadido.
	
	Para actualizar los comentarios de sus dispositivos sincronizados automáticamente, reinicie Acronis Managed Machine Service en **Windows Services** o ejecute los siguientes comandos en el símbolo del sistema:
	`net stop mms`
	`net start mms`
	Para ver el comentario, en **Dispositivos**, seleccione el dispositivo,		

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

	haga clic en **Detalles** y busque la sección **Comentario**.
	
	Para añadir un comentario o modificarlo, haga clic en **Agregar** o **Editar**.
	
	Los dispositivos en los que está instalado un agente de protección tienen dos campos de comentarios independientes:
	
	• Comentario del agente
	  ◦ La descripción del equipo en Windows se copia automáticamente como un comentario para equipos físicos que ejecutan Windows. Este valor se sincroniza cada 15 minutos.
	  ◦ Vacío para otros dispositivos.
	
	Nota
	Si añade texto de forma manual al campo del comentario, se deshabilita la sincronización automática de la descripción de Windows. Para habilitarla de nuevo, borre el comentario que ha añadido.		

Atributo	Significado	Ejemplos de consultas de búsqueda	Se admite para la creación de grupos
	• Comentario del dispositivo ◦ Si el comentario del agente se especifica automáticamente, se copia como comentario del dispositivo. Los comentarios del agente que se añaden manualmente no se copian como comentarios del dispositivo. ◦ Los comentarios del dispositivo no se copian como comentarios del agente. Un dispositivo puede tener uno o ambos comentarios especificados o tener ambos en blanco. Si se especifican ambos comentarios, el comentario del dispositivo tiene prioridad. Para ver un comentario del agente, en **Configuración** > **Agentes**, seleccione el dispositivo con el agente, haga clic en **Detalles** y busque la sección **Comentario**. Para ver un comentario de dispositivo, en		

Atributo	Significado	Ejemplos de consultas de búsqueda	Se admite para la creación de grupos
	Dispositivos, seleccione el dispositivo, haga clic en **Detalles** y busque la sección **Comentario**. Para añadir un comentario o modificarlo de forma manual, haga clic en **Agregar** o **Editar**.		
`ip`	Dirección IP (solo para equipos físicos).	`ip RANGE ('10.250.176.1','10.250.176.50')`	Sí
`cpuArch`	Arquitectura de CPU. Valores posibles: • `'x64'` • `'x86'`	`cpuArch = 'x64'`	Sí
`memorySize`	Tamaño de la RAM en megabytes (MiB).	`memorySize < 1024`	Sí
`cpuName`	Nombre de CPU.	`cpuName LIKE '%XEON%'`	Sí
`insideVm`	Equipo virtual con un agente dentro. Valores posibles: • `true` • `false`	`insideVm = true`	Sí
`tzOffset`	Desfase de la zona horaria del equipo en minutos.	`tzOffset = 120`	Sí
`parameters.Architecture`	Arquitectura del sistema operativo. Valores posibles: • `'x86'` • `'x64'`	`parameters.Architecture = 'x86'`	Sí
`osName`	Nombre del sistema operativo.	`osName LIKE '%Windows XP%'`	Sí

Atributo	Significado	Ejemplos de consultas de búsqueda	Se admite para la creación de grupos
`osType`	Tipo de sistema operativo. Valores posibles: • `'windows'` • `'linux'` • `'macosx'`	`osType IN ('linux', 'macosx')`	Sí
`osProductType`	Tipo de producto de sistema operativo. Valores posibles: • `'dc'` Significa controlador de dominio. • `'server'` • `'workstation'`	`osProductType = 'server'`	Sí
`virtualType`	Tipo de máquina virtual. Valores posibles: • `'vmwesx'` Máquinas virtuales VMware. • `'mshyperv'` Máquinas virtuales Hyper-V. • `'pcs'` Máquinas virtuales Virtuozzo. • `'hci'` Máquinas virtuales de Virtuozzo Hybrid Infrastructure. • `'scale'` Máquinas virtuales de Scale Computing HC3. • `'ovirt'` Máquinas virtuales oVirt	`virtualType = 'vmwesx'`	Sí
`osSp`	Paquete de servicios del	`osSp = 1`	Sí

Atributo	Significado	Ejemplos de consultas de búsqueda	Se admite para la creación de grupos
	sistema operativo.		
`osVersionMajor`	Versión principal del sistema operativo.	`osVersionMajor = 1`	Sí
`osVersionMinor`	Versión menor del sistema operativo.	`osVersionMminor = 1`	Sí
`isOnline`	Disponibilidad del equipo. Valores posibles: • `true` • `false`	`isOnline = true`	No
`tenant`	El nombre de la unidad a la que pertenece el dispositivo.	`tenant = 'Unit 1'`	Sí
`tenantId`	El identificador de la unidad a la que pertenece el dispositivo. Para obtener el ID de la unidad, en **Dispositivos**, seleccione uno, haga clic en **Detalles** > **Todas las propiedades**. El ID aparece en el campo `ownerId`.	`tenantId = '3bfe6ca9-9c6a-4953-9cb2-a1323f454fc9'`	Sí
`state`	Estado del dispositivo. Valores posibles: • `'idle'` • `'interactionRequired'` • `'canceling'` • `'backup'` • `'recover'` • `'install'` • `'reboot'` • `'failback'` • `'testReplica'` • `'run_from_image'`	`state = 'backup'`	No

Atributo	Significado	Ejemplos de consultas de búsqueda	Se admite para la creación de grupos
	• `'finalize'` • `'failover'` • `'replicate'` • `'createAsz'` • `'deleteAsz'` • `'resizeAsz'`		
`status`	Estado de los recursos. Valores posibles: • `'notProtected'` • `'ok'` • `'warning'` • `'error'` • `'critical'`	`status = 'ok'`	No
`protectedByPlan`	Dispositivos que están protegidos por un plan de protección con un ID determinado. Para obtener el ID del plan, haga clic en **Planes** > **Copia de seguridad**, seleccione el plan, haga clic en el diagrama de la columna **Estado** y, a continuación, haga clic en un estado. Se creará una nueva búsqueda con el ID del plan.	`protectedByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	No
`okByPlan`	Dispositivos que están protegidos por un plan de protección con un ID determinado y tienen el estado **Bueno**.	`okByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	No
`errorByPlan`	Dispositivos que están protegidos por un plan de protección con un ID determinado y tienen el estado **Error**.	`errorByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	No

Atributo	Significado	Ejemplos de consultas de búsqueda	Se admite para la creación de grupos
`warningByPlan`	Dispositivos que están protegidos por un plan de protección con un ID determinado y tienen el estado **Advertencia**.	`warningByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	No
`runningByPlan`	Dispositivos que están protegidos por un plan de protección con un ID determinado y tienen el estado **Ejecutando**.	`runningByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	No
`interactionByPlan`	Dispositivos que están protegidos por un plan de protección con un ID determinado y tienen el estado **Interacción necesaria**.	`interactionByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	No
`ou`	Equipos que pertenecen a la unidad organizativa de Active Directory.	`ou IN ('RnD', 'Computers')`	Sí
`id`	ID del dispositivo. Para obtener el ID del dispositivo, debajo de **Dispositivos**, seleccione uno, haga clic en **Detalles** > **Todas las propiedades**. El ID aparece en el campo `id`.	`id != '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	Sí

`lastBackupTime`	La fecha y la hora de la última copia de seguridad realizada correctamente.
	El formato es `'AAAA-MM-DD HH:MM'`.
		`lastBackupTime > '2022-03-11'`
		`lastBackupTime <= '2022-03-11 00:15'`
		`lastBackupTime is null`
			No

`lastBackupTryTime`	La hora del último intento de realización de la copia de seguridad. El formato es `'AAAA-MM-DD`	`lastBackupTryTime >= '2022-03-11'`	No

Atributo	Significado	Ejemplos de consultas de búsqueda	Se admite para la creación de grupos
	`HH:MM'`.		
`nextBackupTime`	La hora de la siguiente copia de seguridad. El formato es `'AAAA-MM-DD HH:MM'`.	`nextBackupTime >= '2022-08-11'`	No
`agentVersion`	Versión del agente de protección instalado.	`agentVersion LIKE '12.0.*'`	Sí
`hostId`	ID interno del agente de protección. Para obtener el ID del agente de protección, debajo de **Dispositivos**, seleccione el equipo, haga clic en **Detalles** > **Todas las propiedades**. Utilice el valor `"id"` de la propiedad `agent`.	`hostId = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	Sí
`resourceType`	Tipo de recurso. Valores posibles: • `'machine'` • `'virtual_machine.vmwesx'` • `'virtual_machine.mshyperv'` • `'virtual_machine.rhev'` • `'virtual_machine.kvm'` • `'virtual_machine.xen'`	`resourceType = 'machine'` `resourceType in ('mssql_aag_database', 'mssql_database')`	Sí
`hasAsz`	Agente de protección en un equipo físico con AcronisSecure Zone. Valores posibles: • `true` • `false`	`hasAsz=true`	Sí
`chassis`	Tipo de chasis del equipo.	`chassis='laptop'`	Sí

Atributo	Significado	Ejemplos de consultas de búsqueda	Se admite para la creación de grupos
	Valores posibles: • unknown • laptop • desktop • server • other		

Nota
Si omite el valor de horas y minutos, la hora de inicio se tomará como AAAA-MM-DD 00:00 y la hora de finalización como AAAA-MM-DD 23:59:59. Por ejemplo, lastBackupTime = 2020-02-20 significa que los resultados de búsqueda incluirán todas las copias de seguridad en el intervalo entre lastBackupTime >= 2020-02-20 00:00 y lastBackupTime <= 2020-02-20 23:59:59

Operadores

La tabla siguiente resume los operadores disponibles.

Operador	Significado	Ejemplos
`AND`	Operador de conjunción lógica.	`name like 'en-00' AND tenant = 'Unit 1'`
`OR`	Operador de disyunción lógica.	`state = 'backup' OR state = 'interactionRequired'`
`IN (<value1>,... <valueN>)`	Este operador se utiliza para probar si una expresión se corresponde con algún valor de una lista de ellos.	`osType IN ('windows', 'linux')`
`NOT`	Operador de negación lógica.	`NOT(osProductType = 'workstation')`
`NOT IN (<value1>,... <valueN>)`	Este operador es el opuesto del operador `IN`.	`NOT osType IN ('windows', 'linux')`

`LIKE 'modelo de comodines'`	Este operador se utiliza para probar si una expresión se corresponde con el modelo de comodines.
	Se pueden utilizar los siguientes operadores comodín:
	• * o % El asterisco y el símbolo de porcentaje representa a ningún carácter, a
		`name LIKE 'en-00'`
		`name LIKE '*en-00'`
		`name LIKE '*en-00*'`
		`name LIKE 'en-00_'`

Operador	Significado	Ejemplos
	uno o a varios • _ El guion bajo representa un solo carácter	
`RANGE(<starting_value>, <ending_value>)`	Este operador se utiliza para probar si una expresión se encuentra dentro de un intervalo de valores.	`ip RANGE ('10.250.176.1','10.250.176.50')`
`= or ==`	Operador *Igual que*.	`osProductType = 'server'`
`!=` o `<>`	Operador *No es igual que*.	`id != '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`
`<`	Operador *Menor que*.	`memorySize < 1024`
`>`	Operador *Mayor que*.	`diskSize > 300 GB`
`<=`	Operador *Menor o igual que*.	`lastBackupTime <= '2022-05-11 00:15'`
`>=`	Operador *Mayor o igual que*.	`nextBackupTime >= '2022-09-11'`

Aplicación de un plan de protección a un grupo

1. Haga clic en **Dispositivos** y seleccione el grupo integrado que contiene a su vez el grupo al que desea aplicar un plan de protección.

   El software muestra la lista de grupos secundarios.
2. Seleccione el grupo al que desea aplicar un plan de protección.
3. Haga clic en **Copia de seguridad de grupo**.

   El software muestra la lista de planes de protección que se pueden aplicar al grupo.
4. Realice uno de los siguientes procedimientos:
   - Expanda un plan de protección existente y haga clic en **Aplicar**.
   - Haga clic en **Crear nuevo** y cree un nuevo plan de protección, como se indica en "Copia de seguridad".

Supervisión e informes

El panel de control de **Información general** le permite supervisar el estado actual de su infraestructura protegida.

La sección de **Informes** le permite generar informes a demanda y planificados sobre su infraestructura protegida. La sección está disponible solo con una licencia Advanced.

Panel de control de Información general

El panel de control de **Información general** proporciona una serie de widgets personalizables que dan una imagen general de su infraestructura protegida. Puede elegir entre más de 20 widgets, presentados como gráficos circulares, tablas, gráficos, diagramas de barras y listas. Tienen elementos interactivos que le permiten investigar y solucionar problemas. La información de los widgets se actualiza cada cinco minutos.

Con la licencia Advanced, también puede descargar el estado actual del panel de información o bien enviarlo por correo electrónico en formato .pdf o .xls. Para enviar el panel de control por correo electrónico, asegúrese de haber configurado el **Servidor de correo electrónico**.

Los widgets disponibles dependen de su edición de Cyber Protect. Los widgets predeterminados se indican a continuación:

Widget	Disponibilidad	Descripción
Ciberprotección	No disponible en las ediciones de Cyber Backup	Muestra información general sobre el tamaño de las copias de seguridad, el malware y las URL bloqueadas, las vulnerabilidades encontradas y los parches instalados.
Estado de la protección	Disponible en todas las ediciones	Muestra el estado de protección actual de todos los equipos.
Actividades	Disponible en todas las ediciones	Muestra un resumen de las actividades realizadas durante un periodo especificado.
Resumen de alertas activas	Disponible en todas las ediciones	Muestra un resumen de las alertas activas por tipo y gravedad.
Estado de instalación del parche	No disponible en las ediciones de Cyber Backup	Muestra el número de equipos agrupados por estado de instalación de parches.
Actualizaciones que faltan por categoría	No disponible en las ediciones de Cyber Backup	Muestra el número de actualizaciones que faltan por categoría.

Estado del disco	No disponible en las ediciones de Cyber Backup	Muestra el número de discos por estado.
Dispositivos	Disponible en todas las ediciones	Muestra información detallada sobre los dispositivos de su entorno.
Detalles de las alertas activas	Disponible en todas las ediciones	Muestra información detallada sobre las alertas activas.
Vulnerabilidades existentes	Disponible en todas las ediciones	Muestra las vulnerabilidades existentes de los sistemas operativos y las aplicaciones de su entorno, así como los equipos afectados.
Historial de instalación de parches	No disponible en las ediciones de Cyber Backup	Muestra información detallada sobre los parches instalados.
Elementos afectados recientemente	Disponible en todas las ediciones	Muestra información detallada sobre los equipos infectados recientemente.
Resumen de ubicaciones	Disponible en todas las ediciones	Muestra información detallada sobre las ubicaciones de la copia de seguridad.

Pasos para agregar un widget

Haga clic en **Añadir widget** y, luego, realice uno de los siguientes procedimientos:

- Haga clic en el widget que quiera añadir. El widget se añadirá con la configuración predeterminada.
- Para editar el widget antes de añadirlo, haga clic en el icono de lápiz cuando el widget esté seleccionado. Después de editar el widget, haga clic en **Listo**.

Pasos para reorganizar los widgets en el panel de información

Haga clic en los nombres de los widgets para arrastrarlos y soltarlos.

Pasos para editar un widget

Haga clic en el icono de lápiz situado al lado del nombre del widget. Al editar un widget, puede cambiarle el nombre, modificar el intervalo de tiempo, establecer filtros y agrupar filas.

Pasos para eliminar un widget

Haga clic en el signo de X situado al lado del nombre del widget.

Cyber Protection

Este widget muestra información general sobre el tamaño de las copias de seguridad, el malware y las URL bloqueadas, las vulnerabilidades encontradas y los parches instalados.

En la fila superior se muestran las estadísticas actuales:

- **Copia de seguridad realizada hoy**: la suma del tamaño de los puntos de recuperación de las últimas 24 horas.
- **Malware bloqueados**: el número de alertas activas actualmente relacionadas con malware bloqueado.
- **URL bloqueadas**: el número de alertas activas actualmente relacionadas con URL bloqueadas.
- **Vulnerabilidades existentes**: el número de vulnerabilidades que existen actualmente.
- **Parches listos para instalarse**: el número de parches disponibles actualmente para instalarse.

En la fila inferior se muestran las estadísticas globales:

- El tamaño comprimido de todas las copias de seguridad
- El número acumulado de elementos de malware bloqueados en todos los equipos
- El número acumulado de URL bloqueadas en todos los equipos
- El número acumulado de vulnerabilidades detectadas en todos los equipos
- El número acumulado de parches o actualizaciones instalados en todos los equipos

Estado de la protección

Estado de la protección

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

Un equipo puede encontrarse en uno de los siguientes estados:

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

Si hace clic en el estado del equipo, se le redirigirá a la lista de equipos con este estado para que obtenga más información.

Equipos detectados

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

Supervisión del estado del disco

La supervisión del estado del disco proporciona información sobre el estado actual del disco y una previsión para que pueda evitar una pérdida de datos que pueda estar relacionada con un fallo del disco. Son compatibles tanto los discos duros como los SSD.

Limitaciones:

- La previsión del estado del disco solo se puede realizar en equipos Windows.
- Únicamente se supervisan los discos de equipos físicos. Los discos de máquinas virtuales no se pueden supervisar ni aparecen en los widgets sobre el estado del disco.
- No se admiten configuraciones RAID.
- En unidades NVMe, solo es posible supervisar el estado del disco de las unidades que comunican los datos SMART mediante la API de Windows. La supervisión del estado del disco no es compatible con las unidades NVMe que necesitan leer los datos SMART directamente desde la unidad.

El estado del disco puede ser uno de los siguientes:

- **OK**:
  El estado del disco se encuentra entre el 70 y el 100 %.
- **Advertencia**:
  El estado del disco se encuentra entre el 30 y el 70 %.
- **Crítico**:
  El estado del disco se encuentra entre el 0 y el 30 %.
- **Calculando datos del disco**:
  Se están calculando tanto el estado del disco actual como su previsión

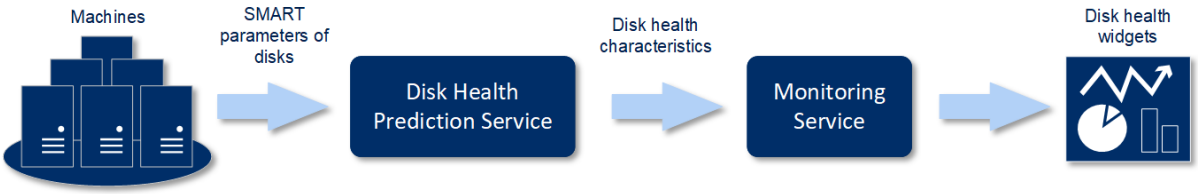
Cómo funciona

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

1. El agente de protección recopila los parámetros SMART de los discos y envía estos datos al servicio de predicción de estado del disco:
   - SMART 5: Número de sectores reasignados.
   - SMART 9: Horas durante las que está encendido.
   - SMART 187: Errores incorregibles de los que se ha informado.
   - SMART 188: Comando de tiempo de espera.
   - SMART 197: Número de sectores pendientes actuales.
   - SMART 198: Número de sectores incorregibles fuera de línea.
   - SMART 200: Tasa de error de escritura.

2. El servicio de previsión de estado de disco procesa los parámetros SMART recibidos, realiza predicciones y proporciona las siguientes características del estado del disco:
   - Estado actual del disco: OK, Advertencia, Crítico.
   - Previsión del estado del disco: negativa, estable, positiva.
   - Probabilidad de la previsión del estado del disco en porcentaje.

   El periodo de predicción siempre es de un mes.
3. El servicio de supervisión recibe estas características y muestra la información relevante en los widgets del estado del disco en la consola web de Cyber Protect.



