Acronis

Acronis Backup 12.5

Update 4

GUÍA DEL USUARIO

Contenido

1 Novedades en Acronis Backup

***Importante** Estas nuevas características están disponibles **solo en implementaciones en una instalación**. Se propagarán a implementaciones en la nube en futuras versiones.*

1.1 Novedades en la actualización 4

Copia de seguridad

- La opción mejorada de copias de seguridad **Ventana de copia de seguridad y rendimiento** (pág. 140) (antes **Performance**) sirve para establecer uno de los tres niveles de rendimiento de copia de seguridad (alto, bajo o sin permiso) para cada hora de la semana. El nivel alto y el bajo se pueden configurar en lo que respecta a la velocidad de salida y prioridad del proceso.
- Opción de copias de seguridad "Envío de datos físicos" (pág. 143) para las copias de seguridad en el cloud

Recuperación

Capacidad de guardar información del sistema en un disco local o una red compartida si falla una acción de recuperación con reinicio.

Escalabilidad

El número máximo de equipos físicos que se pueden registrar en un servidor de gestión ha aumentado de 4000 a 8000 (pág. 35).

Seguridad

- Capacidad de deshabilitar el registro anónimo (pág. 332) para que haya que introducir siempre el nombre de usuario y la contraseña del administrador del servidor de gestión al registrar un dispositivo.
- Toda la comunicación que se lleve a cabo durante el registro de un dispositivo se realiza mediante HTTPS. Funciona perfectamente y no se puede deshabilitar. En Windows (pág. 55) y Linux (pág. 60), se puede aplicar la verificación de certificados durante una instalación sin supervisión.
- Registro masivo de dispositivos mediante el uso de un token en lugar de con nombre de usuario y contraseña (pág. 73)

Aplicaciones

- Compatibilidad con Microsoft Exchange Server 2019 (pág. 27)
- El CBT (seguimiento de archivos modificados a nivel de bloque) (pág. 132) se puede deshabilitar para copias de seguridad de bases de datos de SQL y Exchange.

Active Protection

Nuevas opciones de protección:

- Existe la opción de permitir que ciertos procesos modifiquen los archivos de copia de seguridad cuando la autoprotección esté activada.
- Protección de carpetas de red asignadas como dispositivos locales
- Detección de malware de criptominado

Virtualización

- Conversión a los siguientes tipos de equipos virtuales:
  - VMware Workstation
  - Unidades de disco virtuales VHDX (para conectarse a un equipo virtual Hyper-V)

  Esta conversión se admite en un plan de copias de seguridad (pág. 119) o en un plan de conversión independiente (pág. 209) creado en la pestaña **Planes**.
- Compatibilidad de Windows Server 2019 con Hyper-V y Microsoft Hyper-V Server 2019 (pág. 27)
- Compatibilidad con Citrix XenServer 7.6 (pág. 27)
- El menú de arranque (en forma de texto) se puede usar al iniciar un equipo virtual Citrix XenServer.

Ubicaciones de las copias de seguridad

El nombre de producto "Acronis Storage" ha cambiado a Acronis Cyber Infrastructure (pág. 102).

Administración

- Se puede añadir un comentario a un dispositivo en el panel **Detalles** del dispositivo. Los dispositivos se pueden buscar y organizar en grupos dinámicos por comentarios (pág. 298).
- En un entorno de dominio, las cuentas locales del servidor de gestión no se añaden de forma predeterminada al grupo Acronis Centralized Admins ni a la lista de administradores de la organización.

Compatibilidad con nuevos sistemas operativos

- Compatibilidad con RHEL 7.6, 8.0 (no se admiten configuraciones con Stratis).
- Compatibilidad con Ubuntu 18.10.
- Compatibilidad con Fedora 25, 26, 27, 28 y 29.
- Compatibilidad con Debian 9.5 y 9.6.
- Se reanuda la compatibilidad con Agente para Windows XP SP1 (x64) y SP2 (x64).
- Se reanuda la compatibilidad con Windows XP SP2 (x86) gracias a una versión especial del Agente para Windows (pág. 25).

1.2 Novedades en la actualización 3.2

Copia de seguridad

La capacidad de detener la ejecución de un plan de copias de seguridad desde la pestaña Planes (pág. 204).

Compatibilidad con nuevos sistemas operativos

- Compatibilidad con Windows Server 2019
- Compatibilidad con CentOS 7.5
- Compatibilidad con ClearOS 7.4
- Compatibilidad con macOS Mojave 10.14

Virtualización

- Compatibilidad con Citrix XenServer 7.3, 7.4, 7.5 (pág. 27)
- Compatibilidad con Nutanix AHV (pág. 27)

1.3 Novedades en la actualización 3.1

- El número máximo de equipos físicos que se pueden registrar en un servidor de gestión ha aumentado de 2000 a 4000 (pág. 35).
- Puede limitar el número total de equipos virtuales que el agente para VMware o el agente para Hyper-V puede incluir en la copia de seguridad al mismo tiempo mediante el registro o el archivo de configuración del agente (pág. 290). A diferencia del parámetro similar en las opciones de planes de copias de seguridad, este parámetro limita el número total de equipos virtuales para todos los planes de copias de seguridad que el agente ejecute al mismo tiempo.

1.4 Novedades en la actualización 3

Nuevas características disponibles en todas las implementaciones en una instalación

Copia de seguridad

- La opción de copia de seguridad **Instantánea multivolumen** (pág. 140) está disponible al realizar copias de seguridad de Linux.
- La velocidad de salida de datos (pág. 140) se puede especificar como porcentaje, además de los kilobytes por segundo.
- La opción de copia de seguridad "Seguridad de nivel de archivo" ya no está disponible. Los permisos NTFS de los archivos siempre se guardan en copias de seguridad a nivel de archivo.
- Resolución automática de problemas relacionados con VSS:
  - Al realizar copias de seguridad de discos o volúmenes con Agente para Windows

    Cuando la toma de una instantánea basada en VSS falla, antes de volver a intentarlo, Acronis Backup analiza el registro y lleva a cabo pasos de resolución de problemas, si procede. Si fallan tres reintentos seguidos, el mensaje de error recomienda descargar y utilizar Acronis VSS Doctor.
  - Al realizar copias de seguridad de bases de datos de Microsoft SQL Server

    Antes de tomar una instantánea, Acronis Backup comprueba la configuración de SQL Server para detectar problemas que puedan provocar un fallo en la instantánea de VSS. Si se encuentran problemas, se añade al registro una advertencia con recomendaciones.

Recuperación

La nueva opción de recuperación **Modo de arranque** (pág. 174) determina el modo de arranque (BIOS o UEFI) del sistema Windows que se está recuperando.

Seguridad

La nueva configuración del sistema (pág. 331) está disponible para los administradores de la organización:

- Cierre de sesión de usuarios tras un periodo de inactividad configurable
- Mostrar una notificación sobre el último inicio de sesión del usuario actual
- Advertir sobre la caducidad de la contraseña local o de dominio

Aplicaciones

A partir de Microsoft Exchange 2010, se pueden hacer copias de seguridad de los datos del servidor de Exchange y recuperarlos mediante el uso de una cuenta con menos privilegios que un miembro del grupo de roles **Gestión de la organización**:

- Para las bases de datos (pág. 241), la pertenencia al grupo de funciones **Administración de servidores** es suficiente.
- Para los buzones de correo (pág. 248), la pertenencia al grupo de roles **Gestión de destinatarios** y el rol **ApplicationImpersonation** habilitado son suficientes.

Virtualización

- Compatibilidad con VMware vSphere 6.7 (la copia de seguridad de configuración de ESXi no es compatible)
- Recuperación en el equipo virtual original a partir de una copia de seguridad que no contenga todos los discos de este equipo.

  Anteriormente, esta operación solo era posible mediante el uso de dispositivos de arranque. La consola de copia de seguridad permitía la recuperación solo si la distribución del disco del equipo coincidía exactamente con la de la copia de seguridad.

Dispositivo Acronis Backup

- El tiempo de espera de 15 segundos se elimina del menú de instalación del dispositivo Acronis Backup. El instalador espera a que el usuario revise y confirme la configuración.
- El kernel de CentOS se actualiza en el dispositivo Acronis Backup para abordar las amenazas Meltdown y Spectre.

Dispositivo de arranque

Existe la posibilidad de utilizar cualquier disposición de teclado compatible a la hora de trabajar con dispositivos de arranque. El conjunto de disposiciones se define en el parámetro de kernel LAYOUT.

Compatibilidad con nuevos sistemas operativos

- Kernel Linux versiones 4.12 - 4.15
- Red Hat Enterprise Linux 7.5
- Ubuntu 17.10, 18.04
- Debian 9.3, 9.4
- Oracle Linux 7.4, 7.5

Nuevas características disponibles solo con las licencias de Advanced

Copia de seguridad

Capacidad para configurar un plan de copias de seguridad para utilizar dispositivos y unidades de cintas específicos (pág. 150).

Aplicaciones

Copia de seguridad compatible con aplicaciones de equipos Linux que ejecuten Oracle Database.

Administración

Capacidad para crear grupos dinámicos correspondientes a las unidades organizativas de Active Directory (pág. 298).

1.5 Novedades en la actualización 2

Nuevas características disponibles en todas las implementaciones en una instalación

Administración

- La administración de cuentas de usuario está disponible en un servidor de gestión instalado en Linux (pág. 333)

Instalación e infraestructura

- Dispositivo Acronis Backup (pág. 44) para la implementación automática de Linux, el servidor de gestión, Agente para Linux y Agente para VMware (Linux) en un equipo virtual exclusivo
- Si añade un equipo Windows en la interfaz web, puede seleccionar el nombre o dirección IP que el agente utilizará para acceder al servidor de gestión (pág. 46)
- Búsqueda automática y manual de actualizaciones (pág. 63)

Seguridad

- La consola de copias de seguridad permite el protocolo HTTPS listo para su uso (pág. 77)
- El servidor de gestión puede utilizar un certificado emitido por una autoridad de certificación de confianza en lugar de un certificado autofirmado (pág. 84)
- Los usuarios que no sean raíz pueden añadirse como administradores a un servidor de gestión instalado en Linux (pág. 335)

Planificaciones de las copias de seguridad

- Nuevas opciones de planificación (pág. 103):
  - Activación de un equipo para realizar su copia de seguridad desde el modo de suspensión o hibernación
  - Bloqueo del modo de suspensión o hibernación durante una copia de seguridad
  - Opción de prohibir la ejecución de copias de seguridad omitidas al iniciar el equipo
- Nuevas condiciones de inicio de las copias de seguridad, útiles para realizar copias de seguridad de portátiles y tabletas Windows
  - Ahorrar batería (pág. 110)
  - No iniciar con conexiones de uso medido (pág. 111)
  - No iniciar con conexiones a las siguientes redes Wi-Fi (pág. 112)
  - Comprobar dirección IP del dispositivo (pág. 112)
- En la planificación **Mensual**, selección de los meses individuales en los que ejecutar las copias de seguridad
- Capacidad de iniciar una copia de seguridad diferencial manualmente (pág. 122)

Ubicaciones de las copias de seguridad

- Almacenamiento de las copias de seguridad de cada equipo en una carpeta definida mediante un script (para equipos Windows) (pág. 97)
- Puede usarse una implementación local de Acronis Storage como ubicación de copia de seguridad (pág. 97)

Aplicaciones

- Recuperación de elementos de buzones de correo y buzones de correo de Microsoft Office 365 a Microsoft Exchange Server y viceversa (pág. 261)

Compatibilidad con nuevos sistemas operativos y plataformas de virtualización

- macOS High Sierra 10.13
- Debian 9.1 y 9.2
- Red Hat Enterprise Linux 7.4
- CentOS 7.4
- ALT Linux 7.0
- Red Hat Virtualization 4.1

Mejoras de la usabilidad

- Cambio de nombre de ubicaciones en la pestaña **Copias de seguridad**
- La capacidad de cambiar el vCenter Server o servidor ESXi gestionado por Agente para VMware en **Configuración** > **Agentes** > detalles del agente.

Nuevas características disponibles solo con las licencias de Advanced

Administración

- La creación de unidades está disponible en un servidor de gestión instalado en Linux (pág. 333)

Instalación e infraestructura

- Al añadir una ubicación gestionada, puede determinarse si los agentes accederán al nodo de almacenamiento mediante el nombre de servidor o dirección IP (pág. 322)

Mejoras de la usabilidad

- La adición de una ubicación gestionada puede iniciarse desde el panel de propiedades del nodo de almacenamiento (pág. 322)

Soporte de cintas

- Compatibilidad completa con la tecnología LTO-8. Consulte la lista de compatibilidad de hardware para ver los nombres exactos los dispositivos probados.

1.6 Novedades en la actualización 1

- Compatibilidad con Citrix XenServer 7.0, 7.1, 7.2 y Red Hat Virtualization 4.1 (pág. 27)
- Compatibilidad con Debian 8.6, 8.7, 8.8, 9 y Ubuntu 17.04
- Compatibilidad con Windows Storage Server 2016
- La capacidad de usar una base de datos PostgreSQL con el servidor de gestión en Linux (pág. 43)
- Una herramienta para la implementación y actualización masiva de agentes.

  Para obtener más información sobre cómo usar esta herramienta, consulte http://kb.acronis.com/content/60137.