Widgets sobre el estado del disco

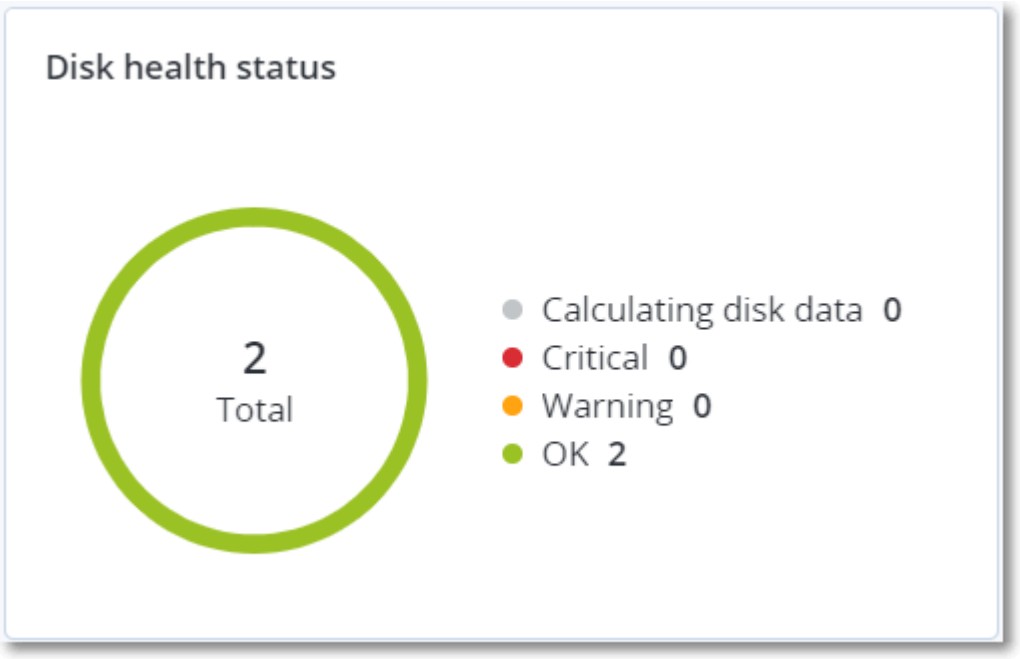
Los resultados de la supervisión del estado del disco se muestran en los siguientes widgets que están disponibles en la consola web de Cyber Protect.

- **Resumen del estado del disco**: Es un widget en estructura de árbol con dos niveles de datos que se pueden cambiar al desplazarse.
  - Nivel de equipo:
    Muestra información resumida sobre el estado del disco de todos los equipos de la unidad organizativa seleccionada. Solo se muestra el estado del disco más crítico. El resto de los estados aparecen en la información sobre herramientas cuando se pasa el ratón por encima de un bloque concreto. El tamaño del bloque del equipo depende del tamaño total de todos los discos del equipo. El color del bloque del equipo depende del estado del disco más crítico encontrado.

- Nivel de disco:
  Muestra el estado actual de todos los discos para el equipo seleccionado. Cada bloque de discos muestra el porcentaje de una de las siguientes previsiones del estado del disco y su probabilidad:
  - Se degradará
  - Permanecerá estable

- Mejorará

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



Alertas sobre el estado del disco

La comprobación del estado del disco se ejecuta cada 30 minutos, pero la alerta correspondiente se genera una vez al día. Cuando el estado del disco cambia de **Advertencia** a **Crítico**, se genera siempre una alerta.

Nombre de la alerta	Gravedad	Estado del disco	Descripción
Es posible que falle el disco	Advertencia	(30 – 70)	Es probable que el disco <disk name> en este equipo falle en el futuro. Ejecute lo antes posible una copia de seguridad de imágenes completa de este disco, reemplácelo y, a continuación, recupere la imagen en el nuevo disco.
El fallo del disco es inminente	Crítico	(0 – 30)	El disco <disk name> en este equipo está en estado crítico y es bastante probable que falle muy pronto. En este punto, no se recomienda realizar una copia de seguridad de imágenes de este disco, ya que la carga añadida podría hacer que el disco falle. Realice inmediatamente una copia de seguridad de los archivos más importantes de este disco y reemplácelo.

Mapa de protección de datos

Gracias a la función del mapa de protección de datos, puede descubrir todos los datos que sean importantes para usted y obtener información detallada sobre el número, el tamaño, la ubicación y el estado de protección de todos los archivos importantes en una vista escalable representada con una estructura de árbol.

El tamaño de cada bloque depende del tamaño o el número total de archivos importantes que pertenecen a una unidad organizativa o un equipo.

Los archivos pueden tener uno de los siguientes estados de protección:

- **Crítico**: hay entre un 51 y un 100 % de archivos sin proteger con las extensiones que ha especificado de los que no se está realizando ni se va a realizar ninguna copia de seguridad con la configuración de copias de seguridad existentes para la ubicación, el inquilino cliente o el equipo seleccionado.
- **Bajo**: hay entre un 21 y un 50 % de archivos sin proteger con las extensiones que ha especificado de los que no se está realizando ni se va a realizar ninguna copia de seguridad con la configuración de copias de seguridad existentes para la ubicación, el inquilino cliente o el equipo seleccionado.
- **Medio**: hay entre un 1 y un 20 % de archivos sin proteger con las extensiones que ha especificado de los que no se está realizando ni se va a realizar ninguna copia de seguridad con la

configuración de copias de seguridad existentes para la ubicación, el inquilino cliente o el equipo seleccionado.

- **Alto**: todos los archivos con las extensiones que ha especificado están protegidos (se ha realizado una copia de seguridad de ellos) para la ubicación o el equipo seleccionado.

Los resultados de la evaluación de la protección de datos se encuentran en el panel de control en el widget del mapa de protección de datos, un widget en estructura de árbol en el que se muestra información sobre el nivel de un equipo.

Pase el ratón por encima del bloque de color para ver más información sobre el número de archivos que no están protegidos y su ubicación. Para protegerlos, haga clic en **Proteger todos los archivos**.

Widgets de evaluación de vulnerabilidades

Equipos vulnerables

Este widget muestra los equipos vulnerables por gravedad de la vulnerabilidad.

La vulnerabilidad encontrada tendrá uno de los siguientes niveles de gravedad de acuerdo con el sistema Common Vulnerability Scoring System (CVSS) v3.0:

- Protegido: no se ha encontrado ninguna vulnerabilidad
- Crítico: 9,0-10,0 CVSS
- Alto: 7,0-8,9 CVSS
- Medio: 4,0-6,9 CVSS
- Bajo: 0,1-3,9 CVSS
- Ninguno: 0,0 CVSS

Vulnerabilidades existentes

Este widget muestra las vulnerabilidades que existen actualmente en los equipos. En el widget **Vulnerabilidades existentes**, hay dos columnas en las que se muestran determinadas marcas de hora y fecha:

- **Primera detección**: fecha y hora en que se detectó por primera vez una vulnerabilidad en el equipo.
- **Última detección**: fecha y hora en que se detectó por última vez una vulnerabilidad en el equipo.

Widgets de instalación de parches

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

Estado de instalación del parche

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

- **Instalado**: todos los parches disponibles están instalados en el equipo.
- **Reinicio necesario**: después de la instalación de un parche, es necesario reiniciar el equipo.
- **Fallida**: la instalación del parche ha fallado en el equipo.

Resumen de la instalación del parche

Este widget muestra el resumen de parches por su estado de instalación.

Historial de instalación de parches

Este widget muestra información detallada sobre los parches instalados en los equipos.

Actualizaciones que faltan por categoría

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

- Actualizaciones de seguridad
- Actualizaciones críticas
- Otros

Detalles del análisis de copias de seguridad

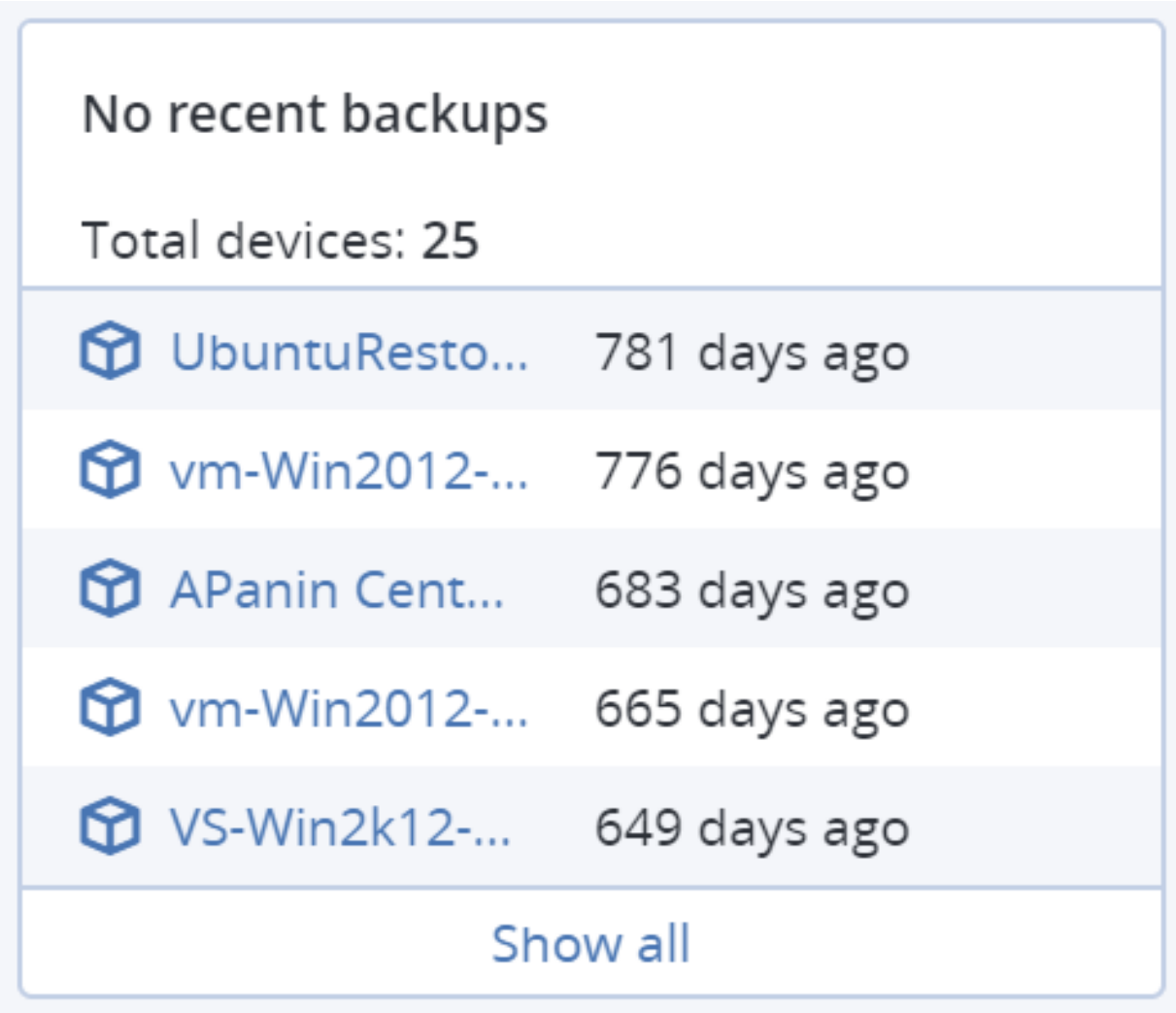
Este widget solo está disponible si Scan Service está instalado en el servidor de gestión. Este widget muestra información detallada sobre las amenazas detectadas en las copias de seguridad.

Elementos afectados recientemente

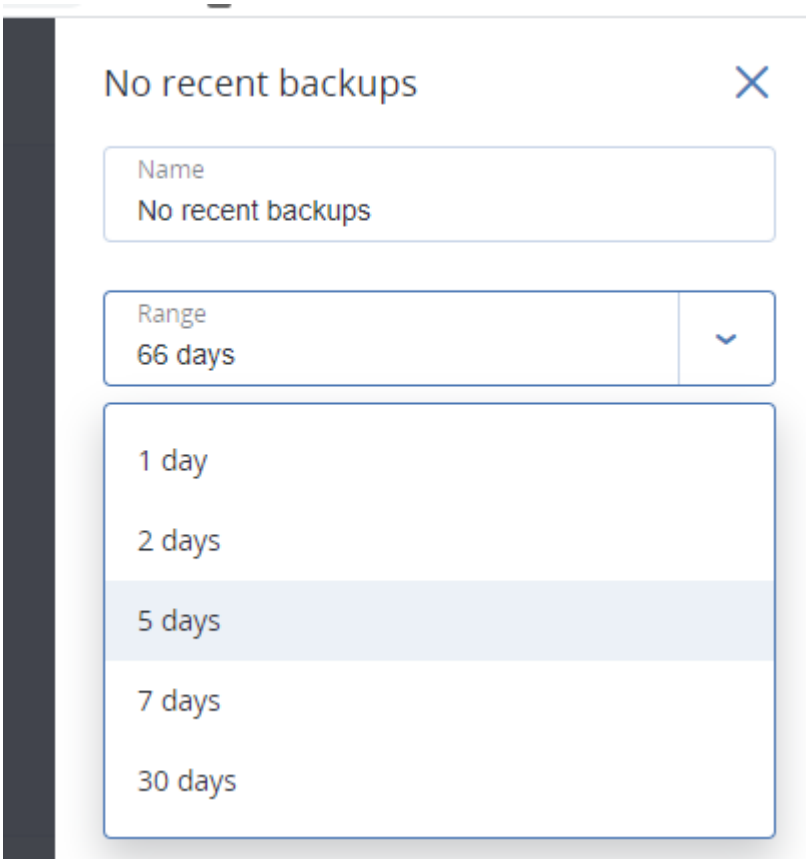
Este widget muestra información detallada sobre los equipos infectados recientemente. Aquí puede encontrar información sobre la amenaza que se detectó y el número de archivos que fueron infectados.

No hay ninguna copia de seguridad reciente

Este widget muestra las cargas de trabajo con planes de protección aplicados cuya fecha de último acceso con éxito es anterior al rango de fechas especificado en la configuración del widget.



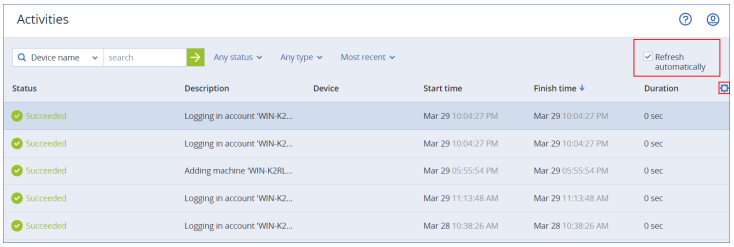
De forma predeterminada, cuando añade este widget, se muestra la información de los últimos cinco días. Puede utilizar el menú desplegable para seleccionar un periodo diferente o indicar el número de días manualmente. Solo puede indicar 180 días como máximo.



La pestaña Actividades

La pestaña **Actividades** ofrece un resumen de las actividades de los últimos 90 días.

Para personalizar la vista de la pestaña **Actividades**, haga clic en el icono del engranaje y seleccione las columnas que desea ver. Para ver el progreso de la actividad en tiempo real, seleccione la casilla de verificación **Actualizar automáticamente**. Tenga en cuenta que las actualizaciones frecuentes de varias actividades podrían mermar el rendimiento del servidor de administración.



Puede buscar las actividades enumeradas a través de los siguientes criterios:

- **Nombre del dispositivo**
  El equipo en el que se lleva a cabo la actividad.
- **Iniciado por**
  La cuenta que inició la actividad.

También puede filtrar las actividades por las siguientes propiedades:

- **Estado**
  Por ejemplo, completada, con errores, en progreso o cancelada.
- **Tipo**
  Por ejemplo, aplicar plan, eliminar copias de seguridad o instalar actualizaciones de software.
- **Período**
  Por ejemplo, las actividades más recientes, las actividades de las últimas 24 horas, o las actividades durante un plazo específico de tiempo dentro del período de retención predeterminado.

Para modificar el periodo de retención predeterminado, edite el archivo de configuración task_manager.yaml.

Para cambiar el período de retención

1. En el equipo que ejecuta el servidor de gestión, abra el siguiente archivo de configuración en un editor de texto:
   - En Windows: `%Program Files%\Acronis\TaskManager\task_manager.yaml`
   - En Linux: `/usr/lib/Acronis/TaskManager/task_manager.yaml`
2. Busque la siguiente sección:

```
database:
  connection-string: ""
  run-cleanup-at: "23:59"
  cleanup-batch-size: 10
  max-cleanup-retries: 10
  log-queries: false
  max-transaction-retries: 10
  shards:
   - connection-string: sqlite://task-manager.sqlite
     days-to-keep: 90
     space: "default"
     key: "00000000-0000-0000-0000-000000000000"
```

3. Edite la línea `days-to-keep` a su conveniencia.
   Por ejemplo:

```
days-to-keep: 30
```

   Nota
   Puede modificar el periodo de retención según sus necesidades. Aumentar el período de retención merma el rendimiento del servidor de gestión.

4. Reinicie **Acronis Service Manager Service** como se indica en "Pasos para reiniciar el servicio del administrador de servicios de Acronis" (p. 243).

Informes

Puede utilizar informes predefinidos o crear un informe personalizado. Un informe puede incluir cualquier conjunto de los widgets del panel de control.

Solo puede configurar informes para las unidades que gestione.

Los informes se pueden enviar a través de correo electrónico o descargarlos de forma programada. Para enviar los informes a través del correo electrónico, asegúrese de que se hayan configurado las opciones del **Servidor de correo electrónico**. Si desea procesar un informe con un software de terceros, programe guardar el informe en el formato .xlsx en una carpeta específica.

Los informes disponibles dependen de su edición de Cyber Protect. Los informes predeterminados se indican a continuación:

Nombre del informe	Disponibilidad	Descripción
Alertas	Cyber Backup Advanced Cyber Protect Advanced	Muestra las alertas que se producen durante un periodo especificado.
Detalles del análisis de copias de seguridad	Cyber Protect Advanced	Muestra información detallada sobre las amenazas detectadas en las copias de seguridad.
Copias de seguridad	Cyber Backup Advanced Cyber Protect Advanced	Muestra los detalles de las copias de seguridad y puntos de recuperación actuales.
Estado actual	Cyber Backup Advanced Cyber Protect Advanced	Muestra el estado actual de su entorno.
Actividades diarias	Cyber Backup Advanced Cyber Protect Advanced	Muestra un resumen de las actividades realizadas durante un periodo especificado.
Mapa de protección de datos	Cyber Protect Advanced	Muestra información detallada sobre el número, el tamaño, la ubicación y el estado de protección de todos los archivos importantes de los equipos.
Amenazas	Cyber Backup	Muestra información sobre los equipos afectados por

detectadas	Advanced Cyber Protect Advanced	número de amenazas bloqueadas, así como la de los equipos en buen estado y los vulnerables.
Equipos detectados	Cyber Backup Advanced Cyber Protect Advanced	Enumera todos los equipos detectados en la red de la organización.
Predicción del estado del disco	Cyber Protect Advanced	Muestra predicciones de cuándo se deteriorará el disco duro/SSD y el estado actual del disco.
Vulnerabilidades existentes	Cyber Backup Advanced Cyber Protect Advanced	Muestra las vulnerabilidades existentes de los sistemas operativos y las aplicaciones de su entorno, así como los equipos afectados.
Licencias	Cyber Backup Advanced Cyber Protect Advanced	Muestra un resumen de las licencias disponibles.
Ubicaciones	Cyber Backup Advanced Cyber Protect Advanced	Muestra estadísticas sobre el uso de las ubicaciones de la copia de seguridad durante un periodo especificado.
Resumen de gestión de parches	Cyber Protect Advanced	Muestra el número de parches que faltan, los instalados y los aplicables. Puede desglosar el informe para obtener información sobre los parches que faltan y los instalados, así como detalles de todos los sistemas.
Resumen	Cyber Backup Advanced Cyber Protect Advanced	Muestra un resumen de los dispositivos protegidos durante un periodo especificado.
Actividades de la cinta	Cyber Backup Advanced Cyber Protect Advanced	Muestra una lista de cintas que se usaron durante las últimas 24 horas.
Actividades semanales	Cyber Backup Advanced Cyber Protect Advanced	Muestra un resumen de las actividades realizadas durante un periodo especificado.

Operaciones básicas con informes

- Para ver un informe, haga clic en su nombre.
- Para operaciones adicionales con un informe, haga clic en el icono de puntos suspensivos (...). Desde dentro del informe están disponibles las mismas operaciones.

Pasos para añadir un informe

1. Haga clic en **Añadir informe**.
2. Realice uno de los siguientes procedimientos:
   - Para añadir un informe predefinido, haga clic en su nombre.
   - Para añadir un informe personalizado, haga clic en **Personalizar**. Se añadirá un nuevo informe con el nombre **Personalizado** a la lista de informes. Abra este informe y añada widgets al mismo.
3. [Opcional] Arrastre y suelte los widgets para reorganizarlos.
4. [Opcional] Edite el informe tal y como se describe a continuación.

Pasos para editar un informe

1. Haga clic en el icono de puntos suspensivos (...) que se encuentra junto al nombre del informe y, a continuación, haga clic en **Configuración**.
2. Edite el informe. Puede:
   - Cambiarle el nombre
   - Cambiar el intervalo de tiempo de todos los widgets incluidos en él
   - Planificar su envío por correo electrónico en formato .pdf o .xls
3. Haga clic en **Guardar**.

Para programar un informe

1. Seleccione un informe y haga clic en **Programación**.
2. Habilite el conmutador **Enviar un informe programado**.
3. Seleccione si enviar el informe a través de correo electrónico, guardarlo en una carpeta o ambas opciones. En función de la elección, especifique las direcciones de correo electrónico, la ruta de la carpeta o ambas opciones.
4. Seleccione el formato del informe: .pdf, .xlsx o ambos.
5. Seleccione el periodo del informe: 1 día, 7 días o 30 días.
6. Seleccione los días y la hora en que se enviará o guardará el informe.
7. Haga clic en **Guardar**.