1.7 Novedades en Acronis Backup 12.5

Nuevas características disponibles en todas las implementaciones en una instalación

Copia de seguridad

- Un nuevo formato de copia de seguridad (pág. 130) que incrementa la velocidad de copia de seguridad y reduce el tamaño de las copias de seguridad
- Hasta cinco ubicaciones para la replicación en un plan de copias de seguridad (pág. 120)

- Conversión a un equipo virtual en un plan de copias de seguridad (pág. 117)
- Planificación por eventos (pág. 105)
- Establecer condiciones para la ejecución de un plan de copias de seguridad (pág. 107)
- Esquema de copias de seguridad del tipo "abuelo-padre-hijo" (GFS) (pág. 103)
- SFTP como ubicación de la copia de seguridad (pág. 97)
- Opciones de copia de seguridad predeterminadas almacenadas en el servidor de gestión (pág. 332)
- Selección del método de copia de seguridad (completa o incremental) al iniciar una copia de seguridad manualmente (pág. 122)
- Opciones de copia de seguridad:
  - Notificaciones por correo electrónico (pág. 134):
    - Especificar el asunto de las notificaciones por correo electrónico
    - Las notificaciones se basan ahora en alertas en lugar de resultados de actividad de copia de seguridad. Puede personalizar la lista de las alertas que desencadenan una notificación.
  - Nombre del archivo de la copia de seguridad (pág. 127)
  - Condiciones de inicio de la copia de seguridad (pág. 131)

Recuperación

- Asignación manual de discos. Capacidad de recuperar discos o volúmenes individuales (pág. 157).

Dispositivo de arranque

- Startup Recovery Manager (pág. 230)

Aplicaciones

- Copia de seguridad de buzones de correo de Microsoft Exchange Server (pág. 247)

Virtualización

- Capacidad de asignar un equipo virtual a un agente concreto (pág. 283) (enlace de VM)

Operaciones con copias de seguridad

- Montar volúmenes en el modo de lectura/escritura (pág. 200)
- ASign permite la firma de un archivo en la copia de seguridad por diferentes personas (pág. 168)

Notificaciones y alertas

- Capacidad de configurar la gravedad de una alerta (a través del archivo de configuración) (pág. 295)
- El estado del dispositivo se deriva ahora de las alertas en lugar de los resultados de la actividad de copia de seguridad. Esto cubre una mayor variedad de eventos, por ejemplo, copias de seguridad omitidas o actividades de ransomware.

Acronis Active Protection

- Protección proactiva del ransomware detectando procesos sospechosos (pág. 264)

Mejoras de la usabilidad

- Panel de control: un conjunto personalizable de más de 20 widgets que se actualizan en tiempo real (pág. 292)
- Una nueva sección de la IU muestra todos los planes de copias de seguridad y otros planes (pág. 204)

- Capacidad de definir una contraseña de cifrado en Backup Monitor (pág. 114)

Nuevas características disponibles solo con las licencias de Advanced

Administración

- Se pueden enviar o guardar informes personalizables siguiendo una planificación (pág. 293)
- Roles en el servidor de gestión: crear unidades y asignarles administradores (pág. 333)
- Gestión de grupos: grupos de dispositivos integrados y personalizados (pág. 296)
- Acronis Notary: demostrar que un archivo es auténtico y no ha cambiado desde que se realizó su copia de seguridad (pág. 116)

Nuevas ubicaciones de copia de seguridad

- Acronis Storage Node con deduplicación (pág. 321)
- Compatibilidad con dispositivos de cintas (pág. 303)

Dispositivo de arranque

- Trabajo con dispositivos de arranque a través de la consola de copia de seguridad (pág. 228)
- Copia de seguridad y recuperación automatizadas mediante la ejecución de un script predefinido o personalizado (pág. 215)
- PXE Server para arranque de red (pág. 232)

Aplicaciones

- Compatibilidad con grupos de disponibilidad de base de datos (DAG) en Microsoft Exchange Server (pág. 244)
- Compatibilidad con grupo de disponibilidad AlwaysOn (AGG) en Microsoft SQL Server (pág. 242)
- Protección de Oracle Database (pág. 264)

Virtualización

- Copia de seguridad de equipos virtuales ESXi desde instantáneas de hardware NetApp (pág. 278)
- Copia de seguridad de equipos virtuales Citrix XenServer, Red Hat Virtualization (RHV/RHEV), equipos virtuales basados en Kernel (KVM) y Oracle (instalando un agente en el sistema invitado) (pág. 18)

Operaciones con copias de seguridad

- La conversión a un equipo virtual, la validación, replicación y retención de copias de seguridad se pueden realizar siguiendo una planificación por un agente dedicado (pág. 205)
- Catalogación: un servicio de catálogo independiente habilita la búsqueda en todas las copias de seguridad de las ubicaciones gestionadas (pág. 327)

2 Instalación

2.1 Información general acerca de la instalación

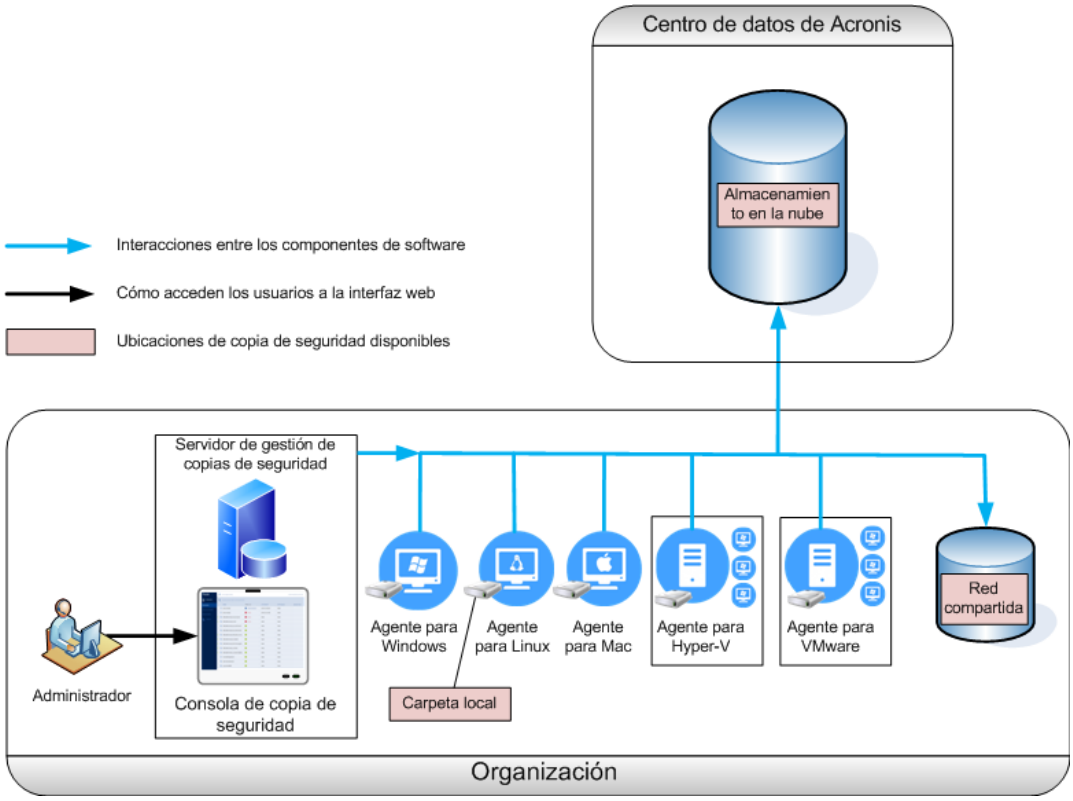
Acronis Backup admite dos métodos de implementación: en una instalación y en la nube. La diferencia principal entre ellos es la ubicación de Acronis Backup Management Server.

Acronis Backup Management Server es el punto central para gestionar todas las copias de seguridad. Con la implementación en una instalación, 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 de copia de seguridad.

Ambos tipos de implementación requieren la instalación de un agente de copias de seguridad 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 Backup.

Implementación en una instalación

La implementación en una instalación 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 las copias de seguridad 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.

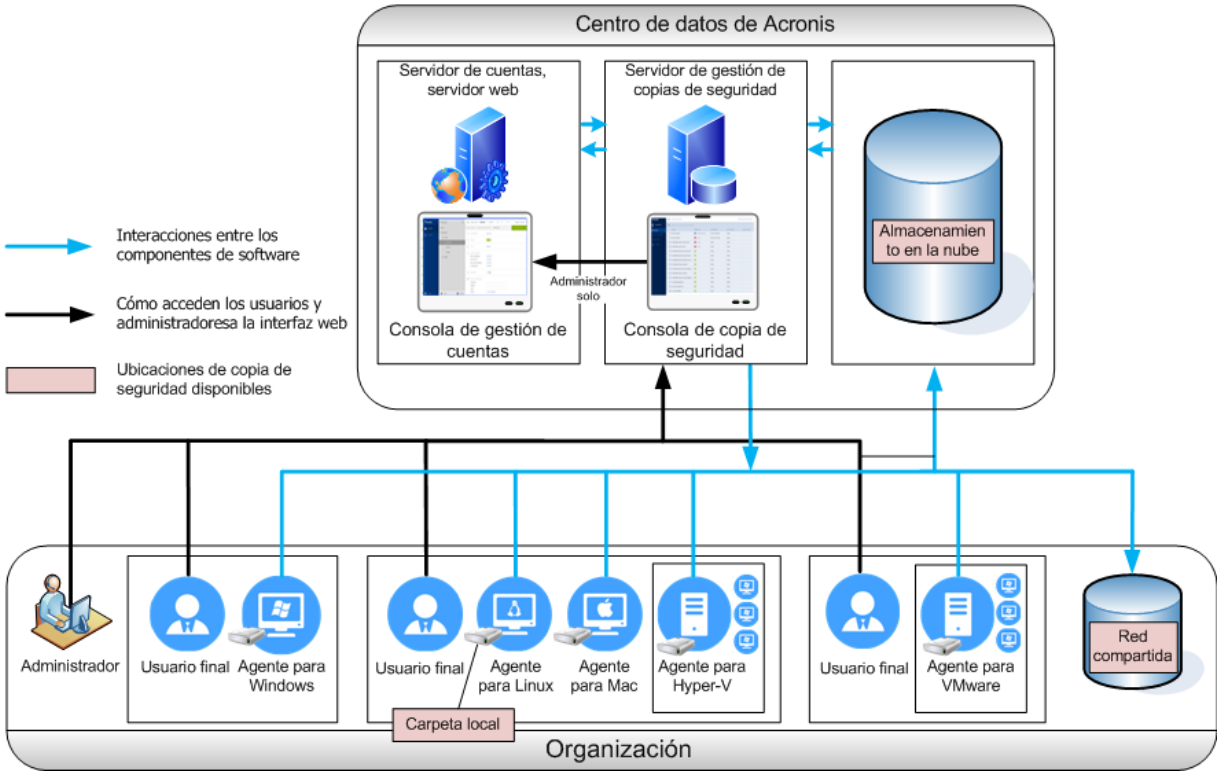
Implementación en la nube

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 Backup un servicio de copias de seguridad 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 de copia de seguridad, 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.



La tabla siguiente resume las diferencias entre las implementaciones en una instalación y en la nube.

Implementación en una instalación	Implementación en la nube
▪ Servidor de gestión en una instalación ▪ Gestión de unidades y cuentas solo con la licencia de Advanced ▪ Se pueden utilizar tanto la licencia de suscripción como la licencia perpetua ▪ Bootable Media Builder ▪ Gestión del disco y de copias de seguridad en dispositivos de arranque ▪ Actualización desde versiones anteriores de Acronis Backup, incluido Acronis Backup para VMware ▪ Participación en el Programa de experiencia del cliente de Acronis ▪ Funciones introducidas en la versión 12.5, que afectan solo a las implementaciones en una instalación. Consulte "Novedades en Acronis Backup" (pág. 8).	▪ Gestión de unidades y cuentas ▪ Se necesita una licencia de suscripción ▪ Recuperación ante desastres como servicio en el cloud

2.2 Componentes

Agentes

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

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.

Tenga en cuenta que 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.

¿Qué se va a incluir en las copias de seguridad?	¿Qué agente se debe instalar?	¿Dónde se debe realizar la instalación?	Disponibilidad del agente	
			Local	Cloud

¿Qué se va a incluir en las copias de seguridad?	¿Qué agente se debe instalar?	¿Dónde se debe realizar la instalación?	Disponibilidad del agente	
			Local	Cloud
Equipos físicos				
Discos, volúmenes y archivos en equipos físicos que ejecutan Windows.	Agente para Windows	En el equipo que se 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	Agent for 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 Office 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 Oracle Database	Agent for Oracle	En el equipo que 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 alojados en Windows Azure.	Los mismo ocurre con los equipos físicos**	En el equipo que se incluirá en la copia de seguridad.	+	+

¿Qué se va a incluir en las copias de seguridad?	¿Qué agente se debe instalar?	¿Dónde se debe realizar la instalación?	Disponibilidad del agente	
			Local	Cloud
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 ejecutan Android.	Aplicación para dispositivos móviles de Android	En el dispositivo móvil que se incluirá en la copia de seguridad.	–	+
Dispositivos móviles que ejecutan iOS	Aplicación para dispositivos móviles de iOS		–	+

*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" (pág. 276).

**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 nube.

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

Otros componentes

Componente	Función	¿Dónde se debe realizar la instalación?	Disponibilidad	
			Local	Cloud

Componente	Función	¿Dónde se debe realizar la instalación?	Disponibilidad	
			Local	Cloud
Servidor de gestión	Gestiona los agentes. 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.	+	–
Servicio de monitorización	Proporciona el panel de control y la función de generación de informes.	En el equipo 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	Proporciona la interfaz de línea de comandos.	En un equipo que ejecuta Windows o Linux.	+	+
Monitorización de copias de seguridad	Permite a los usuarios monitorizar copias de seguridad fuera de la interfaz web.	En un equipo que ejecuta Windows o macOS.	+	+
Nodo de almacenamiento	Almacena copias de seguridad. Es necesario para la catalogación y la deduplicación.	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.	+	–

2.3 Requerimientos de software

2.3.1 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
- Windows Internet Explorer 10 o posterior

  En las implementaciones de la nube, el portal de gestión (pág. 336) es compatible con Internet Explorer 11 o posteriores.
- Microsoft Edge 25 o posterior
- Safari 8 o una versión posterior que se ejecute en los sistemas operativos macOS y iOS

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

2.3.2 Sistemas operativos y entornos compatibles

2.3.2.1 Agentes

Agente para Windows

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

Windows XP Professional SP2 (x86): compatible con una versión especial de Agente para Windows. Consulte Compatibilidad con Windows XP SP2 (pág. 25) para conocer los detalles y las limitaciones de esta compatibilidad.