Exportación e importación de la estructura del informe

Puede exportar e importar la estructura del informe (el conjunto de widgets y los ajustes de la programación) a un archivo .json. Puede resultar útil en caso de tener que volver a instalar el servidor de gestión o para copiar la estructura del informe a un servidor de gestión diferente.

Para exportar la estructura del informe, seleccione un informe y haga clic en **Exportar**.

Para importar la estructura del informe, haga clic en **Crear informe** y, a continuación, en **Importar**.

Volcado de los datos del informe

Puede guardar un volcado de los datos del informe en un archivo .csv. El volcado incluye todos los datos del informe (sin filtrado) para un intervalo de tiempo personalizado.

El software genera el volcado de datos sobre la marcha. Si especifica un periodo largo, esta acción puede tardar bastante tiempo.

Para volcar los datos del informe

1. Seleccione un informe y haga clic en **Abrir**.
2. Haga clic en el icono de puntos suspensivos (...) de la esquina superior derecha y, a continuación, en **Volcar datos**.
3. En **Ubicación**, especifique la ruta de la carpeta para el archivo .csv.
4. En **Intervalo de tiempo**, especifique el intervalo de tiempo.
5. Haga clic en **Guardar**.

Configuración de la gravedad de las alertas

Una alerta es un mensaje que le advierte sobre problemas reales o posibles. Puede utilizar las alertas de varias formas:

- La sección **Alertas** de la pestaña **Resumen** le permite identificar y solucionar problemas rápidamente supervisando las alertas producidas.
- En **Dispositivos**, el estado del dispositivo se deriva de las alertas. La columna **Estado** le permite filtrar los dispositivos con problemas.
- Al configurar las notificaciones por correo electrónico, puede elegir qué alertas desencadenarán una notificación.

Una alerta puede tener una de las gravedades siguientes:

- **Crítico**
- **Error**
- **Advertencia**

Puede cambiar la gravedad de una alerta o desactivar la alerta por completo utilizando el archivo de configuración de alertas como se indica a continuación. Para realizar esta operación es necesario reiniciar el servidor de gestión.

Cambiar la gravedad de una alerta no afecta a las alertas que ya se han generado.

Archivo de configuración de alertas

El archivo de configuración se encuentra en el equipo que ejecuta el servidor de gestión.

- En Windows: `<installation_path>`**\AlertManager\alert_manager.yaml**
  En este caso, `<installation_path>` es la ruta de instalación del servidor de gestión. De manera predeterminada, es **%ProgramFiles%\Acronis** .
- En Linux: **/usr/lib/Acronis/AlertManager/alert_manager.yaml**

El archivo se estructura como documento YAML. Cada alerta es un elemento de la lista `alertTypes`.

La clave `name` sirve para identificar la alerta.

La clave `severity` define la gravedad de la alerta. Debe tener uno de los valores siguientes: `critical`, `error` o `warning`.

La clave opcional `enabled` define si la alerta está habilitada o no. Su valor debe ser `true` o `false`. De forma predeterminada (es decir, sin esta clave) todas las alertas están habilitadas.

Para cambiar la gravedad de una alerta o desactivarla

1. En el equipo en el que esté instalado el servidor de gestión, abra el archivo **alert_manager.yaml** en un editor de texto.
2. Busque la alerta que quiera cambiar o deshabilitar.
3. Realice uno de los siguientes procedimientos:
   - Para modificar la gravedad de la alerta, cambie el valor de la clave `severity`.
   - Para deshabilitar la alerta, añada la clave `enabled` y, luego, establezca su valor en `false`.
4. Guarde el archivo.
5. Reinicie el servicio del servidor de gestión como se indica arriba.

Para reiniciar el servicio del servidor de gestión en Windows

1. En el menú **Inicio**, haga clic en **Ejecutar** y luego escriba **cmd**.
2. Haga clic en **Aceptar**.
3. Ejecute los siguientes comandos:

```
net stop acrmngsrv
net start acrmngsrv
```

Para reiniciar el servicio del servidor de gestión en Linux

1. Abra el **Terminal**.
2. Ejecute el comando siguiente en cualquier directorio:

```
sudo service acronis_ams restart
```

Opciones de almacenamiento avanzadas

Dispositivos de cintas

Las siguientes secciones describen en detalle cómo utilizar dispositivos de cintas para almacenar copias de seguridad.

¿Qué es un dispositivo de cintas?

Un **dispositivo de cintas** es un término genérico que se refiere a una biblioteca de cintas o una unidad de cintas autónoma.

Una **biblioteca de cintas** (biblioteca robotizada) es un dispositivo de alta capacidad de almacenamiento que contiene:

- una o más unidades de cinta
- múltiples (hasta varios miles) ranuras para sujetar cintas
- uno o más cambiadores (mecanismos robotizados) con la función de mover las cintas entre las ranuras y las unidades de cintas.

También puede contener otros componentes, como lectores de códigos de barras o impresoras de códigos de barras.

Un **autocargador** es un tipo específico de bibliotecas de cintas. Contiene una unidad, varias ranuras, un cambiador y un lector de códigos de barras (opcional).

Una **unidad de cintas autónoma** (también denominada **cinta continua**) contiene una ranura y solo puede mantener una cinta por vez.

Información general sobre la compatibilidad de cintas

Los agentes de protección pueden realizar la copia de seguridad de los datos a un dispositivo de cinta directamente o a través de un nodo de almacenamiento. En cualquier cosa, se garantiza la operación completamente automática del dispositivo de cintas. Cuando un dispositivo de cintas con varias unidades se conecta a un nodo de almacenamiento, es posible realizar la copia de seguridad de múltiples agentes a las cintas.

Compatibilidad con RSM y software de terceros

Coexistencia con software de terceros

No se puede trabajar con cintas en un equipo en el que se ha instalado software de terceros con herramientas de gestión de cintas propias. Para usar cintas en un equipo tal, tiene que desinstalar o desactivar el software de gestión de cintas de terceros.

Administrador de almacenamiento extraíble (RSM) de Windows

Los agentes de protección y los nodos de almacenamiento no utilizan RSM. Al detectar el dispositivo de cintas, desactivan el dispositivo desde RSM (a menos que otro software lo esté utilizando). Mientras desee trabajar con el dispositivo de cintas, asegúrese de que ni un usuario ni un software de terceros habilite el dispositivo en RSM. Si el dispositivo de cintas está habilitado en RSM, repita la detección del dispositivo de cintas.

Hardware compatible

Acronis Cyber Protect es compatible con dispositivos SCSI externos. Son dispositivos conectados al canal de fibra o utilizar las interfaces SCSI, iSCSI y Serial Attached SCSI (SAS). Además, Acronis Cyber Protect es compatible con dispositivos de cintas conectados por USB.

En Windows, Acronis Cyber Protect puede realizar la copia de seguridad a un dispositivo de cintas incluso si los controladores para el cambiador de dispositivos no están instalados. Dicho dispositivo de cintas se muestra en el **Administrador de dispositivos** como **Cambiador de dispositivos desconocido**. Sin embargo, deben instalarse los controladores para el dispositivo. En Linux y en los dispositivos de arranque, no es posible realizar la copia de seguridad a un dispositivo de cintas sin controladores.

El reconocimiento de los dispositivos conectados a IDE o SATA no está garantizado. Depende de si los controladores adecuados se han instalado en el sistema operativo.

Para saber si su dispositivo es compatible, use la Herramienta de compatibilidad del hardware como se indica en http://kb.acronis.com/content/57237. Puede enviar a Acronis un informe acerca de los resultados de la prueba. La lista Compatibilidad del hardware contiene todas las compatibilidades confirmadas: https://go.acronis.com/acronis-cyber-protect-advanced-tape-hcl.

Base de datos de gestión de cintas

La información sobre todos los dispositivos de cintas conectados a un equipo se almacena en la base de datos de gestión de cintas. La ruta predeterminada de la base de datos es la siguiente:

- En Windows XP/Server 2003: `%ALLUSERSPROFILE%\Application Data\Acronis\BackupAndRecovery\ARSM\Database`.
- En Windows 7 y versiones posteriores de Windows: `%PROGRAMDATA%\Acronis\BackupAndRecovery\ARSM\Database`.
- En Linux: `/var/lib/Acronis/BackupAndRecovery/ARSM/Database`.

El tamaño de la base de datos depende de la cantidad de copias de seguridad almacenadas en las cintas y es igual a aproximadamente 10 MB por cada cien copias de seguridad. La base de datos puede ser grande si la biblioteca de cintas contiene miles de copias de seguridad. En este caso, puede almacenar la base de datos de cintas en un volumen diferente.

Para reubicar la base de datos en Windows:

1. Detenga el servicio Removable Storage Management.
2. Mueva todos los archivos de la ubicación predeterminada a la nueva ubicación.
3. Localice la clave de registro `HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\ARSM\Settings`.
4. Especifique la nueva ruta de la ubicación en el valor de registro `ArsmDmlDbProtocol`. La cadena puede tener hasta 32765 caracteres.
5. Inicie el servicio Removable Storage Management.

Para reubicar la base de datos en Linux:

1. Detenga el servicio `acronis_rsm`.
2. Mueva todos los archivos de la ubicación predeterminada a la nueva ubicación.
3. Abra el archivo de configuración `/etc/Acronis/ARSM.config` en un editor de texto.
4. Localice la línea `<value name="ArsmDmlDbProtocol" type="TString">`.
5. Cambie la ruta en esta línea.
6. Guarde el archivo.
7. Inicie el servicio `acronis_rsm`.

La carpeta `TapeLocation`

La carpeta `TapeLocation` contiene una caché de los metadatos del sistema de archivos de todos los volúmenes con copia de seguridad en las cintas.

La ruta de la carpeta predeterminada `TapeLocation` es:

- En Windows XP/Server 2003: `%ALLUSERSPROFILE%\Application Data\Acronis\BackupAndRecovery\TapeLocation`
- En Windows 7 y posterior: `%PROGRAMDATA%\Acronis\BackupAndRecovery\TapeLocation`
- En Linux: `/var/lib/Acronis/BackupAndRecovery/TapeLocation`

El tamaño de la carpeta `TapeLocation` representa aproximadamente entre el 0,5 y el 1 % del tamaño de todas las copias de seguridad en las cintas. Para las copias de seguridad a nivel de disco con la opción de recuperación de archivos habilitada, el tamaño de la carpeta `TapeLocation` podría ser ligeramente mayor en función del número de archivos con copia de seguridad.

Parámetros para escribir en cintas

Los parámetros de escritura en cintas (tamaño de bloque y de caché) le permiten ajustar el software para alcanzar el máximo rendimiento. Ambos parámetros son obligatorios para escribir en cintas, pero normalmente solo es necesario ajustar el tamaño de bloque. El valor óptimo depende del tipo de dispositivo de cintas y de los datos para los que se realiza una copia de seguridad, como el número de archivos y su tamaño.

Nota
Cuando el software lee desde una cinta, utiliza el mismo tamaño de bloque que se utilizó al escribir en ella. Si el dispositivo de cintas no admite este tamaño de bloque, la lectura falla.

Los parámetros se configuran en cada equipo con un dispositivo de cintas conectado. Puede ser un equipo donde hay instalado un agente o un nodo de almacenamiento. En un equipo que ejecuta Windows, la configuración se realiza en el registro; en una máquina Linux, se realiza en el archivo de configuración **/etc/Acronis/BackupAndRecovery.config**.

En Windows, cree las claves de registro respectivas y sus valores DWORD. En Linux, añada el siguiente texto al final del archivo de configuración, justo antes de la etiqueta `</registry>`:

```
<key name="TapeLocation">
     <value name="WriteCacheSize" type="Dword">
          "value"
     </value>
     <value name=DefaultBlockSize" type="Dword">
          "value"
     </value>
</key>
```

DefaultBlockSize

Este es el tamaño de bloque (en bytes) empleado al escribir en cintas.

Valores posibles: 0, 32, 64, 128, 256, 512, 1024, 2048, 4096, 8192, 16384, 32768, 65536, 131072, 262144, 524288, 1048576.

Si el valor es 0 o el parámetro está ausente, el tamaño de bloque se determina del siguiente modo:

- En Windows, el valor se toma del controlador del dispositivo de cintas.
- En Linux, el valor es de **64 KB**.

Clave de registro (en un equipo que ejecuta Windows): **HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\BackupAndRecovery\TapeLocation\DefaultBlockSize**

Línea en /etc/Acronis/BackupAndRecovery.config (en un equipo que ejecuta Linux):

```
     <value name=DefaultBlockSize" type="Dword">
          "value"
     </value>
```

Si la unidad de cinta no admite el valor especificado, el software lo divide entre dos hasta que se alcanza el valor aplicable o se llega a los 32 bytes. Si no se encuentra el valor aplicable, el software multiplica el valor especificado por dos hasta que se alcanza el valor aplicable o se llega a 1 MB. Si el controlador no acepta ningún valor, la copia de seguridad fallará.

WriteCacheSize

Este es el tamaño de búfer (en bytes) empleado al escribir en cintas.

Valores posibles: 0, 32, 64, 128, 256, 512, 1024, 2048, 4096, 8192, 16384, 32768, 65536, 131072, 262144, 524288, 1048576, pero no menos que el valor del parámetro **DefaultBlockSize**.

Si el valor es 0, o si el parámetro está ausente, el tamaño de búfer es de **1 MB**. Si el sistema operativo no admite este valor, el software lo divide entre dos hasta que se encuentra el valor aplicable o hasta que se alcanza el valor del parámetro **DefaultBlockSize**. Si no se encuentra el valor admitido por el sistema operativo, la copia de seguridad fallará.

Clave de registro (en un equipo que ejecuta Windows):
HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\BackupAndRecovery\TapeLocation\WriteCacheSize

Línea en /etc/Acronis/BackupAndRecovery.config (en un equipo que ejecuta Linux):

```
<value name="WriteCacheSize" type="Dword">
    "value"
</value>
```

Si especifica un valor distinto de cero no admitido por el sistema operativo, la copia de seguridad fallará.

Opciones de copia de seguridad relacionadas con la cinta

Puede configurar las opciones de copia de seguridad de **Gestión de cintas** para determinar:

- Habilitar la recuperación de archivos de las copias de seguridad del disco almacenadas en cintas.
- Si devolver las cintas a las ranuras de unidad después de que se complete el plan de protección.
- Si expulsar cintas después de que se complete la copia de seguridad.
- Si utilizar una cinta disponible para cada copia de seguridad completa.
- Si sobrescribir una cinta al crear una copia de seguridad completa (solo para unidades de cintas autónomas).
- Si utilizar juegos de cintas para diferenciar las cintas utilizadas (por ejemplo, para copias de seguridad creadas en diferentes días de la semana o para copias de seguridad de diferentes tipos de equipos).

Operaciones paralelas

Acronis Cyber Protect puede realizar simultáneamente las operaciones con varios componentes de un dispositivo de cintas. Durante una operación que utiliza una unidad (copia de seguridad, recuperación, nueva exploración o borrado), puede iniciar la operación que utiliza un cambiador (mover una cinta a otra ranura o expulsar una cinta) y viceversa. Si su biblioteca de cintas tiene más de una unidad, también puede ejecutar la operación que utiliza una de las unidades durante una

operación con unidad. Por ejemplo, varios equipos pueden realizar la copia de seguridad o recuperación simultáneamente con diferentes unidades de la misma biblioteca de cintas.

La operación de detectar los nuevos dispositivos de cintas puede realizarse simultáneamente con cualquier otra operación. Durante el inventario, no está disponible ninguna otra operación, excepto para detectar nuevos dispositivos de cintas.

Las operaciones que no pueden realizarse en paralelo se pondrán en cola.

Limitaciones

Las limitaciones del uso del dispositivo de cintas son las siguientes:

1. No se admiten dispositivos de cintas cuando un equipo se inicia desde dispositivos de arranque basados en Linux de 32 bits.
2. No es posible realizar la copia de seguridad de los tipos de datos siguientes en cintas: Buzones de correo de Microsoft 365, buzones de correo de Microsoft Exchange.
3. No es posible crear copias de seguridad compatibles con la aplicación de equipos físicos y virtuales.
4. En macOS, solo se admite la copia de seguridad a nivel de archivo en una ubicación de cinta.
5. La consolidación de las copias de seguridad ubicadas en las cintas no es posible. Por ello, el esquema de copias de seguridad **Siempre incremental** no estará disponible cuando realice copias de seguridad en cintas.
6. La deduplicación de las copias de seguridad ubicadas en las cintas no es posible.
7. El software no puede sobrescribir automáticamente una cinta que contenga copias de seguridad no eliminadas o si hay copias de seguridad dependientes en otras cintas.
   La única excepción a esta regla es cuando la opción "Sobrescribir una cita en la unidad de cinta independiente al crear una copia de seguridad completa" está activada.
8. No puede realizar la recuperación en un sistema operativo desde una copia de seguridad almacenada en cintas si la recuperación necesita el reinicio del sistema operativo. Utilice un dispositivo de arranque para realizar dicha recuperación.
9. Puede validar cualquier copia de seguridad almacenada en cinta, pero no puede seleccionar la validación de toda una ubicación en cinta o todo un dispositivo de cintas.
10. Una ubicación basada en cintas gestionada no se puede proteger con el cifrado. En su lugar, cifre las copias de seguridad.
11. El software no puede escribir simultáneamente una copia de seguridad a múltiples cintas o múltiples copias de seguridad a través de la misma unidad a la misma cinta.
12. No se admiten los dispositivos que utilizan el protocolo de administración de datos en red (NDMP).
13. Las impresoras de códigos de barras no son compatibles.
14. No se admiten las cintas con formato de Sistema de archivos de cinta lineal (LTFS).

Legibilidad de cintas escritas por productos de Acronis anteriores

La siguiente tabla resume la legibilidad de las cintas escritas por Acronis True Image Echo, Acronis True Image 9.1, Acronis Backup & Recovery 10, Acronis Backup & Recovery 11, Acronis Backup 11.5, 11.7 y la familia de productos de Acronis Cyber Protect 12.5. La tabla también ilustra la compatibilidad de las cintas escritas de varios componentes de Acronis Cyber Protect.

Puede añadir copias de seguridad incrementales y diferenciales a copias de seguridad examinadas de nuevo y creadas por Acronis Backup 11.5 y Backup 12.5.

	...es legible en un dispositivo de cinta conectado en un equipo con...			
	Dispositivo de arranque de Acronis Cyber Protect	Acronis Cyber Protect Agent para Windows	Acronis Cyber Protect Agent para Linux	Nodo de almacenamiento de Acronis Cyber Protect

Cinta escrita en un dispositivo de cinta conectado a nivel local (unidad de cinta o biblioteca de cintas) por...	Dispositivo de arranque	9.1	+	+	+	+
		Echo	+	+	+	+
		ABR10	+	+	+	+
		ABR11/ Acronis Backup 11.5/11.7/12 .5	+	+	+	-
	Agente para Windows	9.1	+	+	+	+
		Echo	+	+	+	+
		ABR10	+	+	+	+
		ABR11/ Acronis Backup 11.5/11.7/12 .5	+	+	+	-
	Agente para Linux	9.1	+	+	+	+
		Echo	+	+	+	+
		ABR10	+	+	+	+
		ABR11/ Acronis Backup 11.5/11.7/12 .5	+	+	+	-
Cinta escrita en un dispositivo de cinta por...	Servidor de copia de seguridad	9.1	-	-	-	-
		Echo	-	-	-	-
	Nodo de almacenamiento	ABR10	+	+	+	+
		ABR11/ Acronis Backup 11.5/11.7/12 .5	+	+	+	+

Comenzar con el uso del dispositivo de cintas

Creación de la copia de seguridad de un equipo en un dispositivo de cinta conectado a nivel local

Requisitos previos

- El dispositivo de cintas se conecta al equipo según las instrucciones del fabricante.
- El agente de protección está instalado en el equipo.

Antes de realizar la copia de seguridad

1. Cargue las cintas en el dispositivo de cintas.
2. Inicie sesión en la consola web de Cyber Protect.
3. En **Configuración** > **Gestión de cintas**, amplíe el nodo del equipo y, a continuación, haga clic en **Dispositivos de cintas**.
4. Asegúrese de que aparezca el dispositivo de cintas conectado. Si no es así, haga clic en **Detectar dispositivos**.
5. Realice el inventario de las cintas:
   a. Haga clic en el nombre del dispositivo de cintas.
   b. Haga clic en **Inventario** para detectar las cintas cargadas. Mantenga activado **Inventario completo**. No habilite el grupo **Mover cintas no reconocidas e importadas al grupo Cintas libres**. Haga clic en **Iniciar ahora el inventario**.

      Resultado. Las cintas cargadas se habrán trasladado a los grupos pertinentes como se indica en la sección "Inventario".

      Nota
      El inventario completo de un dispositivo de cintas completo puede demorar mucho tiempo.

   c. Si las cintas cargadas se enviaron al grupo **Cintas no reconocidas** o **Cintas importadas** y desea utilizarlas para incluir en la copia de seguridad, traslade dichas cintas al grupo **Cintas libres** manualmente.

      Nota
      Las cintas enviadas al grupo **Cintas importadas** contienen las copias de seguridad escritas por el software de Acronis. Antes de trasladar las cintas al grupo **Cintas libres**, asegúrese de que no necesita las copias de seguridad.

Realización de la copia de seguridad

Cree un plan de protección como se indica en la sección "Copia de seguridad". Cuando especifique la ubicación de la copia de seguridad, seleccione **Grupo de cintas 'Acronis'**.

Resultados

- Para acceder a la ubicación donde se crearán las copias de seguridad, haga clic en **Almacenamiento de copias de seguridad** > **Grupos de cintas 'Acronis'**.
- Las cintas con copias de seguridad se trasladarán al grupo **Acronis**.

Copia de seguridad de un dispositivo de cintas conectado a un nodo de almacenamiento

Requisitos previos

- Se registrará un nodo de almacenamiento en el servidor de gestión.
- El dispositivo de cintas se adjunta al nodo de almacenamiento de conformidad con las instrucciones del fabricante.

Antes de realizar la copia de seguridad

1. Cargue las cintas en el dispositivo de cintas.
2. Inicie sesión en la consola web de Cyber Protect.
3. Haga clic en **Configuración** > **Gestión de cintas**, amplíe el nodo con el nombre del nodo de almacenamiento y, a continuación, haga clic en **Dispositivos de cintas**.
4. Asegúrese de que aparezca el dispositivo de cintas conectado. Si no es así, haga clic en **Detectar dispositivos**.
5. Realice el inventario de las cintas:
   a. Haga clic en el nombre del dispositivo de cintas.
   b. Haga clic en **Inventario** para detectar las cintas cargadas. Mantenga activado **Inventario completo**. No active **Mover cintas no reconocidas o grupos de cintas importados en el grupo 'Cintas libres'**. Haga clic en **Iniciar ahora el inventario**.
   Resultado. Las cintas cargadas se habrán trasladado a los grupos pertinentes como se indica en la sección "Inventario".

   Nota
   El inventario completo de un dispositivo de cintas completo puede demorar mucho tiempo.

   c. Si las cintas cargadas se enviaron al grupo **Cintas no reconocidas** o **Cintas importadas** y desea utilizarlas para incluir en la copia de seguridad, traslade dichas cintas al grupo **Cintas libres** manualmente.

   Nota
   Las cintas enviadas al grupo **Cintas importadas** contienen las copias de seguridad escritas por el software de Acronis. Antes de trasladar las cintas al grupo **Cintas libres**, asegúrese de que no necesita las copias de seguridad.

d. Decida si desea realizar la copia de seguridad en el grupo **Acronis** o crear un grupo nuevo.

   Detalles. Tener varios grupos le permite utilizar un conjunto de cintas independiente para cada equipo o cada departamento de la empresa. Al utilizar múltiples grupos, puede evitar que las copias de seguridad creadas con diferentes planes de protección se mezclen en una cinta.

e. Si el grupo seleccionado puede admitir cintas del grupo **Cintas libres** cuando proceda, omita este paso.

   Si no, traslade las cintas del grupo **Cintas libres** al grupo seleccionado.

   Consejo. Para saber si un grupo puede admitir cintas del grupo **Cintas libres**, haga clic en el grupo y, a continuación, en **Información**.

Realización de la copia de seguridad

Cree un plan de protección como se indica en la sección "Copia de seguridad". Al especificar la ubicación de la copia de seguridad, seleccione el grupo de cintas creado.

Resultados

- Para acceder a la ubicación donde se crearán las copias de seguridad, haga clic en **Copias de seguridad** y, a continuación, en el nombre del pool de cintas creado.
- Se moverán las cintas con las copias de seguridad al grupo seleccionado.

Consejos para otros usos de la biblioteca de cintas

- No debe realizar el inventario completo cada vez que carga una nueva cinta. Para ahorrar tiempo, siga el procedimiento descrito en la sección "Inventario" debajo de "Combinación del inventario rápido y completo".
- Puede crear otros grupos en la misma biblioteca de cintas y seleccionar cualquiera de ellas como el destino de las copias de seguridad.

Recuperación en un sistema operativo desde un dispositivo de cintas

Para recuperar en un sistema operativo desde un dispositivo de cintas:

1. Inicie sesión en la consola web de Cyber Protect.
2. Haga clic en **Dispositivos** y, a continuación, seleccione el equipo del que se ha realizado la copia de seguridad.
3. Haga clic en **Recuperación**.
4. Seleccione un punto de recuperación. Tenga en cuenta que los puntos de recuperación se filtran por ubicación.
5. El software le muestra la lista de cintas necesarias para la recuperación. Las cintas faltantes están en color gris. Si su dispositivo de cintas posee ranuras vacías, cargue estas cintas en el dispositivo.
6. Configure otros ajustes de recuperación.

7. Haga clic en **Iniciar recuperación** para comenzar la operación de recuperación.
8. Si por cualquier razón alguna de las cintas necesarias no se carga, el software mostrará un mensaje con el identificador de la cinta necesaria. Realice lo siguiente:
   a. Cargue la cinta.
   b. Realice el inventario rápido.
   c. Haga clic en **Generalidades** > **Actividades** y, a continuación, en la actividad de recuperación con el estado **Interacción obligatoria**.
   d. Haga clic en **Mostrar detalles** y, a continuación, en **Reintentar** para continuar con la recuperación.

¿Qué sucede si no veo las copias de seguridad almacenadas en las cintas?

Puede significar que la base de datos con el contenido de las cintas está dañada o falta por alguna razón.

Para restaurar la base de datos, realice lo siguiente:

1. Realice el inventario rápido.

   Advertencia.
   Durante el inventario, *no* active **Mover cintas no reconocidas e importadas al grupo Cintas libres**. Si el conmutador está activado, puede perder todas sus copias de seguridad.

2. Vuelva a escanear el pool **Cintas no reconocidas**. Como resultado, obtendrá el contenido de la cintas cargadas.
3. Si alguna de las copias de seguridad detectadas continúa en otras cintas que todavía no se han vuelto a escanear, cargue estas cintas cuando se le solicite y vuelva a escanearlas.

Recuperación en un dispositivo de arranque desde un dispositivo de cintas conectado localmente

Para recuperar en un dispositivo de arranque desde un dispositivo de cintas conectado localmente.

1. Cargue las cintas necesarias para la recuperación en el dispositivo de cintas.
2. Inicie el equipo desde el dispositivo de arranque.
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 el dispositivo de cintas está conectado mediante la interfaz iSCSI, configure el dispositivo según se describe en "Configuración de dispositivos iSCSI y NDAS".
5. Haga clic en **Gestión de cintas**.
6. Haga clic en **Inventario**.
7. En **Objetos que se deben incluir en el inventario**, seleccione el dispositivo de cintas.

8. Haga clic en **Comenzar** para iniciar el inventario.
9. Cuando haya terminado el inventario, haga clic en **Cerrar**.
10. Haga clic en **Acciones** > **Recuperar**.
11. Haga clic en **Seleccionar datos** y después haga clic en **Examinar**.
12. Expanda **Dispositivos de cintas** y, a continuación, seleccione el dispositivo necesario. El sistema le pedirá que confirme el nuevo escaneo. Haga clic en **Sí**.
13. Seleccione el pool **Cintas no reconocidas**.
14. Seleccione las cintas que se volverán a escanear. Para seleccionar todas las cintas del pool, seleccione la casilla de verificación al lado del encabezado de columna **Nombre de la cinta**.
15. Si las cintas contienen una copia de seguridad protegida con contraseña, active la casilla de verificación correspondiente y especifique la contraseña de la copia de seguridad en el cuadro **Contraseña**. Si no especifica una contraseña o si la contraseña es incorrecta, la copia de seguridad no se detectará. Tenga en cuenta que en este caso no ve las copias de seguridad después del nuevo escaneo.

    Consejo. Si las cintas contienen varias copias de seguridad protegidas por diversas contraseñas, vuelva a examinar varias veces especificando la contraseña apropiada cada vez.
16. Haga clic en **Comenzar** para iniciar el nuevo escaneo. Como resultado, obtendrá el contenido de la cintas cargadas.
17. Si alguna de las copias de seguridad detectadas continúa en otras cintas que todavía no se han vuelto a escanear, cargue estas cintas cuando se le solicite y vuelva a escanearlas.
18. Después de volver a examinar, haga clic en **Aceptar**.
19. En la **Vista Archivo comprimido**, seleccione la copia de seguridad cuyos datos se recuperarán y después seleccione los datos que desea recuperar. Después de hacer clic en **Aceptar**, la página **Recuperar datos** le mostrará la lista de cintas necesarias para la recuperación. Las cintas faltantes están en color gris. Si su dispositivo de cintas posee ranuras vacías, cargue estas cintas en el dispositivo.
20. Configure otros ajustes de recuperación.
21. Haga clic en **Aceptar** para comenzar la recuperación.
22. Si por cualquier razón alguna de las cintas necesarias no se carga, el software mostrará un mensaje con el identificador de la cinta necesaria. Realice lo siguiente:
    a. Cargue la cinta.
    b. Realice el inventario rápido.
    c. Haga clic en **Generalidades** > **Actividades** y, a continuación, en la actividad de recuperación con el estado **Interacción obligatoria**.
    d. Haga clic en **Mostrar detalles** y, a continuación, en **Reintentar** para continuar con la recuperación.

Recuperación en un dispositivo de arranque desde un dispositivo de cintas conectado a un nodo de almacenamiento

Para recuperar un dispositivo de arranque desde un dispositivo de cintas conectado a un nodo de almacenamiento:

1. Cargue las cintas necesarias para la recuperación en el dispositivo de cintas.
2. Inicie el equipo desde el dispositivo de arranque.
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. Haga clic en **Recuperar**.
5. Haga clic en **Seleccionar datos** y después haga clic en **Examinar**.
6. En la casilla **Ruta**, escriba `bsp://<storage node address>/<pool name>/`, en que `<storage node address>` es la dirección IP del nodo de almacenamiento que contiene la copia de seguridad necesaria y `<pool name>` es el nombre del pool de cintas. Haga clic en **Aceptar** y especifique las credenciales para el pool.
7. Seleccione la copia de seguridad y después seleccione los datos que desea recuperar. Después de hacer clic en **Aceptar**, la página **Recuperar datos** le mostrará la lista de cintas necesarias para la recuperación. Las cintas faltantes están en color gris. Si su dispositivo de cintas posee ranuras vacías, cargue estas cintas en el dispositivo.
8. Configure otros ajustes de recuperación.
9. Haga clic en **Aceptar** para comenzar la recuperación.
10. Si por cualquier razón alguna de las cintas necesarias no se carga, el software mostrará un mensaje con el identificador de la cinta necesaria. Realice lo siguiente:
    a. Cargue la cinta.
    b. Realice el inventario rápido.
    c. Haga clic en **Generalidades** > **Actividades** y, a continuación, en la actividad de recuperación con el estado **Interacción obligatoria**.
    d. Haga clic en **Mostrar detalles** y, a continuación, en **Reintentar** para continuar con la recuperación.

Gestión de cintas

Detección de dispositivos de cintas

Al detectar dispositivos de cintas, el software de copia de seguridad encuentra los dispositivos de cintas conectados al equipo y coloca la información acerca de estos en la base de datos de gestión de cintas. Los dispositivos de cintas detectados están desactivados de RSM.

Por lo general, un dispositivo de cintas se detecta de forma automática en cuanto se conecta a un equipo con el producto instalado. No obstante, es posible que tenga que detectar dispositivos de cintas en los casos siguientes:

- Después de conectar o reconectar un dispositivo de cintas.
- Después de haber instalado o reinstalado el software de copia de seguridad en el equipo en donde está conectado el dispositivo de cintas.

Para detectar los dispositivos de cintas

1. Haga clic en **Configuración** > **Gestión de cintas**.
2. Seleccione el equipo al que se conectará el dispositivo de cintas.
3. Haga clic en **Detectar dispositivo de cintas**. Verá los dispositivos de cintas conectados, sus unidades y sus ranuras.

Grupos de cintas

El software de copia de seguridad utiliza pools de cintas, es decir, grupos lógicos de cintas. El software contiene los siguientes grupos de cintas predefinidos: **Cintas no reconocidas**, **Cintas importadas**, **Cintas disponibles** y **Acronis**. Además, puede crear sus propios grupos personalizados.

El pool **Acronis** y los pools personalizados se utilizan también como ubicaciones de copia de seguridad.

Grupos predefinidos

Cintas no reconocidas

El grupo contiene las cintas que se escribieron con aplicaciones de terceros. Para escribir en dichas cintas, necesita moverlas al grupo **Cintas disponibles** explícitamente. No puede mover las cintas de este grupo a otro grupo, excepto para el grupo **Cintas disponibles**.

Cintas importadas

El grupo contiene cintas que fueron escritas por Acronis Cyber Protect en un dispositivo de cintas conectado a otro nodo de almacenamiento o agente. Para escribir en dichas cintas, necesita moverlas al grupo **Cintas disponibles** explícitamente. No puede mover las cintas de este grupo a otro grupo, excepto para el grupo **Cintas disponibles**.

Cintas libres

El grupo contiene las cintas libres (vacías). Puede mover manualmente las cintas de este grupo o otros grupos.

Cuando mueve una cinta al pool **Cintas disponibles**, el software la marca como vacía. Si la cinta contiene copias de seguridad, se marcan con el icono  . Cuando el software comienza a sobrescribir la cinta, eliminará los datos relacionados con las copias de seguridad de la base de datos.

Acronis

El grupo se utiliza para la copia de seguridad de manera predeterminada, cuando no desea crear sus propios grupos. Generalmente se aplica a una unidad de cintas con un pequeño número de cintas.

Grupos personalizados

Necesita crear varios grupos si desea separar las copias de seguridad de diferentes datos. Por ejemplo, es posible que desee crear grupos personalizados para separar:

- copias de seguridad de diferentes departamentos de su empresa
- copias de seguridad de diferentes equipos
- copias de seguridad de volúmenes del sistema y datos del usuario.

Operaciones con grupos

Creación de un grupo

Para crear un grupo:

1. Haga clic en **Configuración** > **Gestión de cintas**.
2. Seleccione el equipo o el nodo de almacenamiento al cual su dispositivo de cintas está conectado y después haga clic en **Pools de cintas** en este equipo.
3. Haga clic en **Crear grupo**.
4. Especifique el nombre del grupo.
5. [Opcional] Anule la marca de la casilla de verificación **Sacar cintas del grupo 'Cintas libres' automáticamente...**. Si se desmarca, solo las cintas que se incluyen en el nuevo grupo en un momento determinado se utilizarán para la copia de seguridad.
6. Haga clic en **Crear**.

Edición de un grupo

Puede modificar los parámetros del grupo **Acronis** o su propio grupo personalizado.

Para editar un grupo:

1. Haga clic en **Configuración** > **Gestión de cintas**.
2. Seleccione el equipo o el nodo de almacenamiento al cual su dispositivo de cintas está conectado y después haga clic en **Pools de cintas** en este equipo.
3. Seleccione el grupo pertinente y, a continuación, haga clic en **Editar grupo**.
4. Puede cambiar el nombre o la configuración del grupo. Para obtener más información acerca de la configuración de los grupos, consulte la sección "Creación de un grupo".
5. Haga clic en **Guardar** para guardar los cambios.

Eliminación de un grupo

Puede eliminar solo grupos personalizados. No es posible eliminar los grupos de cintas predefinidos (**Cintas no reconocidas**, **Cintas importadas**, **Cintas libres** y **Acronis**).

Nota
Una vez eliminado un grupo, no se olvide de modificar los planes de protección que tengan al grupo como ubicación de la copia de seguridad. De lo contrario, estos planes de protección no podrán llevarse a cabo.

Para eliminar un grupo:

1. Haga clic en **Configuración** > **Gestión de cintas**.
2. Seleccione el equipo o el nodo de almacenamiento al cual su dispositivo de cintas está conectado y después haga clic en **Pools de cintas** en este equipo.
3. Seleccione el grupo necesario y haga clic en **Eliminar**.
4. Seleccione el grupo al cual se moverán las cintas del grupo que se está eliminando después de la eliminación.
5. Haga clic en **Aceptar** para eliminar el grupo.

Operaciones con cintas

Mover a otra ranura

Utilice esta operación en las siguientes situaciones:

- Debe retirar varias cintas del dispositivo de cintas simultáneamente.
- Su dispositivo de cintas no posee una ranura de correo y las cintas que se retirar están ubicadas en ranuras de cargadores no extraíbles.

Necesita mover las cintas de un cargador de ranuras y después retirar manualmente el cargador.

Pasos para mover una cinta a otra ranura

1. Haga clic en **Configuración** > **Gestión de cintas**.
2. Seleccione el equipo o el nodo de almacenamiento al cual su dispositivo de cintas está conectado y después haga clic en **Pools de cintas** en este equipo.
3. Haga clic en el grupo que contiene la cinta necesaria y después seleccione la cinta necesaria.
4. Haga clic en **Mover a ranura de la unidad**.
5. Seleccione una nueva ranura a la que mover la cinta seleccionada.
6. Haga clic en **Mover** para iniciar la operación.

Mover a otro pool

La operación le permite mover una o más cintas de un grupo a otro.

Cuando mueve una cinta al pool **Cintas disponibles**, el software la marca como vacía. Si la cinta contiene copias de seguridad, se marcan con el icono  . Cuando el software comienza a sobrescribir la cinta, eliminará los datos relacionados con las copias de seguridad de la base de datos.

Notas sobre los tipos específicos de cintas

- No puede mover cintas protegidas contra escritura o grabadas como WORM (una sola escritura múltiples lecturas) al pool **Cintas libres**.
- Las cintas de limpieza siempre se muestran en el grupo **Cintas no reconocidas**; no puede moverlas a otro grupo.

Pasos para mover las cintas a otro grupo

1. Haga clic en **Configuración** > **Gestión de cintas**.
2. Seleccione el equipo o el nodo de almacenamiento al cual su dispositivo de cintas está conectado y después haga clic en **Pools de cintas** en este equipo.
3. Haga clic en el grupo que contiene las cintas necesarias y después seleccione las cintas necesarias.
4. Haga clic en **Mover a pool**.
5. [Opcional] Haga clic en **Crear nuevo pool** si desea crear otro pool para las cintas seleccionadas. Realice las acciones descritas en la sección "Creación de un pool".
6. Seleccione el grupo al que desea mover las cintas.
7. Haga clic en **Mover** para guardar los cambios.

Nota
Si tiene copias de seguridad restaurables en la cinta y mueve la cinta a otro pool, asegúrese de actualizar el almacén en Almacenamiento para copias de seguridad después de moverla. Las copias de seguridad estarán disponibles en el segundo pool independientemente del destino de la copia de seguridad original.

Inventario

La operación de inventario detecta las cintas cargadas en el dispositivo de cintas y les asigna nombres a las que no tienen ninguno.

Métodos de inventario

Hay dos formas de realizar el inventario.

Inventario rápido

El agente o el nodo de almacenamiento busca códigos de barras. Con los códigos de barras, el software puede volver una cinta al grupo en la que se encontraba antes.

Seleccione este método para reconocer las cintas utilizadas por el mismo dispositivo de cintas conectado al mismo equipo. Se enviarán otras cintas al grupo **Cintas no reconocidas**.

Si su biblioteca de cintas no contiene ningún lector de códigos de barras, las cintas se enviarán al grupo **Cintas no reconocidas**. Para reconocer sus cintas, realice el inventario completo o combine los inventarios completo y rápido según se describe a continuación en esta sección.

Inventario completo

El agente o el nodo de almacenamiento lee las etiquetas escritas anteriormente y analiza otra información acerca del contenido de las cintas cargadas. Seleccione este método para reconocer las cintas vacías y las cintas escritas por el mismo software en cualquier dispositivo de cintas y equipo.

La siguiente tabla muestra los grupos a los que se envían las cintas como resultado del inventario completo.

La cinta fue usada por...	La cinta está lista por...	La cinta se envía al grupo...
Agente	El mismo agente	En donde estaba la cinta
	Otro agente	**Cintas importadas**
	Nodo de almacenamiento	**Cintas importadas**
Nodo de almacenamiento	El mismo nodo de almacenamiento	En donde estaba la cinta
	Otro nodo de almacenamiento	**Cintas importadas**
	Agente	**Cintas importadas**
Aplicación de copia de seguridad de terceros	Agente o nodo de almacenamiento	**Cintas no reconocidas**

Las cintas de ciertos tipos se envían a grupos específicos:

tipo de cinta	La cinta se envía al grupo...
Cinta vacía	**Cintas libres**
Cinta vacía protegida contra escritura	**Cintas no reconocidas**
Limpieza de cintas	**Cintas no reconocidas**

El inventario rápido se puede aplicar a dispositivos de cintas completos. El inventario completo puede aplicarse a bibliotecas de cintas completas, unidades o ranuras individuales. Para unidades de cinta independientes, siempre se lleva a cabo un inventario completo, incluso si se ha seleccionado un inventario rápido.