Windows Server 2003 SP1/2003 R2 y posterior – Standard y Enterprise editions (x86, x64)

Windows Small Business Server 2003/2003 R2

Windows Vista: todas las ediciones

Windows Server 2008: ediciones Standard, Enterprise, Datacenter 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 2003/2008/2008 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

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

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 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

Agente para Office 365

Windows Server 2008: Standard, Enterprise, Datacenter y Web Edition (solo x64)

Windows Small Business Server 2008

Windows Server 2008 R2: ediciones Standard, Enterprise, Datacenter, Foundation y Web

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

Agent for 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 (indicados a continuación)

Agente para Linux

Linux con la versión de kernel 2.6.9 a 4.19.8 y glibc 2.3.4 o versiones posteriores

Varias distribuciones de Linux x86 y x86_64, incluidas:

- Red Hat Enterprise Linux 4.x, 5.x, 6.x, 7.0, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6 y 8.0 (no se admiten configuraciones con Stratis)
- 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 y 18.10
- Fedora 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28 y 29
- SUSE Linux Enterprise Server 10 y 11
- SUSE Linux Enterprise Server 12: compatible con los sistemas de archivos excepto Btrfs
- Debian 4, 5, 6, 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 y 9.6
- CentOS 5.x, 6.x, 7, 7.1, 7.2, 7.3, 7.4, 7.5 y 7.6
- Oracle Linux 5.x, 6.x, 7.0, 7.1, 7.2, 7.3, 7.4, 7.5 y 7.6: tanto Unbreakable Enterprise Kernel como Red Hat Compatible Kernel
- CloudLinux 5.x, 6.x, 7, 7.1, 7.2, 7.3, 7.4 y 7.5
- ClearOS 5.x, 6.x, 7, 7.1 y 7.4
- 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`**

Agente para Mac

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

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

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.

Agent for Hyper-V

Windows Server 2008 (solo 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 (solo x64) con Hyper-V

Windows 10: ediciones Pro, Education y Enterprise 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

2.3.2.2 Servidor de gestión (solo para implementación en una instalación)

En Windows

Windows Server 2008: ediciones Standard, Enterprise y Datacenter (x86, x64)

Windows Small Business Server 2008

Windows 7: todas las ediciones (x86, x64)

Windows Server 2008 R2: ediciones Standard, Enterprise, Datacenter y Foundation

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 R2/2016

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

En Linux

Linux con la versión de kernel 2.6.23 a 4.19.8 y glibc 2.3.4 o versiones posteriores

Varias distribuciones Linux x86_64, incluyendo:

- Red Hat Enterprise Linux 6.x, 7.0, 7.1, 7.2, 7.3, 7.4, 7.5 y 7.6
- 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 y 18.10
- Fedora 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28 y 29
- SUSE Linux Enterprise Server 11, 12
- Debian 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 y 9.6
- CentOS 6.x, 7, 7.1, 7.2, 7.3, 7.4, 7.5 y 7.6
- Oracle Linux 6.x, 7.0, 7.1, 7.2, 7.3, 7.4, 7.5 y 7.6: tanto Unbreakable Enterprise Kernel como Red Hat Compatible Kernel
- CloudLinux 6.x, 7, 7.1, 7.2, 7.3, 7.4, 7.5
- ALT Linux 7.0

2.3.2.3 Nodo de almacenamiento (solo para implementación en una instalación)

Windows Server 2008: ediciones Standard, Enterprise y Datacenter (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 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 y Enterprise

Windows Server 2016: todas las opciones de instalación, excepto Nano Server

2.3.2.4 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.

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 la monitorización de copias de seguridad 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 (pág. 105).
- No se admiten las condiciones para la ejecución de un plan de copias de seguridad (pág. 107).
- Únicamente se admiten los siguientes destinos de copias de seguridad:
  - Almacenamiento en el 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 (pág. 143). La opción **Ventana de copia de seguridad y rendimiento** (pág. 140), 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 (pág. 205).
- 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 (pág. 119)
  - Montaje de volúmenes desde una copia de seguridad (pág. 200)
  - Extracción de archivos desde copias de seguridad locales (pág. 170)
  - Exportación (pág. 202) 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 (pág. 267).

2.3.3 Versiones compatibles de Microsoft SQL Server

- Microsoft SQL Server 2017
- Microsoft SQL Server 2016
- Microsoft SQL Server 2014
- Microsoft SQL Server 2012
- Microsoft SQL Server 2008 R2

- Microsoft SQL Server 2008
- Microsoft SQL Server 2005

2.3.4 Versiones admitidas 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.

2.3.5 Versiones de Microsoft SharePoint compatibles

Acronis Backup 12.5 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.

2.3.6 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.

2.3.7 Plataformas de virtualización compatibles

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

Plataforma	Copia de seguridad a nivel de hipervisor (sin agente)	Copia de seguridad desde dentro de un SO huésped
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 **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		+
Microsoft		

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	+	+
Microsoft Virtual PC 2004 y 2007 Windows Virtual PC		+
Microsoft Virtual Server 2005		+
Citrix		
Citrix XenServer 4.1.5, 5.5, 5.6, 6.0, 6.1, 6.2, 6.5, 7.0, 7.1, 7.2, 7.3, 7.4, 7.5 y 7.6		Sólo invitados completamente virtualizados (también denominados HVM)
Red Hat y Linux		
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		+
Equipos virtuales basados en Kernel (KVM)		+
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		
Oracle VM Server 3.0, 3.3 y 3.4		Sólo invitados completamente virtualizados (también denominados HVM)
Oracle VM VirtualBox 4.x		+
Nutanix		
Nutanix Acropolis Hypervisor (AHV) 20160925.x mediante 20180425.x		+
Amazon		
Instancias de Amazon EC2		+
Microsoft Azure		
Equipos virtuales de Azure		+

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

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

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 copias de seguridad. 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.