Combinación del inventario rápido y completo

El inventario completo de un dispositivo de cintas completo puede demorar mucho tiempo. Si necesita realizar el inventario de solo algunas cintas, realice lo siguiente:

1. Realice el inventario rápido del dispositivo de cintas.
2. Haga clic en el grupo **Cintas no reconocidas**. Encuentre las cintas de las que desea realizar el inventario y anote las ranuras que ocupan.
3. Realice el inventario completo de estas ranuras.

Qué hacer después del inventario

Si desea realizar la copia de seguridad de las cintas que se colocaron en el grupo **Cintas no reconocidas** o **Cintas importadas**, trasládelas al grupo **Cintas libres** y, a continuación, al grupo **Acronis** o a un grupo personalizado. Si el grupo del que desea realizar la copia de seguridad es rellenable, puede dejar las cintas en el grupo **Cintas libres**.

Si desea recuperar desde una cinta que se colocó en el grupo **Cintas no reconocidas** o **Cintas importadas**, tiene que volver a escanearla. La cinta se trasladará al grupo seleccionado durante el nuevo escaneo y las copias de seguridad almacenadas en la cinta aparecerán en la ubicación.

Secuencia de las acciones

1. Haga clic en **Configuración** > **Gestión de cintas**.
2. Seleccione el equipo al que se conectará el dispositivo de cintas, y luego seleccione el dispositivo de cintas que desea inventariar.
3. Haga clic en **Inventario**.
4. [Opcional] Para seleccionar el inventario rápido, desactive el **Inventario completo**.
5. [Opcional] Active **Mover cintas no reconocidas e importadas al grupo Cintas libres**.

   Advertencia.
   Active únicamente este conmutador si está totalmente seguro de que los datos almacenados en las cintas se pueden sobrescribir.

6. Haga clic en **Iniciar ahora el inventario** para comenzar el inventario.

Nuevo escaneo

La información acerca del contenido de las cintas se almacena en una base de datos dedicada. La operación de volver a escanear lee el contenido de las cintas y actualiza la base de datos si la información en la misma no coincide con los datos almacenados en las cintas. Las copias de seguridad detectadas como resultado de la operación se colocan en el pool especificado.

Con esta operación, puede volver a escanear las cintas de un grupo. Para la operación pueden seleccionarse solo las cintas en línea.

Para volver a escanear las cintas con una copia de seguridad con múltiples transmisiones o con múltiples transmisiones y con multiplex, como mínimo deberá disponer de la misma cantidad de unidades utilizadas para crear la copia de seguridad. Esta copia de seguridad no se puede volver a escanear mediante una unidad de cinta independiente.

Ejecución del nuevo escaneo:

- Si la base de datos de un nodo de almacenamiento o equipo gestionado está dañado o no se encuentra.
- Si la información acerca de la cinta en la base de datos está desactualizada (por ejemplo, un nodo de almacenamiento o agente modificó el contenido de la cinta).
- Para obtener acceso a las copias de seguridad almacenadas en las cintas al trabajar con un dispositivo de arranque.
- Si por error quitó la información acerca de la cinta de la base de datos. Al realizar un nuevo escaneo de una cinta quitada, las copias de seguridad almacenadas en la misma vuelven a aparecer en la base de datos y están disponibles para la recuperación de los datos.
- Si las copias de seguridad se eliminaron de una cinta ya sea manualmente o mediante reglas de retención, pero desea que estén accesibles para la recuperación de los datos. Antes de volver a escanear dicha cinta, expúlsela, retire la información sobre la misma de la base de datos y después inserte la cinta nuevamente en el dispositivo de cintas.

Pasos para volver a escanear las cintas

1. Haga clic en **Configuración** > **Gestión de cintas**.
2. Seleccione el equipo o el nodo de almacenamiento al cual su dispositivo de cintas está conectado y después haga clic en **Dispositivos de cintas** en este equipo.
3. Seleccione el dispositivo de cintas en el que se cargaron las cintas.
4. Realice el inventario rápido.

   Nota
   Durante el inventario, *no* active el conmutador **Mover cintas no reconocidas e importadas al pool Cintas disponibles**.

5. Seleccione el pool **Cintas no reconocidas**. Este es el grupo al cual se envía la mayoría de las cintas como resultado del inventario rápido. También puede volver a examinar cualquier otro pool.
6. [Opcional] Para volver a examinar solo cintas individuales, selecciónelas.
7. Haga clic en **Volver a escanear**.
8. Seleccione el pool en donde se colocarán las copias de seguridad recién detectadas.
9. Si fuera necesario, seleccione la casilla de verificación **Habilitar la recuperación de archivos de las copias de seguridad del disco almacenadas en cintas**.

   Detalles. Si esta casilla de verificación está seleccionada, el software creará archivos complementarios en el disco duro del equipo donde está conectado el dispositivo de cintas. La recuperación desde las copias de seguridad de discos es posible siempre y cuando estos archivos complementarios estén intactos. Asegúrese de seleccionar la casilla de verificación si las cintas contienen copias de seguridad compatibles con la aplicación. De lo contrario, no podrá recuperar los datos de programa de estas copias de seguridad.
10. Si las cintas contienen una copia de seguridad protegida con contraseña, seleccione la casilla de verificación correspondiente y después especifique la contraseña para las copias de seguridad.

Si no especifica una contraseña, o la contraseña es incorrecta, no se detectarán las copias de seguridad. Tenga en cuenta que en este caso no ve las copias de seguridad después del nuevo escaneo.

Consejo. Si las cintas contienen copias de seguridad protegidas por varias contraseñas, debe repetir el nuevo escaneado varias veces especificando cada contraseña cada vez.

11. Haga clic en **Comenzar nuevo escaneo** para iniciar el nuevo escaneo.

Resultado. Las cintas seleccionadas se mueven al pool seleccionado. Las copias de seguridad almacenadas en las cintas pueden encontrarse en este pool. Una copia de seguridad esparcida por varias cintas no aparecerá en el pool hasta que todas las cintas se hayan vuelto a escanear.

Cambio de nombre

Cuando el software detecta una nueva cinta, se le asigna automáticamente un nombre en el siguiente formato: **Cinta XXX**, donde **XXX** es un número único. Las cintas están numeradas en orden. La operación de cambio de nombre le permite cambiar manualmente el nombre de una cinta.

Pasos para cambiar el nombre de las cintas

1. Haga clic en **Configuración** > **Gestión de cintas**.
2. Seleccione el equipo o el nodo de almacenamiento al cual su dispositivo de cintas está conectado y después haga clic en **Pools de cintas** en este equipo.
3. Haga clic en el grupo que contiene la cinta necesaria y después seleccione la cinta necesaria.
4. Haga clic en **Cambiar nombre**.
5. Escriba el nuevo nombre de la cinta seleccionada.
6. Haga clic en **Cambiar nombre** para guardar los cambios.

Borrado

Borrar una cinta elimina físicamente todos las copias de seguridad almacenadas en la cinta y elimina la información acerca de estas copias de seguridad de la base de datos. Sin embargo, la información acerca de la cinta misma permanece en la base de datos.

Después del borrado, una cinta ubicada en el grupo **Cintas no reconocidas** o **Cintas importadas** se trasladará al grupo **Cintas libres**. Una cinta ubicada en cualquier otro grupo no se mueve.

Pasos para borrar las cintas

1. Haga clic en **Configuración** > **Gestión de cintas**.
2. Seleccione el equipo o el nodo de almacenamiento al cual su dispositivo de cintas está conectado y después haga clic en **Pools de cintas** en este equipo.
3. Haga clic en el grupo que contiene las cintas necesarias y después seleccione las cintas necesarias.
4. Haga clic en **Borrar**. El sistema le pedirá que confirme la operación.

5. Seleccione el método de borrado: rápido o completo.
6. Haga clic en **Borrar** para iniciar la operación.
   Detalles. No puede cancelar la operación de borrado.

Expulsión

Para una expulsión correcta de una cinta de una biblioteca de cintas, la biblioteca de cintas debe tener la ranura de correo y la ranura no debe estar bloqueada por otro usuario o software.

Pasos para expulsar las cintas

1. Haga clic en **Configuración** > **Gestión de cintas**.
2. Seleccione el equipo o el nodo de almacenamiento al cual su dispositivo de cintas está conectado y después haga clic en **Pools de cintas** en este equipo.
3. Haga clic en el grupo que contiene las cintas necesarias y después seleccione las cintas necesarias.
4. Haga clic en **Expulsar**. El software le pedirá que proporcione la descripción de la cinta. Le recomendamos que describa la ubicación física donde se guardarán las cintas. Durante la recuperación, el software le mostrará la descripción para que pueda encontrar fácilmente las cintas.
5. Haga clic en **Expulsar** para iniciar la operación.

Después de expulsar una cinta de forma manual o automática, es recomendable escribir su nombre en la cinta.

Eliminación

La operación de eliminación borra la información sobre las copias de seguridad almacenada en la cinta seleccionada y acerca de la cinta misma de la base de datos.

Solo puede quitar una cinta fuera de línea (expulsada).

Pasos para quitar una cinta

1. Haga clic en **Configuración** > **Gestión de cintas**.
2. Seleccione el equipo o el nodo de almacenamiento al cual su dispositivo de cintas está conectado y después haga clic en **Pools de cintas** en este equipo.
3. Haga clic en el grupo que contiene la cinta necesaria y después seleccione la cinta necesaria.
4. Haga clic en **Quitar**. El sistema le pedirá que confirme la operación.
5. Haga clic en **Quitar** para quitar la cinta.

¿Qué sucede si quito una cinta por error?

A diferencia de una cinta borrada, los datos de una cinta eliminada no se borran físicamente. Por lo tanto, puede realizar copias de seguridad almacenadas en dicha cinta nuevamente. Para hacerlo:

1. Cargue la cinta en su dispositivo de cintas.
2. Realice un inventario rápido para detectar la cinta.

   Nota
   Durante el inventario, *no* active el conmutador **Mover cintas no reconocidas e importadas al pool Cintas disponibles**.

3. Realice el nuevo escaneo para hacer coincidir los datos almacenados en la cinta con la base de datos.

Especificación de un juego de cintas

La operación le permite especificar un juego de cintas para cintas.

Un **juego de cintas** es un grupo de cintas dentro de un pool.

A diferencia de especificar juegos de cintas en las opciones de copia de seguridad, donde se pueden usar variables, en este caso solo se puede especificar un valor de cadena.

Realice esta operación si desea que el software realice una copia de seguridad de cintas *concretas* siguiendo una regla determinada (por ejemplo, si desea guardar las copias de seguridad del lunes en la Cinta 1, las del martes en la Cinta 2, etc). Especifique un cierto juego de cintas para cada una de las cintas necesarias y, a continuación, especifique el mismo juego de cintas o utilice variables apropiadas en las opciones de copia de seguridad.

Para el ejemplo anterior, especifique el juego de cintas `Monday` para Cinta 1, `Tuesday` para Cinta 2, etc. En las opciones de copia de seguridad, especifique `[Weekday]`. En este caso, se usará una cinta apropiada en el día respectivo de la semana.

Pasos para especificar un juego de cintas para una o varias cintas

1. Haga clic en **Configuración** > **Gestión de cintas**.
2. Seleccione el equipo o el nodo de almacenamiento al cual su dispositivo de cintas está conectado y después haga clic en **Pools de cintas** en este equipo.
3. Haga clic en el grupo que contiene las cintas necesarias y después seleccione las cintas necesarias.
4. Haga clic en **Juego de cintas**.
5. Escriba el nombre del juego de cintas. Si ya se ha especificado otro juego de cintas para las cintas seleccionadas, el nombre se sustituirá. Si desea excluir las cintas del juego de cintas sin especificar otro, elimine el nombre de juego de cintas existente.
6. Haga clic en **Guardar** para guardar los cambios.

Nodos de almacenamiento

Un nodo de almacenamiento es un servidor diseñado para optimizar el uso de diversos recursos (como, por ejemplo, la capacidad de almacenamiento corporativo, el ancho de banda de red o la

carga de la CPU de los servidores de producción) necesarios para proteger los datos de la empresa. Este objetivo se consigue gracias a la organización y la gestión de ubicaciones que funcionan como ubicaciones de almacenamiento dedicadas de las copias de seguridad de la empresa (ubicaciones gestionadas).

El propósito principal del nodo de almacenamiento de Acronis es habilitar un acceso centralizado a unidades de cinta o bibliotecas, por ejemplo, a datos de copia de seguridad y restauración de múltiples dispositivos en una misma unidad de cinta o biblioteca (almacén gestionado en cinta).

Otro caso de uso la habilitación de capacidades avanzadas de deduplicación, por ejemplo, si datos de varios dispositivos deben deduplicarse juntos y almacenarse en una misma ubicación (almacén gestionado con deduplicación habilitada).

Instalación de un nodo de almacenamiento y un servicio de catálogo

Antes de instalar un nodo de almacenamiento, asegúrese de que el equipo cumpla los requisitos del sistema.

Se recomienda instalar un nodo de almacenamiento y un servicio de catalogación en equipos independientes. Los requisitos del sistema para un equipo que ejecute un servicio de catalogación se describen en "Catalogación de las prácticas recomendadas" (p. 696).

Para instalar un nodo de almacenamiento o un servicio de catalogación

1. Inicie sesión como administrador e inicie el programa de instalación de Acronis Cyber Protect.
2. [Opcional] Para cambiar el idioma del programa de instalación, haga clic en **Idioma de instalación**.
3. Acepte los términos del acuerdo de licencia y la declaración de privacidad y, a continuación, haga clic en **Siguiente**.
4. Haga clic en **Instalar un agente de protección**.
5. Haga clic en **Personalizar configuración de la instalación**.
6. Junto a **Qué instalar**, haga clic en **Cambiar**.
7. Seleccione los componentes que desee instalar:
   - Para instalar un nodo de almacenamiento, marque la casilla de verificación **Nodo de almacenamiento**. La casilla de verificación **Agente para Windows** se marca automáticamente.
   - Para instalar un servicio de catálogo, marque la casilla de verificación **Servicio de catálogo**.
   - Si no desea instalar otros componentes en este equipo, desmarque las casillas de verificación que corresponda.

   Haga clic en **Realizado** para continuar.
8. Especifique el servidor de gestión en el que se registrarán los componentes:
   a. Junto a **Acronis Cyber Protect Management Server**, haga clic en **Especificar**.

b. Especifique el nombre del servidor o la dirección IP del equipo donde está instalado el servidor de gestión.
c. Especifique las credenciales de un administrador del servidor de gestión o un token de registro.
   Para obtener más información sobre cómo generar un token de registro, consulte "Paso 1: Generar un token de registro" (p. 221).
d. Haga clic en **Realizado**.

9. Si se le pregunta, seleccione si desea que el equipo con el nodo de almacenamiento o el servicio de catalogación se añada a la organización o a una de sus unidades.
   Este mensaje aparece si ha administrado más de una unidad o una organización con al menos una unidad. De lo contrario, el equipo se añadirá silenciosamente a la unidad que administra o a la organización. Para obtener más información, consulte la sección "Administradores y unidades".
10. [Opcional] Cambie otros ajustes de la instalación según se describe en "Personalización de los ajustes de instalación".
11. Haga clic en **Instalar** para proceder con la instalación.
12. Cuando haya terminado la instalación, haga clic en **Cerrar**.

Actualizar el servicio de catálogo con la actualización 4 de Acronis Cyber Protect 15

La actualización 4 deAcronis Cyber Protect 15 utiliza una nueva versión del servicio de catálogo. La nueva versión no es directamente compatible con los datos del catálogo que se crearon con versiones anteriores.

Durante la actualización 4 de Acronis Cyber Protect 15, puede migrar los datos de forma manual a la nueva versión del servicio de catálogo. O bien, puede omitir la migración y volver a crear los datos del catálogo más tarde. Se tarda más tiempo en volver a crear los datos del catálogo que en la migración.

Pasos para migrar los datos del catálogo

1. Ejecute el programa de instalación de Acronis Cyber Protect en el equipo donde esté instalado el catálogo de servicio.
2. Acepte los términos del acuerdo de licencia y la declaración de privacidad y, a continuación, haga clic en **Siguiente**.
3. Seleccione la casilla de verificación **Lo entiendo** y haga clic en **Actualizar**.
4. Seleccione la casilla de verificación **Especifique una carpeta temporal**.
5. Especifique la carpeta a la que se exportarán los datos del catálogo.
   Los datos exportados están cifrados. Cuando se complete la migración, la carpeta temporal se eliminará de forma automática.
6. Haga clic en **Realizado**.

Pasos para omitir la migración de los datos del catálogo

1. Ejecute el programa de instalación de Acronis Cyber Protect en el equipo donde esté instalado el catálogo de servicio.
2. Acepte los términos del acuerdo de licencia y la declaración de privacidad y, a continuación, haga clic en **Siguiente**.
3. Seleccione la casilla de verificación **Lo entiendo** y haga clic en **Actualizar**.
4. Borre la casilla de verificación **Especifique una carpeta temporal**.
5. Haga clic en **Realizado**.
6. Confirme su elección.

Como resultado, los datos del catálogo existentes dejarán de estar disponibles después de cambiar a la actualización 4 de Acronis Cyber Protect 15. Para volver a crear los datos del catálogo, ejecute una copia de seguridad.

Nota
Si el servicio de catálogo, el nodo de almacenamiento y el servidor de gestión se ejecutan en equipos individuales, asegúrese de que todos están actualizados a la actualización 4 de Acronis Cyber Protect 15 en este orden:

1. Servidor de gestión
2. Nodo de almacenamiento
3. Servicio de catálogo

Incorporación de la ubicación gestionada

Una ubicación gestionada puede organizarse:

- En una carpeta local:
  - En una unidad del disco duro local al nodo de almacenamiento
  - En un almacenamiento SAN que aparezca en el sistema operativo como un dispositivo conectado localmente
- En una carpeta de red:
  - En un recurso compartido SMB/CIFS
  - En un almacenamiento SAN que aparezca en el sistema operativo como carpeta de red
  - En un NAS
- En un dispositivo de cintas conectado localmente al nodo de almacenamiento
  Las ubicaciones basadas en cintas se crean en forma de pool de cintas. Hay un pool de cintas presente de forma predeterminada. Si es necesario, puede crear otros pools de cintas, como se describe más adelante en esta sección.

Para crear una ubicación gestionada en una carpeta local o de red

1. Realice uno de los siguientes procedimientos:
   - Haga clic en **Almacenamiento de copias de seguridad** > **Agregar ubicación** y haga clic en **Nodo de almacenamiento**.
   - Cuando cree un plan de protección, haga clic en **Dónde guardar las copias de seguridad** > **Agregar ubicación** y haga clic en **Nodo de almacenamiento**.
   - Haga clic en **Configuración** > **Nodos de almacenamiento**, seleccione el nodo de almacenamiento que gestionará la ubicación y haga clic en **Agregar ubicación**.
2. En **Nombre**, escriba un nombre único para la ubicación. "Único" significa que no puede haber otra ubicación con el mismo nombre gestionada por el mismo nodo de almacenamiento.
3. [Opcional] Seleccione el nodo de almacenamiento que gestionará la ubicación. Si ha seleccionado la última opción en el paso 1, no podrá cambiar el nodo de almacenamiento.
4. Seleccione el nombre o la dirección IP del nodo de almacenamiento que los agentes utilizarán para acceder a la ubicación.

   De forma predeterminada, se elige el nombre del nodo de almacenamiento. Es posible que tenga que cambiar este ajuste si el servidor DNS no puede resolver el nombre a la dirección IP, lo que ocasiona un error de acceso. Para cambiar este ajuste posteriormente, haga clic en **Almacenamiento de copias de seguridad** > la ubicación > **Editar** y cambie el valor del campo **Dirección**.
5. Introduzca la ruta de la carpeta o navegue hasta la carpeta deseada.
6. Haga clic en **Realizado**. El software comprueba el acceso a la carpeta especificada.
7. [Opcional] Habilite la deduplicación de copias de seguridad en la ubicación.

   La deduplicación minimiza la transferencia de datos de la copia de seguridad y reduce el tamaño de las copias de seguridad almacenadas en la ubicación eliminando bloques de disco duplicados.

   Para obtener más información sobre las restricciones de la deduplicación, consulte "Restricciones de deduplicación".
8. [Solo si se ha habilitado la deduplicación] Especifique o cambie el valor del campo **Ruta de la base de datos de deduplicación**.

   Debe ser una carpeta en un disco duro local al nodo de almacenamiento. Para mejorar el rendimiento del sistema, le recomendamos crear la base de datos de deduplicación y la ubicación gestionada en discos diferentes.

   Para obtener más información sobre la base de datos de deduplicación, consulte "Mejores prácticas de deduplicación".
9. [Opcional] Seleccione si desea proteger la ubicación con cifrado. Todo lo que se guarda en la ubicación se cifra, y todo lo que se lee desde ella es descifrado de modo claro por el nodo de almacenamiento mediante una clave de encriptación específica de la ubicación almacenada en el nodo de almacenamiento.

   Para obtener más información sobre el cifrado, consulte la sección "Cifrado de la ubicación".
10. [Opcional] Seleccione si quiere catalogar las copias de seguridad almacenadas en la ubicación. El catálogo de datos permite encontrar fácilmente la versión necesaria de los datos y seleccionarla para la recuperación.

Si hay registrados varios servicios de catalogación en el servidor de gestión, puede seleccionar el servicio que catalogará las copias de seguridad almacenadas en la ubicación.

La catalogación se puede habilitar o deshabilitar más adelante, como se describe en "Cómo habilitar o deshabilitar la catalogación".

11. Haga clic en **Realizado** para crear la ubicación.

Para crear una ubicación gestionada en un dispositivo de cintas:

1. Haga clic en **Almacenamiento de copias de seguridad** > **Agregar ubicación** o, al crear un plan de protección, haga clic en **Dónde guardar las copias de seguridad** > **Agregar ubicación**.
2. Haga clic en **Cintas**.
3. [Opcional] Seleccione el nodo de almacenamiento que gestionará la ubicación.
4. Siga los pasos descritos en "Creación de un grupo", a partir del paso 4.

Nota
De forma predeterminada, los agentes usan el nombre del nodo de almacenamiento para acceder a una ubicación de cinta. Para que los agentes usen la dirección IP del nodo de almacenamiento, haga clic en **Almacenamiento de copias de seguridad** > la ubicación > **Editar** y cambie el valor del campo **Dirección**.

Deduplicación

Restricciones de deduplicación

Restricciones comunes

Las copias de seguridad cifradas no se pueden deduplicar. Si quiere usar tanto el proceso de deduplicación y como el de cifrado a la vez, deje las copias de seguridad sin cifrar y póngalas en una ubicación en la que estén habilitadas ambas opciones.

Copia de seguridad a nivel de discos

La deduplicación de los bloques del disco no se realiza si el tamaño de la unidad de asignación del volumen, conocido también como tamaño del clúster o tamaño de bloque, no es divisible por 4 KB.

Nota
El tamaño de la unidad de asignación en la mayoría de los volúmenes NTFS y ext3 es de 4 KB. Esto permite una deduplicación a nivel de bloques. Otros ejemplos de tamaños de unidades de asignación que permiten la deduplicación a nivel de bloque serían 8 KB, 16 KB y 64 KB.

Copia de seguridad a nivel de archivos

La deduplicación de un archivo no se realiza si el archivo se encuentra cifrado.

La deduplicación y los flujos de datos de NTFS

En un sistema de archivos NTFS, un archivo puede poseer uno o más conjuntos de datos adicionales asociados llamados normalmente *flujos de datos alternativos*.

Cuando se realiza una copia de seguridad de esos archivos, se hace lo mismo con sus flujos de datos alternativos. Sin embargo, estos flujos nunca se deduplican, incluso aunque se deduplique el propio archivo.

Mejores prácticas de deduplicación

La deduplicación es un proceso complejo que depende de muchos factores.

Los factores más importantes que tienen influencia sobre la velocidad de la deduplicación son:

- La velocidad de acceso a la base de datos de deduplicación
- La capacidad de RAM del nodo de almacenamiento
- El número de ubicaciones de deduplicación creado en el nodo de almacenamiento.

Para incrementar el rendimiento de la deduplicación, siga las recomendaciones a continuación.

Coloque la base de datos de deduplicación y la ubicación de deduplicación en equipos físicos independientes

La base de datos de deduplicación incluye los valores hash de todos los elementos almacenados en la ubicación, excepto aquellos que no pueden deduplicarse, como los archivos cifrados.

Para aumentar la velocidad de acceso a una base de datos de deduplicación, la base de datos y la ubicación deben estar colocadas en dispositivos físicos independientes.

Es mejor asignar dispositivos exclusivos para la ubicación y la base de datos. Si esto no es posible, al menos no coloque una ubicación o una base de datos en el mismo disco con el sistema operativo. El motivo es que el sistema operativo realiza una gran cantidad de operaciones de lectura/escritura en el disco duro, lo que ralentiza en gran medida la deduplicación.

Selección de un disco para una base de datos de deduplicación

- La base de datos deberá residir en una unidad fija. No intente colocar la base de datos de deduplicación en unidades extraíbles externas.
- Para minimizar el tiempo de acceso a la base de datos, almacénela en una unidad que esté conectada directamente en lugar de en un volumen de red montado. La latencia de la red puede reducir de forma considerable el rendimiento de la deduplicación.
- El espacio de disco necesario para una base de datos de deduplicación puede estimarse utilizando la siguiente fórmula:

$$S = U * 90 / 65536 + 10$$

Aquí,

S es el tamaño del disco en GB

U es la cantidad planificada de datos únicos en el almacén de datos de deduplicación en GB

Por ejemplo, si la cantidad planificada de datos únicos en el almacén de datos de deduplicación es U=5 TB, la base de datos de deduplicación necesitará, como mínimo, el espacio libre que se indica a continuación:

S = 5000 * 90 / 65536 + 10 = 17 GB

Selección de un disco para una ubicación de deduplicación

Con el fin de impedir la pérdida de datos, se recomienda utilizar RAID 10, 5 o 6. No es recomendable usar RAID 0 porque no es tolerante a errores. RAID 1 no es recomendable debido a su velocidad relativamente baja. No existe preferencia sobre discos locales o SAN, ambos son adecuados.

De 40 a 160 MB de RAM por 1 TB de datos únicos

Cuando se alcanza el límite, la deduplicación se detendrá, pero la copia de seguridad y la recuperación continuarán. Si añade más RAM al nodo de almacenamiento, la deduplicación se reanudará después de la siguiente copia de seguridad. En general, cuanta más memoria RAM tenga, mayores volúmenes de datos únicos podrá almacenar.

Solo una ubicación de deduplicación en cada nodo de almacenamiento

Le recomendamos encarecidamente que cree una sola ubicación de deduplicación en un nodo de almacenamiento. De lo contrario, todo el volumen de RAM disponible puede distribuirse en proporción a la cantidad de ubicaciones.

Ausencia de aplicaciones que compitan por recursos

El equipo con el nodo de almacenamiento no debe ejecutar aplicaciones que necesiten muchos recursos del sistema; por ejemplo, sistemas de gestión de bases de datos (DBMS) o sistemas de planificación de recursos empresariales (ERP).

Procesador de varios núcleos con al menos 2,5 GHz de frecuencia del reloj

Se recomienda utilizar un procesador con al menos cuatro núcleos y una frecuencia de al menos 2,5 GHz.

Espacio libre suficiente en la ubicación

La deduplicación en destino requiere tanto espacio libre como el ocupado por los datos de los que se ha realizado la copia de seguridad inmediatamente después de guardarse en la ubicación. Sin una compresión o deduplicación en el origen, este valor es igual al tamaño original de los datos incluidos en la copia de seguridad durante la operación de copia de seguridad dada.

LAN de alta velocidad

Se recomienda una LAN de 1 Gbit. Permite que el software realice 5-6 copias de seguridad con deduplicación en paralelo y la velocidad no disminuirá considerablemente.

Copia de seguridad de un equipo típico antes de la copia de seguridad de varios equipos con contenido similar

Al realizar la copia de seguridad de varios equipos con contenido similar, es recomendable que realice la copia de seguridad de un equipo primero y espere hasta que finalice la indexación de los datos incluidos en la copia de seguridad. Después de esto, los demás equipos se incluirán en la copia de seguridad más rápidamente debido a una eficaz deduplicación. Como la copia de seguridad del primer equipo se ha indexado, la mayoría de los datos ya se encuentran en el almacén de datos de deduplicación.

Copia de seguridad de distintos equipos en diferentes momentos

Si realiza la copia de seguridad de un gran número de equipos, divida la s operaciones de copia de seguridad en el tiempo. Para ello, cree varios planes de protección con varias programaciones.

Cifrado local

Si protege una ubicación con cifrado, todo lo escrito en la ubicación se cifrará y lo leído de ello lo descifrará de forma transparente el nodo de almacenamiento mediante el uso de una clave de cifrado específica de la ubicación almacenada en el nodo. Si una persona no autorizada le roba o accede al soporte de almacenamiento, esta persona no podrá descifrar el contenido de la ubicación si no tiene acceso al nodo de almacenamiento.

Este cifrado no tiene nada que ver con el cifrado de la copia de seguridad especificado por el plan de protección y realizado por un agente. Si lacopia de seguridad ya está cifrada, el cifrado del lado del nodo de almacenamiento se aplica al cifrado realizado por el agente.

Para proteger la ubicación mediante cifrado

1. Especifique y confirme una palabra (contraseña) que se utilizará para generar la clave de encriptación.

   La palabra distingue mayúsculas de minúsculas. Se le pedirá esta palabra solo al conectar la ubicación a otro nodo de almacenamiento.
2. Seleccione uno de los siguientes algoritmos de cifrado:
   - **AES 128**: el contenido de la ubicación se cifrará mediante el uso de el algoritmo Advanced Encryption Standard (AES) con una clave de 128 bits.
   - **AES 192**: el contenido de la ubicación se cifrará mediante el uso del algoritmo AES con una clave de 192 bits.
   - **AES 256**: el contenido de la ubicación se cifrará mediante el uso del algoritmo AES con una clave de 256 bits.
3. Haga clic en **Aceptar**.

El algoritmo de cifrado EEA funciona en el modo Cipher-block chaining (CBC) y utiliza una clave generada de manera aleatoria con un tamaño definido por el usuario de 128, 192 o 256 bits. Cuanto

mayor sea el tamaño de la clave, más tardará el programa en cifrar las copias de seguridad almacenadas en la ubicación y más seguras serán estas.

Entonces, la clave de cifrado se cifra con AES-256 usando un hash SHA-256 de la palabra seleccionada como clave. La palabra no se almacena en ninguna parte del disco; el hash de la palabra se usa para verificación. Con esta seguridad de dos niveles, las copias de seguridad están protegidas ante accesos no autorizados, aunque no es posible la recuperación de una palabra perdida.

Catalogación

Catálogo de datos

El catálogo de datos permite encontrar fácilmente la versión necesaria de los datos y seleccionarla para la recuperación. En el catálogo de datos se muestran los datos almacenados en las ubicaciones gestionadas en las que la catalogación está o estaba habilitada.

La sección **Catálogo** aparece en la pestaña **Almacenamiento de la copia de seguridad** solo si se ha registrado un servicio de catálogo como mínimo en el servidor de gestión. Para obtener más información acerca de cómo instalar el servicio de catálogo, consulte "Instalación de un nodo de almacenamiento y un servicio de catálogo".

La sección **Catálogo** aparece solo para los administradores de la organización.

Limitaciones

Solo se admite la catalogación con copias de seguridad a nivel de disco y a nivel de archivo de equipos físicos, y en copias de seguridad de equipos virtuales.

No pueden aparecer los datos siguientes en el catálogo:

- Datos de copias de seguridad cifradas
- Datos incluidos en copia de seguridad a dispositivo de cintas
- Datos incluidos en copia de seguridad a almacenamiento en la nube
- Datos de los que se ha realizado la copia de seguridad desde versiones del producto anteriores a Acronis Cyber Protect 12.5

Selección de los datos incluidos en la copia de seguridad para su recuperación

1. Haga clic en **Almacenamiento de copias de seguridad** > **Catálogo**.
2. Si hay varios servicios de catalogación registrados en el servidor de gestión, seleccione el servicio que catalogue las copias de seguridad almacenadas en la ubicación.

   Nota
   Para ver qué servicio cataloga una ubicación, seleccione la ubicación en **Copia de seguridad Almacenamiento**> **Ubicaciones** > **Ubicaciones** y haga clic en **Detalles**.

3. El software muestra los equipos de los que se ha realizado la copia de seguridad en las ubicaciones gestionadas que se han catalogado mediante el servicio de catalogación seleccionado.

   Examine las carpetas o realice una búsqueda para seleccionar los datos que desea recuperar.

   - **Examinación**

     Haga doble clic en un equipo para ver los discos, volúmenes, carpetas y archivos de los que se ha realizado la copia de seguridad.

     Para recuperar un disco, seleccione el disco marcado con el icono siguiente: 

     Para recuperar un volumen, haga doble clic en el disco que contenga el volumen y selecciónelo.

     Para recuperar archivos y carpetas, examine el volumen en el que estén ubicados. Puede examinar volúmenes marcados con el icono de carpeta: 

   - **Búsqueda**

     En el campo de búsqueda, escriba la información que ayude a identificar los elementos de datos necesarios (esto puede ser un nombre de equipo, un nombre de archivo o carpeta, o una etiqueta de disco) y, a continuación, haga clic en **Buscar**.

     Puede utilizar asteriscos (*) y signos de interrogación (?) como caracteres comodín.

     Como resultado de la búsqueda, verá la lista de elementos de datos de los que se ha realizado la copia de seguridad cuyos nombres coinciden total o parcialmente con el valor introducido.

4. De forma predeterminada, los datos se revertirán al momento específico más reciente posible. Si se selecciona un único elemento, puede utilizar el botón **Versiones** para seleccionar un punto de recuperación.
5. Una vez seleccionados los datos necesarios, elija de una de las opciones que se indican a continuación:
   - Haga clic en **Recuperar** y, a continuación, configure los parámetros de la operación de recuperación como se indica en ''Recuperación".
   - [Solo para archivos/carpetas] Si desea guardar los archivos en un archivo .zip, haga clic en **Descargar**, seleccione la ubicación en la que se guardarán los datos y haga clic en **Guardar**.

Catalogación de las prácticas recomendadas

Para incrementar el rendimiento de la catalogación, siga las recomendaciones que se indican a continuación.

Instalación

Le recomendamos que instale un servicio de catálogo y un nodo de almacenamiento en equipos independientes. Si no, estos componentes competirán por los recursos de la CPU y la memoria RAM.

Si hay varios nodos de almacenamiento registrados en el servidor de gestión, un solo servicio de catálogo será suficiente, a menos que se reduzca el rendimiento de la indexación o la búsqueda.

Por ejemplo, si ve que la catalogación funciona constantemente (es decir, que no hay pausas entre las actividades de catalogación), instale un servicio de catálogo más en un equipo independiente. A continuación, elimine algunas de las ubicaciones gestionadas y vuelva a crearlas con el nuevo servicio de catálogo. Se conservarán intactas las copias de seguridad almacenadas en estas ubicaciones.

Requisitos del sistema

Parámetro	Valor mínimo	Valor recomendado
Número de núcleos de la CPU	2	4 y más
RAM	8 GB	16 GB y más
Disco Duro	HDD de 7200 r. p. m.	SSD
Conexión de red entre el equipo con el nodo de almacenamiento y el equipo con el servicio de catálogo	100 Mbps	1 Gbps

Cómo habilitar o deshabilitar la catalogación

Si la catalogación está habilitada para una ubicación gestionada, el contenido de cada copia de seguridad enviado a la ubicación se añade al catálogo de datos en cuanto se crea la copia de seguridad.

Puede habilitar la catalogación al añadir una ubicación gestionada o en otro momento. Una vez que la catalogación esté habilitada, todas las copias de seguridad que estén almacenadas en la ubicación y que no se hayan catalogado previamente se catalogarán después de que se realice la siguiente copia de seguridad en la ubicación.

El proceso de catalogación puede requerir mucho tiempo, sobre todo si en la misma ubicación se encuentran las copias de seguridad de muchos equipos. Puede deshabilitar la catalogación en cualquier momento. Se completará la catalogación de las copias de seguridad que se crearon antes de la deshabilitación. Las copias de seguridad recién creadas no se catalogarán.

Pasos para configurar la catalogación para una ubicación existente

1. Haga clic en **Almacenamiento de copias de seguridad** > **Ubicaciones**.
2. Haga clic en **Ubicaciones** y, a continuación, seleccione la ubicación gestionada para la que quiere configurar la catalogación.
3. Haga clic en **Editar**.
4. Habilite o deshabilite el conmutador **Catalogar servicio**.
5. Haga clic en **Realizado**.

Configuración del sistema

Esta configuración solo está disponible para implementaciones locales.

Para acceder a esta configuración, haga clic en **Configuración** > **Configuración del sistema**.

La sección **Configuración del sistema** aparece solo para administradores de la organización.

Notificaciones por correo electrónico

Puede configurar los ajustes globales para las notificaciones por correo electrónico que se envían desde el servidor de administración cuando se produce un evento.

Nota
Estos ajustes no afectan al envío por correo electrónico de los informes programados. Consulte "Informes" (p. 657).

En las opciones de copia de seguridad predeterminadas, puede anular esta configuración solo para los eventos que suceden durante la copia de seguridad. En este caso, la configuración general será eficaz para las operaciones que no estén relacionadas con la copia de seguridad.

Al crear un plan de protección, puede elegir qué configuración desea utilizar: la configuración general o la configuración especificada en las opciones de copia de seguridad predeterminadas. Puede anular estas opciones con valores personalizados que sean específicos del plan.

Importante
Cambiar la configuración general de las notificaciones por correo electrónico afecta a todos los planes de protección que usan esta configuración.

Antes de ajustar estas opciones de configuración, asegúrese de que se hayan configurado las opciones del **servidor de correo electrónico**.

Para ajustar la configuración general de las notificaciones por correo electrónico:

1. Haga clic en **Configuración** > **Configuración del sistema** > **Notificaciones por correo electrónico**.
2. En el campo **Direcciones de correo electrónico de los destinatarios**, escriba la dirección de correo electrónico de destino. Puede introducir varias direcciones separadas por punto y coma.
3. [Opcional] En **Asunto**, cambie el asunto de la notificación por correo electrónico.
   Puede utilizar las variables siguientes:
   - `[Alert]` - resumen de alerta.
   - `[Device]` - nombre del dispositivo.
   - `[Plan]` - el nombre del plan que ha generado la alerta.
   - `[ManagementServer]` - el nombre del servidor del equipo en el que está instalado el servidor de

gestión.

- `[Unit]` - el nombre de la unidad al que pertenece el equipo.

  El asunto predeterminado es `[Alert]` **Dispositivo:** `[Device]` **Plan:** `[Plan]`

4. [Opcional] Seleccione la casilla de verificación **Resumen diario de alertas activas** y, a continuación, haga lo siguiente:
   a. Especifique el momento en que el resumen se enviará.
   b. [Opcional] Seleccione la casilla de verificación **No enviar mensajes de "No hay alertas activas"**.
5. [Opcional] Seleccione el idioma que se utilizará en las notificaciones por correo electrónico.
6. Seleccione las casillas de verificación de los eventos sobre los que desea recibir notificaciones. Puede hacerlo mediante la lista de todas las alertas posibles, agrupadas en función de la gravedad.
7. Haga clic en **Guardar**.

Servidor de correo electrónico

Puede especificar un servidor de correo electrónico que se utilizará para enviar notificaciones por correo electrónico desde el servidor de gestión.

Para especificar el servidor de correo electrónico

1. Haga clic en **Configuración** > **Configuración del sistema** > **Servidor de correo electrónico**.
2. En **Servicio de correo electrónico**, seleccione una de las siguientes opciones:
   - **Personalizado**
   - **Gmail**
   - **Correo Yahoo**
   - **Outlook.com**
3. [Solo en el caso de un servicio de correo electrónico personalizado] Especifique los ajustes siguientes:
   - En el campo **Servidor SMTP**, escriba el nombre del servidor de correo saliente (SMTP).
   - En **Puerto SMTP**, indique el puerto del servidor de correo saliente. El puerto predeterminado es el 25.
   - Seleccione si desea utilizar el cifrado TLS o SSL. Seleccione **Ninguno** para deshabilitar el cifrado.
   - Si el servidor SMTP necesita autenticación, seleccione la casilla de verificación **El servidor SMTP necesita autenticación** y, a continuación, especifique las credenciales de la cuenta que se utilizará para enviar mensajes. Si no está seguro de que el servidor SMTP requiera autenticación, póngase en contacto con su administrador de red o su proveedor de servicios de correo electrónico para obtener ayuda.

4. [Solo para Gmail, Yahoo Mail y Outlook.com] Especifique las credenciales de la cuenta que se utilizará para enviar mensajes.
5. [Solo en el caso de un servicio de correo electrónico personalizado] En **Remitente**, escriba el nombre del remitente. Este nombre aparecerá en el campo **De** en las notificaciones de correo electrónico. Si deja este campo en blanco, los mensajes contendrán la cuenta especificada en el paso 3 o 4.
6. [Opcional] Haga clic en **Enviar mensaje de correo electrónico de prueba** para comprobar si las notificaciones por correo electrónico funcionan correctamente con la configuración especificada. Introduzca una dirección de correo electrónico a la que enviar el mensaje de prueba.

Seguridad

Utilice estas opciones para mejorar la seguridad de la implementación local de Acronis Cyber Protect.

Cerrar la sesión de los usuarios inactivos tras

Esta opción le permite especificar un tiempo de espera para el cierre de sesión automático debido a la inactividad del usuario. Cuando falta un minuto del tiempo de espera establecido, el software solicita al usuario que mantenga la sesión iniciada. De lo contrario, se cerrará la sesión del usuario y se perderán los cambios que no se hayan guardado.