- **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 copias de seguridad. 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 VMware y Agente para Hyper-V no realizan copias de seguridad de volúmenes de LUN conectados mediante un iniciador iSCSI que funciona en el sistema operativo huésped. Como los hipervisores Hyper-V y ESXi no son compatibles 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 Linux que contienen volúmenes lógicos (LVM)**

  Agente para VMware y Agente para Hyper-V no admiten las operaciones siguientes para equipos Linux con volúmenes lógicos:

  - Migración P2V y V2P. Use Agente para Linux o un dispositivo de arranque para crear la copia de seguridad y el dispositivo de arranque para la recuperación.
  - Ejecución de un equipo virtual desde una copia de seguridad creada por Agente para Linux o un dispositivo de arranque.
  - Conversión de una copia de seguridad creada por Agente para Linux o un dispositivo de arranque en un equipo virtual.

- **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 imprescindible para usted, habilite las copias de seguridad al crear un plan de copias de seguridad (pág. 114).
  - 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)

  Arranque seguro está deshabilitado cuando un equipo virtual se ha recuperado como nuevo equipo virtual. Puede habilitar el cifrado manualmente una vez se haya completado la recuperación.

- La **copia de seguridad de configuración de ESXi** no es compatible con VMware vSphere 6.7.

2.3.8 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 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 intérprete Perl.

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

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

¿Los paquetes requeridos ya están instalados?

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

1. Ejecute el siguiente comando para encontrar la versión de kernel y la versión GCC requerida:
   ```
   cat /proc/version
   ```
   Este comando devuelve líneas similares a las siguientes: **`Linux version 2.6.35.6`** y **`gcc version 4.5.1`**
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`** en el 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`** en el paso 1.
4. Ejecute el siguiente comando para comprobar si el intérprete Perl está instalado:
   ```
   perl --version
   ```
   Si observa la información sobre la versión de Perl, el intérprete está instalado.

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**	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**	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.

2.3.9 Compatibilidad con software de cifrado

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

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

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

- Microsoft BitLocker Drive Encryption
- McAfee Endpoint Encryption
- PGP Whole Disk Encryption.

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

Regla común de instalación

Es altamente recomendable instalar el software de cifrado antes de instalar los agentes de copias de seguridad.

Cómo utilizar Secure Zone

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

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

Regla común de copia de seguridad

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

Procedimientos de recuperación específicos del software

Microsoft BitLocker Drive Encryption

Para recuperar un sistema cifrado con BitLocker:

1. Inicie desde el dispositivo de arranque.
2. Recupere el sistema. Los datos recuperados no estarán cifrados.
3. Reinicie el sistema recuperado.
4. Encienda BitLocker.

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

McAfee Endpoint Encryption y PGP Whole Disk Encryption

Puede recuperar una partición de sistema cifrada solo al utilizar un dispositivo de arranque.

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

2.4 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 ocupado	Consumo de memoria mínimo
Agente para Windows	850 MB	150 MB
Agente para Windows y uno de los agentes siguientes: ▪ Agente para SQL ▪ Agent for 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	720 MB	130 MB
Agente para Mac	500 MB	150 MB
Solo para implementaciones en una instalación		
Servidor de gestión en Windows	1,7 GB	200 MB
Servidor de gestión en Linux	0,6 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	1,2 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 la sección "Mejores prácticas de deduplicación" (pág. 324).	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.

Un dispositivo de arranque o una recuperación de disco con reinicio requiere al menos 1 GB de memoria.

Un servidor de gestión con un equipo registrado consume 200 MB de memoria. Cada uno de los equipos recientemente registrados contribuye con unos 2 MB al consumo. Por tanto, un servidor con 100 equipos registrados consume aproximadamente 400 MB aparte del sistema operativo y las aplicaciones en funcionamiento. El número máximo de equipos registrado está entre 900 y 1000. Esta limitación procede del SQLite integrado del servidor de gestión.

Puede superar esta limitación especificando una instancia de Microsoft SQL Server externa durante la instalación del servidor de gestión. Con una base de datos SQL externa, se pueden registrar hasta 8000 equipos sin que eso suponga una degradación significativa del rendimiento. Así, el servidor SQL consumirá unos 8 GB de RAM. Para disfrutar de un mayor rendimiento de copia de seguridad, le recomendamos gestionar los equipos por grupos, formados por 100 equipos en cada uno, aproximadamente.

2.5 Sistemas de archivos compatibles

Un agente de copia de seguridad 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	

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 la copia de seguridad del disco.
ReiserFS3		-	+	-	
ReiserFS4		-	+	-	▪ Los archivos no se pueden excluir de la copia de seguridad del disco. ▪ No se puede cambiar el tamaño de los volúmenes durante la recuperación
ReFS	Todos los agentes	+	+	+	
XFS		+	+	+	
Linux swap	Agente para Linux	-	+	-	Sin limitaciones

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

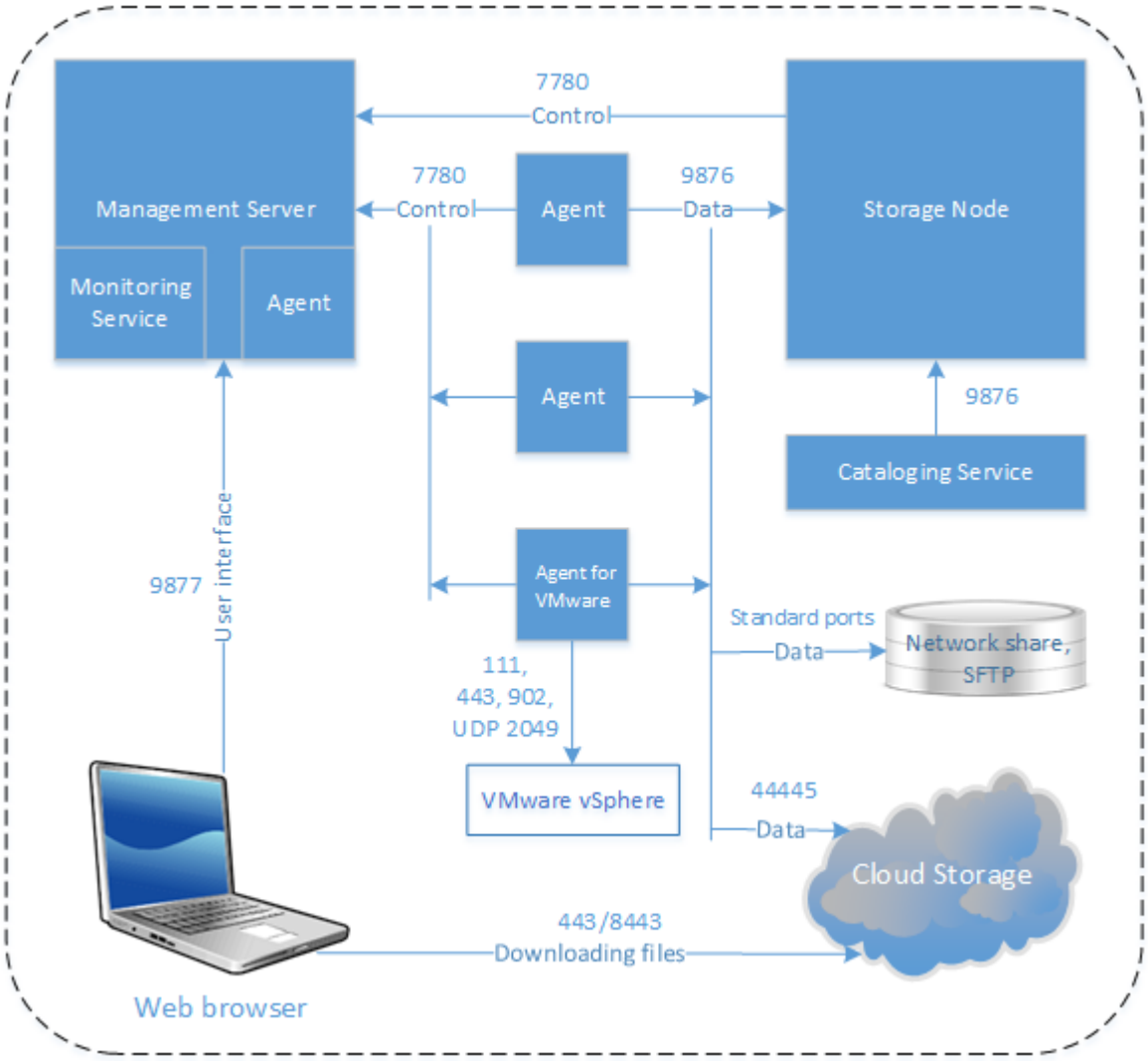
El software cambia automáticamente al modo sector por sector al hacer copias de seguridad de unidades con sistemas de archivos no reconocidos o incompatibles. Es posible realizar una copia de seguridad sector por sector para cualquier sistema de archivos que:

- 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.

2.6 Implementación en una instalación

Una implementación local incluye varios componentes de software, descritos en la sección Componentes (pág. 18). El diagrama siguiente muestra la interacción de componentes y los puertos requeridos para esta interacción. El sentido de la flecha muestra qué componente inicia una conexión.



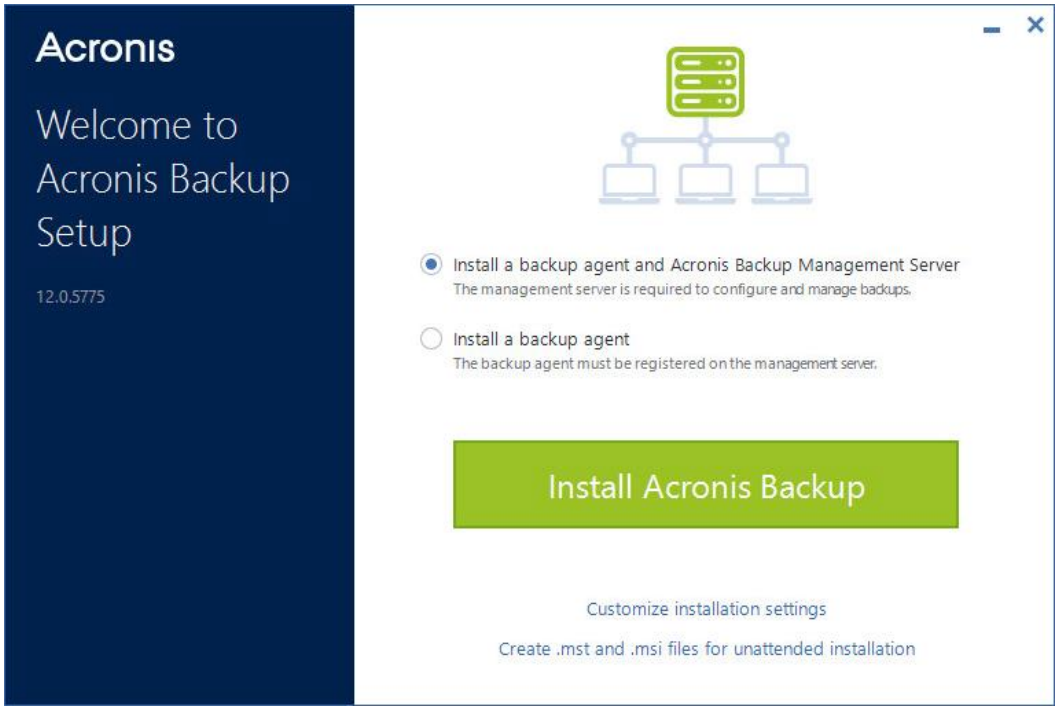
2.6.1 Instalación del servidor de gestión

2.6.1.1 Instalación en Windows

Para instalar el servidor de gestión

1. Inicie sesión como administrador e inicie el programa de instalación de Acronis Backup.
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 seleccione si el equipo participará en el Programa de experiencia del cliente (PEC) de Acronis.

4. Mantenga la configuración predeterminada **Instalar un agente de copias de seguridad y Acronis Backup Management Server**.



5. Realice una de las siguientes operaciones:
   - Haga clic en **Instalar Acronis Backup**.

     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
     - Servicio de monitorización
     - 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
     - Monitorización de copias de seguridad
   - 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" (pág. 42).
   - 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" (pág. 73).
6. Continúe con la instalación.
7. Cuando haya terminado la instalación, haga clic en **Cerrar**.

Personalización de los ajustes de instalación

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

Configuraciones comunes

- Los componentes que se instalarán.
- La carpeta donde se instalará el producto.
- Las cuentas con las que se ejecutarán los servicios.

  Puede escoger una de las siguientes acciones:

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

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

    Los nombres de cuenta serán **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.

    Asimismo, elija esta opción si desea que el servidor de gestión utilice un servidor de Microsoft SQL existente instalado en otro equipo y use Autenticación de Windows para SQL Server.

  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.

Instalación del servidor de gestión

- La base de datos que debe utilizar el servidor de gestión. De manera predeterminada, se utiliza la base de datos SQLite incorporada.

  Puede seleccionar cualquier edición de las siguientes versiones de Microsoft SQL Server:

  - Microsoft SQL Server 2012
  - Microsoft SQL Server 2014
  - Microsoft SQL Server 2016
  - Microsoft SQL Server 2017 (ejecutada en Windows)

  La instancia que escoja se puede usar también en otros programas.

  Antes de seleccionar una instancia instalada en otro equipo, asegúrese de que SQL Server Browser Service y el protocolo TCP/IP estén habilitados en el equipo. Para obtener instrucciones 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.

- 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 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.

Instalación del agente

- Determina si el agente se conectará a Internet mediante un servidor proxy HTTP cuando se realizan copias de seguridad a un almacenamiento en la cloud o una recuperación desde este almacenamiento.

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

2.6.1.2 Instalación en Linux

Preparación

1. 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`**.
2. Si desea instalar Agente para Linux junto con el servidor de gestión, asegúrese de que los paquetes de Linux (pág. 31) necesarios se han instalado en el equipo.
3. Seleccione la base de datos que debe utilizar el servidor de gestión.