El valor predeterminado es el siguiente: **Habilitado. Tiempo de espera: 10 minutos.**

Mostrar una notificación sobre el último inicio de sesión del usuario actual

Esta opción permite mostrar la fecha y hora del último inicio de sesión correcto del usuario, el número de fallos de autenticación desde el último inicio de sesión correcto y la dirección IP de este. Esta información aparece en la parte inferior de la pantalla cada vez que el usuario inicia sesión.

El valor predeterminado es el siguiente: **Deshabilitado**.

Advertir sobre la caducidad de la contraseña local o de dominio

Esta opción permite mostrar la caducidad de la contraseña de acceso del usuario a Acronis Cyber Protect Management Server. Se trata de la contraseña local o del dominio con la que el usuario inicia sesión en el equipo donde está instalado el servidor de gestión. El tiempo que queda hasta que caduque la contraseña se muestra en la parte inferior de la pantalla y en el menú de la cuenta, situado en la esquina superior derecha.

El valor predeterminado es el siguiente: **Deshabilitado**.

Actualizaciones

Esta opción establece si Acronis Cyber Protect busca una nueva versión cada vez que un administrador de la organización inicie sesión en la consola web de Cyber Protect.

El valor predeterminado es el siguiente: **Habilitado**.

Si esta opción está deshabilitada, el administrador puede buscar actualizaciones manualmente, como se describe en "Buscar actualizaciones de software".

Opciones de copia de seguridad predeterminadas

Los valores predeterminados de opciones de copia de seguridad son los mismos para todos los planes de protección del servidor de gestión. Un administrador de organización puede cambiar el valor de una opción predeterminada por uno predefinido. El nuevo valor se utilizará de forma predeterminada en todos los planes de protección creados cuando se aplica el cambio.

Al crear un plan de protección, un usuario puede anular un valor predeterminado con un valor personalizado que será específico del plan en cuestión únicamente.

Para cambiar el valor de la opción predeterminada

1. Inicie sesión en la consola web de Cyber Protect como administrador de la organización.
2. Haga clic en **Configuración** > **Configuración del sistema**.
3. Amplíe la sección **Opciones de copia de seguridad predeterminadas**.
4. Seleccione la opción y, a continuación, realice los cambios necesarios.
5. Haga clic en **Guardar**.

Configuración de la protección

Para configurar los ajustes sobre protección, vaya a **Configuración** > **Protección** en la consola web de Cyber Protect.

Para obtener más información sobre la configuración y los procedimientos específicos, consulte el tema correspondiente en esta sección.

Actualización de las definiciones de protección

De forma predeterminada, todos los agentes de protección se pueden conectar a Internet para los siguientes componentes:

- Antimalware
- Evaluación de vulnerabilidades
- Gestión de parches

Agentes con el rol de actualizador

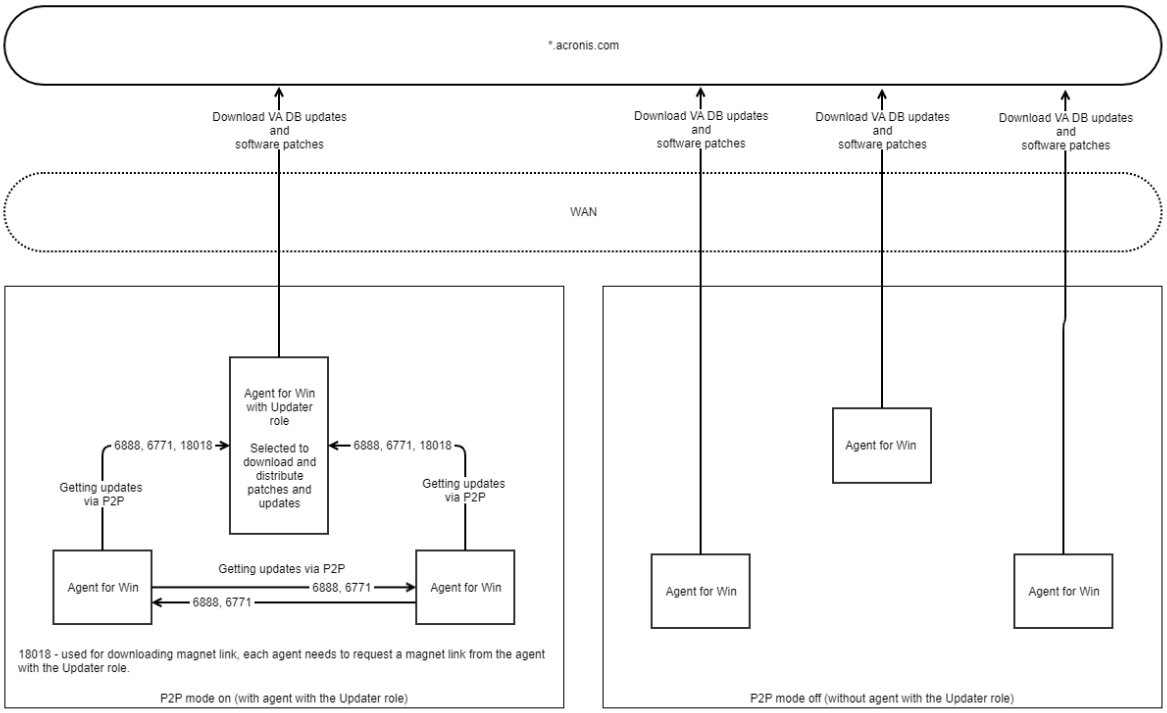
Un administrador puede minimizar el tráfico de ancho de banda de red al seleccionar uno o más agentes de protección en el entorno y asignarles el rol de actualizador. Así, los agentes dedicados se conectarán a Internet y descargarán actualizaciones. El resto de los agentes se conectará a los agentes del actualizador dedicado mediante tecnología de par a par y descargarán las actualizaciones.

Los agentes sin el rol de actualizador se conectarán a Internet si no hay un agente actualizador dedicado en el entorno o si no se puede establecer la conexión a un agente actualizador dedicado durante aproximadamente cinco minutos.

Antes de asignar el rol de actualizador a un agente, asegúrese de que el equipo en el que se ejecuta el agente es lo suficientemente potente y de que tenga una conexión a internet de alta velocidad estable y espacio suficiente en el disco.

Puede asignar el rol de actualizador a varios agentes en el entorno. De este modo, si un agente con el rol de actualizador no está conectado, otros agentes con este mismo rol serán una fuente para definiciones de protección actualizadas.

El siguiente diagrama ilustra las opciones para descargar las actualizaciones de protección. A la izquierda, se asigna el rol de actualizador a un agente. El agente se conecta a Internet para descargar las actualizaciones de protección y sus agentes del mismo nivel se conectan al agente actualizador para obtener las actualizaciones más recientes. A la derecha, no se asigna el rol de actualizador a ningún agente, por lo que todos los agentes se conectan a Internet para descargar las actualizaciones de protección.



Para preparar un equipo para el rol de actualizador

1. En el equipo en el que se ejecutará un agente con el rol de actualizador, aplique las siguientes reglas del cortafuegos:
   - Entrada "updater_incoming_tcp_ports": Permite la conexión a los puertos TCP 18018 y 6888 para todos los perfiles de cortafuegos (público, privado, y dominio).
   - Entrada "updater_incoming_udp_ports": Permite la conexión al puerto UDP 6888 para todos los perfiles de cortafuegos (público, privado, y dominio).
2. Reinicie el servicio Acronis Agent Core.
3. Reinicie el servicio de cortafuegos.

Si no aplica estas reglas y habilita el cortafuegos, los agentes del mismo nivel descargarán las actualizaciones de la nube.

Pasos para asignar el rol de actualizador a un agente

1. En la consola web de Cyber Protect, vaya a **Configuración** > **Agentes**.
2. Seleccione el equipo con el agente al que desea asignar el rol de actualizador.
3. Haga clic en **Detalles** y habilite el conmutador **Utilice este agente para descargar y distribuir parches y actualizaciones**.

Planificación de las actualizaciones

Puede planificar las actualizaciones automáticas de las definiciones de protección en todos los agentes o actualizarlas manualmente en los agentes seleccionados.

Pasos para programar actualizaciones automáticas

1. En la consola web de Cyber Protect, vaya a **Configuración** > **Protección** > **Actualización de definiciones de protección**.
2. Seleccione **Planificación**.
3. En **Tipo de planificación**, seleccione una de las siguientes opciones:
   - **Diariamente**

     Seleccione los días de la semana en los que desea que se actualicen las definiciones de protección.

     En **Iniciar a las**, seleccione la hora en que se iniciarán las actualizaciones.
   - **Cada hora**

     Defina una planificación granular para las actualizaciones.

     En **Ejecutar cada** defina la periodicidad de las actualizaciones.

     En **Desde las... Hasta**, establezca un intervalo de tiempo específico para las actualizaciones.

Pasos para actualizar las definiciones de protección de forma manual

1. En la consola web de Cyber Protect, vaya a **Configuración** > **Agentes**.
2. Seleccione los equipos en cuyos agentes desea actualizar las definiciones de protección y haga clic en **Actualizar definiciones**.

Cambio de ubicación de las descargas

Las definiciones de protección se descargan a la carpeta temporal predeterminada de su equipo y, a continuación, se guardan en la carpeta del programa de Acronis.

Pasos para cambiar la carpeta temporal de las descargas

1. En el equipo del servidor de gestión, abra el archivo `atp-database-mirror.json` para editarlo.

   Puede encontrar este archivo en las siguiente ubicación:
   - Windows: `%programdata%\Acronis\AtpDatabaseMirror\`
   - Linux: `/var/lib/Acronis/AtpDatabaseMirror/`
2. Cambie el valor de `"enable_user_config"` a `true`.

```
{
"sysconfig":
{
...
"enable_user_config": true
```

```
}
...
}
```

3. En el equipo del servidor de gestión, abra el archivo `config.json` para editarlo.
   Puede encontrar este archivo en las siguiente ubicación:
   - Windows: `%programdata%\Acronis\AtpDatabaseMirror\`
   - Linux: `/var/lib/Acronis/AtpDatabaseMirror/`
4. Añada la siguiente línea: `"mirror_temp_dir": "<path_to_new_download_location>"`
   Por ejemplo:

   ```
   {
           "mirror_temp_dir": "C:\\temp"
   }
   ```

   La ruta puede ser absoluta o relativa con respecto a la carpeta `AppData`.
   Si no se puede crear la carpeta o el servidor de gestión no puede escribir en ella, se utilizará la ubicación predeterminada.

Opciones de almacenamiento de caché

Los datos en la caché se almacenan en la siguiente ubicación:

- Windows: `C:\ProgramData\Acronis\Agent\var\atp-downloader\Cache`
- Linux: `/opt/acronis/var/atp-downloader/Cache`
- macOS: `/Library/Application Support/Acronis/Agent/var/atp-downloader/Cache`

Puede configurar una planificación para eliminar los datos en caché obsoletos y establecer un límite para el tamaño. Puede configurar diferentes límites para los equipos con agentes no actualizadores y los equipos con agentes actualizadores.

Fuente de las últimas definiciones de protección

Puede descargar las últimas definiciones de protección desde las siguientes ubicaciones:

- **La nube**
  Los agentes de protección se conectan a Internet y descargan las últimas definiciones de protección desde Acronis Cloud. De forma predeterminada, todos los agentes que están registrados en el servidor de gestión buscan las actualizaciones y las distribuyen. Para obtener más información sobre los agentes con el rol de actualizador, consulte "Actualización de las definiciones de protección" (p. 702).
- **Cyber Protect Servidor de administración**

Con esta opción, los agentes no necesitan acceso a Internet. Solo se conectan al servidor de gestión cuando las definiciones de protección están almacenadas. Sin embargo, el servidor de gestión necesita conectarse a Internet para descargar las últimas definiciones de protección.

- **Servidores web personalizados**
  Esta opción solo está destinada a la solución de problemas y para fines de prueba o para su uso en entornos aislados. Para obtener más información, consulte "Actualización de definiciones de protección en un entorno aislado" (p. 706). Por lo general, solo debe seleccionarla cuando el equipo de soporte técnico de Acronis se lo indique.

Conexión remota

Cuando habilite la conexión remota, las opciones **Conectar a través del cliente RDP** y **Conectar a través del cliente HTML5** aparecerán en la consola web de Cyber Protect, debajo del **Escritorio de ciberprotección** en el menú de la derecha. El menú de la derecha se abre cuando selecciona una carga de trabajo en la pestaña **Dispositivos**.

Activar o desactivar la conexión remota afecta a todos los usuarios de su organización.

Pasos para habilitar la conexión remota

1. En la consola web de Cyber Protect, vaya a **Configuración** > **Protección**.
2. Haga clic en **Conexión remota** y habilite el conmutador **Conexión de escritorio remoto**.

Además, puede activar el uso compartido de la conexión remota. Con esta opción, podrá generar un enlace para acceder a la carga de trabajo seleccionada de forma remota. Puede compartir estos enlaces con otros usuarios.

Pasos para habilitar el uso compartido de la conexión remota

1. En la consola web de Cyber Protect, vaya a **Configuración** > **Protección**.
2. Seleccione la casilla de verificación **Compartir conexión de escritorio remoto**.

Como resultado, la opción **Compartir conexión remota** aparece en la consola web de Cyber Protect, debajo del **Escritorio de ciberprotección**, en el menú de la derecha.

Actualización de definiciones de protección en un entorno aislado

Acronis Cyber Protect admite la actualización de las definiciones de protección en entornos aislados.

Pasos para actualizar las definiciones de protección en un entorno aislado

1. Instale un segundo servidor de administración que pueda acceder a Internet, fuera de su entorno aislado.

Para obtener más información sobre cómo hacerlo, consulte "Instalación del servidor de gestión" (p. 105).

2. Copie las definiciones de protección del servidor de administración en línea a una unidad extraíble y transfiera las definiciones a un servidor HTTP en el entorno aislado.

   Para obtener más información sobre este paso, consulte "Descarga de definiciones en un servidor de administración en línea" (p. 707) y "Transferencia de definiciones a un servidor HTTP" (p. 708).

3. En el servidor de administración aislado, configure el servidor HTTP como fuente de las definiciones de protección actualizadas.

   Para obtener más información sobre este paso, consulte "Configuración de la fuente de definiciones en el servidor de administración aislado" (p. 709).

Descarga de definiciones en un servidor de administración en línea

Después de instalar un segundo servidor de administración con acceso a Internet, descargue las últimas definiciones de protección y cópielas a una unidad extraíble, como una memoria flash USB o un disco duro externo.

Pasos para descargar y copiar las definiciones de protección

1. En el equipo con el servidor de administración en línea, copie la carpeta `AtpDatabaseMirror` a una ubicación de su elección, por ejemplo, el escritorio o la carpeta `Temp`.

   Puede encontrar la carpeta `AtpDatabaseMirror` en la siguiente ubicación:

   - Windows: `%ProgramData%\Acronis\`
   - Linux: `/usr/lib/Acronis/`

2. Abra el archivo `atp_database_mirror.json` para editarlo. Puede encontrar el archivo en la siguiente ubicación:

   - Windows: `%Program Files%\Acronis\AtpDatabaseMirror`

     Nota
     En Windows, esta carpeta no es la misma que la carpeta del paso anterior.

   - Linux: `/usr/lib/Acronis/AppDatabaseMonitor`

3. Edite el archivo `atp_database_mirror.json` del siguiente modo:

   a. Cambie el valor de `"enable_appdata_as_root"` a `false`.

   b. Cambie los valores de todas las entradas de `"local_path"` a la ruta absoluta de la ubicación en la que desee guardar las definiciones de protección.

4. Guarde los cambios en el archivo `atp_database_mirror.json`.

5. En el equipo con el servidor de administración en línea, detenga **Acronis Management Server Service** mediante el siguiente comando:

   - Windows (símbolo del sistema):

     ```
     sc stop AcrMngSrv
     ```

- Linux (Terminal):

```
sudo systemctl stop acronis_ams.service
```

6. En la carpeta `AtpDatabaseMirror` que copió a una ubicación de su elección, inicie la herramienta `AtpDatabaseMirror` con el siguiente comando:
   - Windows (símbolo del sistema):

```
atp_database_mirror.exe -config atp_database_mirror.json
```

   - Linux (Terminal):

```
sudo ./atp_database_mirror -config atp_database_mirror.json
```

   Cuando se descarguen todas las actualizaciones a la carpeta que especificó en `"local_path"`, aparecerá la siguiente línea en símbolo del sistema o la ventana de terminal:

```
standing by for 1m0s
```

7. Detenga la herramienta `AtpDatabaseMirror` presionando CTRL+C.
8. Copie los archivos de la carpeta que especificó en `"local_path"` a una unidad extraíble.

A continuación, debe copiar los archivos de una unidad extraíble a un servidor HTTP de su entorno aislado. Puede utilizar el servidor de administración aislado como un servidor HTTP. Para obtener más información, consulte "Transferencia de definiciones a un servidor HTTP" (p. 708).

Transferencia de definiciones a un servidor HTTP

Para distribuir las definiciones de protección en su entorno aislado, necesita un servidor HTTP dedicado. Puede utilizar el servidor de administración aislado como un servidor HTTP.

Pasos para transferir definiciones de protección a un servidor HTTP

1. En el equipo en el que ejecutará el servidor HTTP, copie las definiciones de protección a una carpeta de su elección.
2. Desde la carpeta en donde haya copiado las definiciones de protección, inicie un servidor HTTP. Por ejemplo, puede utilizar Python y ejecutar el siguiente comando:

```
python -m http.server 8080
```

   Nota
   Puede utilizar el servidor HTTP que prefiera.

3. En la carpeta en donde haya copiado las definiciones de protección, abra los archivos `update-index.json` para editarlos:
   - `./ngmp/update-index.json`
   - `./vapm/update-index.json`

4. En ambos archivos `update-index.json`, edite todos los campos `productos > so > arch > componentes > versiones > url` como sigue:
   a. Como valores de `IP` y `puerto`, establezca la dirección IP y el puerto de su servidor HTTP.
   b. No cambie la otra parte de la ruta.

   Por ejemplo, `"url": "http://192.168.1.10:8080/ngmp/win64/ngmp.zip"`, donde 192.168.1.10 es la dirección IP del servidor HTTP y 8080 es su puerto. No cambie la parte `/ngmp/win64/ngmp.zip`.
5. Guarde los cambios en ambos archivos `update-index.json`.

A continuación, debe configurar la fuente de definiciones de protección en el servidor de administración aislado. Para obtener más información, consulte "Configuración de la fuente de definiciones en el servidor de administración aislado" (p. 709).

Configuración de la fuente de definiciones en el servidor de administración aislado

Una vez configurado el servidor HTTP, debe configurarlo en el servidor de administración aislado como fuente de las definiciones de protección.

Pasos para configurar la fuente de definiciones de protección en el servidor de administración aislado

1. En la consola web de Cyber Protect del servidor de administración aislado, vaya a **Configuración** > **Protección** > **Actualización de definiciones de protección**.
2. Seleccione **Definiciones**.
3. Seleccione **Personalizar** y especifique las siguientes rutas:

- Para las **Definiciones de antivirus y antimalware**:
  `http://<IP address of your HTTP server>:8080/scanner`
- Para las **Definiciones de detecciones avanzadas**:
  `http://<IP address of your HTTP server>:8080/ngmp`
- Para las **Definiciones de evaluación de vulnerabilidades y gestión de parches**:
  `http://<IP address of your HTTP server>:8080/vapm`

Como resultado, los agentes en el entorno aislado descargarán las definiciones de protección del servidor HTTP.

Administración de cuentas de usuario y unidades de organización

Implementación local

La funcionalidad descrita en esta sección solo está disponible para administradores de la organización.

Para acceder a esta configuración, haga clic en **Configuración** > **Cuentas**.

Unidades y cuentas administrativas

Para gestionar unidades y cuentas administrativas, en la Cyber Protect consola web, vaya a **Configuración** > **Cuentas**. El panel **Cuentas** muestra el grupo **Organización** con las unidades del árbol (si las hubiera) y la lista de cuentas administrativas en el nivel jerárquico seleccionado.

Unidades

El grupo **Organización** se crea automáticamente al instalar el servidor de gestión. Con la licencia Acronis Cyber Protect Advanced puede crear grupos secundarios llamados unidades, que normalmente corresponden a unidades o departamentos de la organización, y añadir cuentas administrativas a dichas unidades. De esta forma, puede delegar la gestión de protección a otras personas cuyos permisos de acceso estarán estrictamente limitados a las unidades correspondientes. Para obtener información sobre cómo crear una unidad, consulte "Creación de unidades" (p. 715).

Cada unidad puede tener unidades secundarias. Las cuentas administrativas de la unidad principal tienen los mismos derechos en todas las unidades secundarias. El grupo **Organización** es la unidad principal de máximo nivel, y las cuentas administrativas de este nivel tienen los mismos derechos en todas las unidades.

Cuentas administrativas

Cualquier cuenta con la que se pueda iniciar sesión en la Cyber Protect consola web se considera cuenta administrativa.

En la Cyber Protect consola web, cualquier cuenta administrativa puede ver o gestionar todo lo que se encuentre en el nivel jerárquico de su unidad o por debajo de él. Por ejemplo, una cuenta administrativa en la *Organización* tiene acceso a este máximo nivel y, por lo tanto, acceso a todas las unidades de esta organización, mientras que una cuenta administrativa en determinada *unidad* solo puede acceder a dicha unidad y a sus unidades secundarias.

¿Qué cuentas pueden ser administrativas?

Si el servidor de gestión está instalado en un equipo de Windows incluido en un dominio de Active Directory, puede otorgar derechos administrativos a usuarios locales o usuarios y grupos de usuarios del bosque de dominios de Active Directory.

De forma predeterminada, el servidor de gestión establece una conexión protegida mediante SSL/TLS con el controlador de dominio de Active Directory. Si esto no es posible, no se establecerá ninguna conexión. Sin embargo, puede permitir conexiones no seguras editando el archivo `auth-connector.json5`.

Si quiere utilizar una conexión segura, compruebe que LDAP over SSL (LDAPS) esté configurado para su Active Directory.

Configurar LDAPS para Active Directory

1. En el controlador de dominio, cree e instale un certificado LDAPS que cumpla los requisitos de Microsoft.
   Para obtener más información sobre cómo realizar estas operaciones, consulte Habilitar LDAP sobre SSL con una entidad de certificación de terceros en la documentación de Microsoft.
2. En el controlador de dominio, abra **Microsoft Management Console** y verifique que el certificado existe en **Certificados (Equipo Local)** > **Personal** > **Certificados**.
3. Reinicie el controlador de dominio.
4. Verifique que LDAPS está habilitado.

Pasos para permitir conexiones no seguras al controlador de dominio

1. Inicie sesión en el equipo donde está instalado el servidor de gestión.
2. Abra el archivo `auth-connector.json5` para editarlo.
   El archivo `auth-connector.json5` está ubicado en `%ProgramFiles%\Acronis\AuthConnector`.
3. Vaya a la sección **sync** y, en todas las líneas **"connectionMode"**, sustituya **"ssl_only"** por **"auto"**.
   En el modo **auto**, se establece una conexión no segura si no es posible conectarse a través del TLS.
4. Reinicie **Acronis Service Manager Service** como se indica en "Pasos para reiniciar el servicio del administrador de servicios de Acronis" (p. 243).

Nota
Si el servidor de gestión no se incluye en un dominio de Active Directory o si está instalado en un equipo Linux, puede otorgar derechos administrativos a usuarios y grupos locales.

Para saber cómo añadir una cuenta administrativa al servidor de gestión, consulte la sección "Incorporación de cuentas administrativas" (p. 714).

Roles de las cuentas administrativas

A cada cuenta administrativa se le asigna un rol con los derechos predefinidos necesarios para desempeñar determinadas tareas. Los roles de las cuentas administrativas son los siguientes:

- **Administrador**
  Este rol proporciona acceso completo de administrador a la organización o a una unidad.
- **Solo lectura**
  Este rol proporciona acceso de solo lectura a la Cyber Protect consola web. Solo permite recopilar datos de diagnóstico, como informes del sistema. El rol de solo lectura no permite consultar copias de seguridad o examinar el contenido de buzones de correo de los que se haya realizado una copia de seguridad.
- **Auditor**
  Este rol proporciona acceso de solo lectura a la pestaña **Actividades** de la Cyber Protect consola web. Para obtener más información sobre esta pestaña, consulte "La pestaña Actividades" (p. 655). Este rol no permite recopilar ni explorar ningún dato, incluida la información del sistema del servidor de gestión.

Los cambios de los roles se muestran en la pestaña **Actividades**.

Herencia de roles

Las unidades secundarias heredan los roles de su unidad principal. Si la misma cuenta de usuario tiene diferentes roles asignados en la unidad principal y en una unidad secundaria, tendrá ambos roles.

Los roles también se pueden asignar de forma explícita a una cuenta de usuario específica o heredada de un grupo de usuarios. Por lo tanto, una cuenta de usuario puede tener tanto un rol asignado de forma específica como uno heredado.

Si una cuenta de usuario tiene diferentes roles (asignado y/o heredado), podrá acceder a objetos y ejecutar acciones permitidas por cualquiera de estos roles. Por ejemplo, una cuenta de usuario con un rol asignado de solo lectura y un rol heredado de administrador tendrá derechos de administrador.

Importante
En la consola web de Cyber Protect, solo se muestran los roles asignados de forma explícita a la unidad actual. No se muestran las posibles discrepancias con los roles heredados. Le recomendamos encarecidamente asignar roles de administrador, de solo lectura y de auditor a cuentas o grupos independientes para evitar posibles problemas con los roles heredados.

Administradores predeterminados

En Windows

Al instalar el servidor de gestión en un equipo, sucede lo siguiente:

- Se crea el grupo de usuarios **Acronis Centralized Admins** en el equipo.

  En un controlador de dominio, el grupo se llama *DCNAME* **$ Acronis Centralized Admins**. Aquí, *DCNAME* representa el nombre NetBIOS del controlador de dominio.
- Todos los miembros del grupo **Administradores** se añaden al grupo **Acronis Centralized Admins**. Si el equipo se encuentra en un dominio, pero este no es un controlador de dominio, los usuarios locales (es decir, que no formen parte del dominio) están excluidos. En un controlador de dominio, no existe ningún usuario que no forme parte de él.
- Los grupos **Acronis Centralized Admins** y **Administradores** se añaden al servidor de gestión como **administradores de la organización**. Si el equipo se encuentra en un dominio, pero este no es un controlador de dominio, no se añade el grupo de **administradores**, por lo que los usuarios locales (es decir, que no formen parte del dominio) no se convierten en administradores de la organización.

Puede eliminar el grupo **Administradores** de la lista de los administradores de la organización. No obstante, el grupo **Acronis Centralized Admins** no se puede eliminar. En el caso poco probable de que todos los administradores de la organización se hayan eliminado, puede añadir una cuenta al grupo **Acronis Centralized Admins** en Windows, y luego iniciar sesión en la consola web de Cyber Protect mediante esta cuenta.

En Linux

Al instalar el servidor de gestión en un equipo, el usuario **raíz** se añade al servidor de gestión como **administrador de la organización**.

Puede añadir otros usuarios de Linux a la lista de administradores del servidor de gestión como se describe más adelante y eliminar al usuario **raíz** de esta lista. En el caso poco probable de que se hayan eliminado todos los administradores de la organización, podrá reiniciar el servicio `acronis_asm`. Como resultado, el usuario **raíz** volverá a añadirse automáticamente como administrador de la organización.

Cuentas administrativas en varias unidades

Una cuenta puede recibir derechos administrativos en cualquier número de unidades. En una cuenta de este tipo, así como para cuentas administrativas del nivel de la organización, el selector de unidades se muestra en la Cyber Protect consola web. Mediante este selector, esta cuenta puede ver y gestionar cada unidad por separado.

Aunque una cuenta tenga permisos para todas las unidades de la organización, no tiene permiso para la organización. Las cuentas administrativas del nivel de la organización deben añadirse al grupo **Organización** explícitamente.

Cómo poblar las unidades con equipos

Cuando un administrador añade un equipo a través de la interfaz web, el equipo se añade a la unidad gestionada por el administrador. Si el administrador gestiona varias unidades, el equipo se

añade a la unidad seleccionada en el selector de unidades. Por tanto, el administrador debe seleccionar la unidad antes de hacer clic en **Añadir**.

Al instalar agentes localmente, el administrador proporciona sus credenciales. El equipo se añade a la unidad gestionada por el administrador. Si el administrador gestiona varias unidades, el instalador le pedirá que elija una a la que se añadirá el equipo.

Incorporación de cuentas administrativas

Nota
Esta característica no está disponible en las ediciones Standard y Essentials.

Pasos para añadir cuentas

1. Haga clic en **Ajustes** > **Cuentas**.
   El software muestra la lista de administradores del servidor de gestión y las unidades del árbol (si las hubiera).
2. Seleccione **Organización** o seleccione la unidad a la que desea añadir un administrador.
3. Haga clic en **Agregar cuenta**.
4. En **Dominio**, seleccione el dominio que contiene las cuentas de usuario que desea añadir. Si el servidor de gestión no está incluido en un dominio de Active Directory o está instalado en Linux, solo pueden añadirse usuarios locales.
5. Busque el nombre del usuario o el nombre del grupo de usuarios.
6. Haga clic en "+" al lado del nombre del usuario o del grupo.
7. Seleccione el rol de la cuenta.
8. Repita los pasos del 4 al 6 para todos los usuarios o grupos que desee añadir.
9. Al finalizar, haga clic en **Listo**.
10. [Solo en Linux] Añada los nombres de usuario a la configuración del módulo de autenticación conectable (PAM) para los módulos de Acronis tal como se describe a continuación.

Pasos para añadir usuarios a la configuración de PAM para Acronis

Este proceso se aplica a los servidores de gestión que se ejecutan en equipos Linux y en el dispositivo todo en uno de Acronis Cyber Protect.

1. En el equipo que ejecuta el servidor de gestión, abra el archivo **/etc/security/acronisagent.conf** como usuario raíz en un editor de texto.
2. En este archivo, escriba los nombres de usuario que ha añadido como administradores del servidor de gestión, uno en cada línea.
3. Guarde y cierre el archivo.

Creación de unidades

1. Haga clic en **Ajustes** > **Cuentas**.
2. El software muestra la lista de administradores del servidor de gestión y las unidades del árbol (si las hubiera).
3. Seleccione **Organización** o bien la unidad principal de la nueva unidad.
4. Haga clic en **Crear Unidad**.
5. Especifique un nombre para la nueva unidad y, a continuación, haga clic en **Crear**.

Implementación en la nube

La administración de cuentas de usuario y de unidades de la organización está disponible en el portal de gestión. Para acceder al portal de gestión, haga clic en **Portal de administración** cuando inicie sesión en el servicio Cyber Protection o bien haga clic en el icono  de la parte superior derecha y en **Portal de administración**. Solo los usuarios con privilegios administrativos pueden acceder a este portal.

Para obtener información sobre la administración de cuentas de usuario y unidades de la organización, consulte la Guía del administrador del portal de gestión. Para acceder a este documento, haga clic en el icono del signo de interrogación en el portal de gestión.

Esta sección proporciona información adicional sobre la administración del servicio de ciberprotección.

Cuotas

Las cuotas le permiten limitar la capacidad de los usuarios de utilizar el servicio. Para establecer las cuotas, seleccione el usuario en la pestaña **Usuarios** y haga clic en el icono del lápiz en la sección **Cuotas**.

Cuando se supera una cuota, se envía una notificación a la dirección de correo electrónico del usuario. Si no establece un uso por encima del límite de cuota, la cuota se considera "blanda". Esto significa que no se aplican restricciones para usar el servicio de ciberprotección.

También puede especificar usos por encima del límite de la cuota. Un uso por encima del límite permite al usuario sobrepasar la cuota en un valor especificado. Si el uso por encima del límite se sobrepasa, se aplican las restricciones sobre el uso del servicio de ciberprotección.

Copia de seguridad

Puede especificar la cuota de almacenamiento en la cloud, la de copia de seguridad local y el número máximo de equipos, dispositivos o buzones de correo que un usuario puede proteger. Están disponibles las cuotas siguientes:

- **Almacenamiento en la cloud**
- **Estaciones de trabajo**
- **Servidores**
- **Windows Server Essentials**
- **Servidores virtuales**
- **Universal**
  Esta cuota se puede utilizar en lugar de cualquiera de las cuatro cuotas mencionadas anteriormente: estaciones de trabajo, servidores, Windows Server Essentials y servidores virtuales.
- **Dispositivos móviles**
- **Buzones de correo de Microsoft 365**
- **Copia de seguridad local**

Se considera que un equipo, dispositivo o un buzón de correo están protegidos si se les aplica como mínimo un plan de protección. Un dispositivo móvil se considera protegido después de la primera copia de seguridad.

Si se supera este uso por encima del límite de la cuota de almacenamiento en la cloud, no se realizan copias de seguridad. Cuando se supera el límite de exceso de dispositivos, el usuario no puede aplicar un plan de protección a más dispositivos.

La cuota de las **copias de seguridad locales** limita el tamaño total de las copias de seguridad locales que se crean mediante el uso de la infraestructura en la cloud. Para esta cuota no se puede establecer un uso por encima del límite.

Recuperación ante desastres

Estas cuotas las aplica el proveedor de servicios de toda la empresa. Los administradores de la empresa pueden ver las cuotas y el uso en el portal de gestión, pero no pueden establecer cuotas para un usuario.

- **Almacenamiento de recuperación ante desastres**
  Este almacenamiento lo usan los servidores principales y los de recuperación. Si se alcanza el uso por encima del límite para esta cuota, no se podrán crear servidores principales ni de recuperación ni agregar o extender discos de los servidores principales existentes. Si se supera el uso por encima del límite para esta cuota, no se podrá iniciar una conmutación por error ni simplemente iniciar un servidor detenido. Los servidores en ejecución siguen funcionando. Cuando la cuota se deshabilita, todos los servidores se eliminan. La pestaña **Sitio web de recuperación en la nube** desaparece de la consola web de Cyber Protect.
- **Puntos del equipo**
  Esta cuota limita los recursos de la CPU y la RAM que consumen los servidores principales y los de recuperación durante un periodo de facturación. Si se alcanza el uso por encima del límite para esta cuota, todos los servidores principales y de recuperación se apagarán. Estos servidores

no se pueden usar hasta que comience el siguiente periodo de facturación. El periodo de facturación predeterminado es un mes completo.

Cuando la cuota se deshabilita, los servidores no se pueden usar, independientemente del periodo de facturación.

- **Direcciones IP públicas**

  Esta cuota limita el número de direcciones IP públicas que se pueden asignar a los servidores principales y de recuperación. Si se alcanza el uso por encima del límite para esta cuota, no se podrán habilitar direcciones IP públicas para más servidores. Desmarque la casilla de verificación **Dirección IP pública** de la configuración del servidor para hacer que no pueda usar ninguna IP pública. Después, puede permitir que otro servidor use una dirección IP pública, que normalmente no será la misma.

  Cuando la cuota se deshabilita, todos los servidores dejan de usar direcciones IP públicas y, por tanto, no se puede acceder a ellos desde Internet.
- **Servidores en la cloud**

  Esta cuota limita el número total de servidores primarios y de recuperación. Si se alcanza el uso por encima del límite para esta cuota, no se podrán crear servidores principales ni de recuperación.

  Cuando la cuota se deshabilita, los servidores se pueden ver en la consola web de Cyber Protect, pero la única operación disponible es **Eliminar**.
- **Acceso a Internet**

  Esta cuota habilita o deshabilita el acceso a Internet desde servidores principales y de recuperación.

  Cuando está deshabilitada, los servidores principales y de recuperación se desconectan de Internet inmediatamente. El conmutador de **acceso a Internet** de las propiedades del servidor se borra y se deshabilita.

Notificaciones

Para cambiar los ajustes de notificaciones para un usuario, seleccione el usuario en la pestaña **Usuarios** y haga clic en el icono del lápiz en la sección **Configuración**. Están disponibles los siguientes ajustes de notificaciones:

- **Notificaciones de uso excesivo de las cuotas** (habilitado de forma predeterminada)

  Las notificaciones sobre cuotas superadas.
- **Informes de uso planificados**

  Informes de uso descritos a continuación que se envían el primer día de cada mes.
- **Notificaciones de error**, **Notificaciones de advertencia** y **Notificaciones de acciones realizadas correctamente** (deshabilitado de forma predeterminada)

  Notificaciones relacionadas con los resultados de la ejecución de planes de protección y con los resultados de las operaciones de recuperación ante desastres de cada dispositivo.
- **Resumen diario de alertas activas** (habilitado de forma predeterminada)

Resumen que informa sobre copias de seguridad fallidas u omitidas, y otros problemas. El resumen se envía a las 10:00 (hora del centro de datos). Si no hay problemas en ese momento, no se envía el resumen.

Todas las notificaciones se envían a la dirección de correo electrónico del usuario.

Informes

El informe sobre el uso del servicio de ciberprotección incluye los datos siguientes sobre la organización o una unidad:

- Tamaño de las copias de seguridad por unidad, usuario o tipo de dispositivo.
- Número de dispositivos protegidos por unidad, usuario o tipo de dispositivo.
- Precio por unidad, usuario o tipo de dispositivo.
- El tamaño total de las copias de seguridad.
- La cantidad total de dispositivos protegidos.
- Precio total.

Referencia de la línea de comandos

La referencia de la línea de comandos es un documento independiente disponible en https://www.acronis.com/en-us/support/documentation/AcronisCyberProtect_15_Command_Line_Reference/index.html.

Solución de problemas

Esta sección detalla cómo guardar un registro de Agente en un archivo .zip. Si se produce un fallo sin un motivo claro en una copia de seguridad, este archivo ayudará al personal de soporte técnico a identificar el problema.

Para recopilar registros

1. Realice uno de los siguientes procedimientos:
   - En **Dispositivos**, seleccione el equipo cuyos registros desea recopilar y haga clic en **Actividades**.
   - En **Configuración** > **Agentes**, seleccione el equipo cuyos registros desea recopilar y haga clic en **Detalles**.
2. Haga clic en **Recopilar información del sistema**.
3. Si se lo pide el navegador web, indique dónde quiere guardar el archivo.

Glosario

C

Conjunto de copias de seguridad

Es un grupo de copias de seguridad al que se le puede aplicar una regla de retención individual. Para el esquema personalizado de copia de seguridad, los conjuntos de copias de seguridad se corresponden con los métodos de copia de seguridad (completa, diferencial e incremental). En los demás casos, los conjuntos de copias de seguridad son mensual, diaria, semanal o cada hora. Una copia de seguridad mensual es la primera copia de seguridad creada una vez comenzado un mes. Una copia de seguridad semanal es la primera copia de seguridad que se crea el día de la semana seleccionado en la opción Copia de seguridad semanal (haga clic en el icono de engranaje y, a continuación, en Opciones de copia de seguridad > Copia de seguridad semanal). Si una copia de seguridad semanal es también la primera copia de seguridad que se crea en un nuevo mes, se considerará mensual. En ese caso, se creará una copia de seguridad semanal el día de la semana siguiente seleccionado. Una copia de seguridad diaria es la primera copia de seguridad que se crea en un día, excepto si puede considerarse mensual o semanal. Una copia de seguridad de cada hora es la primera copia de seguridad que se crea en una hora, excepto si puede considerarse mensual, semanal o diaria.

Copia de seguridad completa

Es una copia de seguridad autosuficiente que contiene todos los datos seleccionados para la copia de seguridad. No necesita acceso a otra copia de seguridad para recuperar los datos de una copia de seguridad completa.

Copia de seguridad diferencial

Una copia de seguridad diferencial almacena todos los cambios desde la última copia de seguridad completa. Necesita tener acceso a la copia de seguridad completa correspondiente para recuperar los datos de una copia de seguridad diferencial.

Copia de seguridad incremental

Es una copia de seguridad que almacena los cambios de los datos a partir de la última copia de seguridad. Necesita tener acceso a otras copias de seguridad para recuperar los datos de una copia de seguridad incremental.

F

Formato de copia de seguridad de archivo único

Es un nuevo formato de copia de seguridad en el que las copias de seguridad iniciales completas e incrementales subsiguientes se guardan en un único archivo .tib en lugar de una cadena de archivos. 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, por ejemplo: servidores SFTP.

S

Startup Recovery Manager

Una modificación del agente reiniciable, que reside en el disco del sistema y está configurado para iniciarse al momento del inicio al presionarse F11. Startup Recovery Manager elimina la necesidad de un dispositivo de rescate o conexión de red para iniciar la utilidad de rescate de arranque. Startup Recovery Manager es especialmente útil para los usuarios móviles. En caso de fallo, el usuario reinicia el equipo, pulsa F11 cuando aparezca el aviso "Pulse F11 para Startup Recovery Manager..." y realiza una recuperación de datos de la misma forma que con un soporte de arranque común.
Limitación: requiere la reactivación de cargadores que no sean los de Windows ni GRUB.

U

Ubicación gestionada

Es una ubicación copia de seguridad gestionada por un nodo de almacenamiento.
Físicamente, las ubicaciones gestionadas pueden residir en una red compartida, SAN, NAS, en un disco duro local conectado al nodo de almacenamiento, o en una biblioteca de cintas conectada de manera local al nodo de almacenamiento. El nodo de almacenamiento lleva a cabo la limpieza y la validación (si estas tareas están incluidas en un plan de protección) para cada copia de seguridad almacenada en la ubicación gestionada. Usted puede especificar las operaciones adicionales que el nodo de almacenamiento debe realizar (cifrado, deduplicación).

Índice

L

O

P

S

T

U

V

W