   De manera predeterminada, se utiliza la base de datos SQLite incorporada. Como alternativa, puede utilizar PostgreSQL. Para obtener información sobre cómo configurar el servidor de gestión para usar PostgreSQL, consultehttp://kb.acronis.com/content/60395.

   Nota *Si cambia a PostgreSQL después de que el servidor de gestión haya estado funcionando durante algún tiempo, deberá añadir dispositivos y configurar planes de copias de seguridad y otros ajustes desde cero.*

Instalación

Para instalar el servidor de gestión

1. Ejecute el archivo de instalación como usuario raíz.
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 de copia de seguridad se abrirá en el navegador web predeterminado.

2.6.1.3 Dispositivo Acronis Backup

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

- CentOS
- Componentes de Acronis Backup:
  - 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`** es **`true`**.

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 Backup** 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-`**`<parte aleatoria>`).
   - La contraseña de la cuenta raíz que se utilizará para iniciar sesión en la consola de copias de seguridad (de forma predeterminada, **no especificado**).

     Si mantiene el valor predeterminado, se le pedirá que especifique la contraseña una vez instalado Acronis Backup. Sin la contraseña, no podrá iniciar sesión en la consola de copias de seguridad 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 Backup se instalarán en el equipo.

Otras acciones

Una vez finalizada la instalación, el software muestra los enlaces a la consola de copias de seguridad y a la consola web Cockpit. Conéctese a la consola de copias de seguridad para empezar a utilizar Acronis Backup (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 Backup 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 Backup** 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 Backup. 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 Backup.

2.6.2 Adición de equipos a través de la interfaz web

Para empezar a añadir un equipo al servidor de gestión, haga clic en **Todos los dispositivos** > **Añadir**.

Si el servidor de gestión se instala en Linux, se le pedirá que seleccione el programa de instalación según el tipo de equipo que desea añadir. Una vez que el programa de instalación se haya descargado, ejecútelo localmente en ese equipo.

Las operaciones que se describen al final de esta sección serán posibles si el servidor de gestión se ha instalado en Windows. En la mayoría de los casos, el agente se implementará de forma silenciosa en el equipo seleccionado.

2.6.2.1 Adición de un equipo que ejecute Windows

Preparación

1. Para que la instalación se realice correctamente en un equipo remoto que ejecuta Windows XP, la opción **Panel de control > Opciones de carpeta > Ver > Utilizar uso compartido simple de archivos** se debe *desactivar* en ese equipo.

   Para que la instalación se realice correctamente en un equipo remoto que ejecuta Windows Vista o posterior, la opción **Panel de control > Opciones de carpeta > Ver > Uso del asistente para compartir** se debe *desactivar* en ese equipo.
2. 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* (pág. 47).
3. El uso compartido de archivos e impresoras deben estar *habilitado* en el equipo remoto. Para acceder a esta opción:
   - En un equipo con Windows XP o Windows 2003 Server: vaya a **Panel de control > Firewall de Windows > Excepciones > Uso compartido de archivos e impresoras**.
   - En un equipo con Windows Vista, Windows Server 2008, Windows 7 o posterior: vaya a **Panel de control > Cortafuegos de Windows > Centro de redes y uso compartido > Cambiar las configuraciones avanzadas de uso compartido**.
4. Acronis Backup utiliza los puertos TCP 445, 25001 y 43234 la para 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.

Paquetes de instalación

Los agentes se instalan desde paquetes de instalación. El servidor de gestión toma los paquetes de la carpeta local especificada en la siguiente clave de registro: **HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\RemoteInstallationFiles**<número de compilación del producto>. La ubicación predeterminada es **%ProgramFiles%\Acronis\RemoteInstallationFiles**<número de compilación del producto>.

Deberá descargar los paquetes de instalación en las siguientes situaciones:

- Los componentes para la instalación remota no se instalaron durante la instalación del servidor de gestión.
- Los paquetes de instalación se han eliminado manualmente de la ubicación especificada en la clave de registro.
- Debe añadir un equipo de 32 bits al servidor de gestión de 64 bits o viceversa.
- Debe actualizar agentes en un equipo de 32 bits desde el servidor de gestión de 64 bits o viceversa mediante la pestaña **Agentes**.

Para obtener los paquetes de instalación

1. En la consola de copias de seguridad, haga clic en el icono de la cuenta en la esquina superior derecha y seleccione **Descargas**.

2. Seleccione **Programa de instalación fuera de línea para Windows**. Tenga en cuenta la versión apropiada (32 o 64 bits).
3. Guarde el programa de instalación en la ubicación de los paquetes.

Adición del equipo

1. Haga clic en **Todos los dispositivos** > **Añadir**.
2. Haga clic en **Windows** o en el botón que se corresponda con la aplicación que desea proteger. Dependiendo del botón en el que haga clic, se seleccionará una de las opciones siguientes:
   - Agente para Windows
   - 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, irá directamente al paso 5.
   - Agente para Active Directory + Agente para Windows
   - Agente para Office 365
3. Especifique el nombre del servidor o la dirección IP del equipo, y las credenciales de una cuenta con privilegios de administración en ese equipo.
4. 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 de registro del agente.
5. Haga clic en **Agregar**.
6. Si ha hecho clic en **Microsoft Exchange Server** > **Buzones de correo de Exchange** en el paso 2, 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 buzones de correo" (pág. 247).

Requisitos del control de cuentas de usuario (UAC)

En un equipo que ejecute Windows Vista o posterior y no sea miembro de un dominio de Active Directory, las operaciones de gestión centralizada (incluyendo la instalación remota) necesitan que UAC esté deshabilitado.

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.

2.6.2.2 Adición de un equipo que ejecute Linux

1. Haga clic en **Todos los dispositivos** > **Añadir**.
2. Haga clic en **Linux**. Se descargará el archivo de instalación.
3. En el equipo que desea proteger, ejecute el programa de instalación localmente (pág. 53).

2.6.2.3 Adición de un equipo que ejecute OS X

1. Haga clic en **Todos los dispositivos** > **Añadir**.
2. Haga clic en **Mac**. Se descargará el archivo de instalación.
3. En el equipo que desea proteger, ejecute el programa de instalación localmente (pág. 54).

2.6.2.4 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 Agent para VMware (dispositivo virtual) (pág. 48)

  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) (pág. 49)

  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" (pág. 276).

  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 (pág. 49)

  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 (pág. 50)

  Se trata de un paso necesario una vez que haya instalado manualmente el Agente para VMware (Windows) o implementado el dispositivo Acronis Backup (pág. 44). 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 (pág. 286) en el servidor vCenter Server o ESXi.
5. 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 de registro del agente.
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" (pág. 46).

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. Especifique el nombre del servidor o la dirección IP del equipo, y las credenciales de una cuenta con privilegios de administración en ese equipo.
5. 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 de registro del agente.
6. Haga clic en **Conectar**.
7. 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 (pág. 286) en el servidor vCenter Server o ESXi.
8. 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 (pág. 51).

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. 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.
5. 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 de registro del agente.
6. Haga clic en **Conectar**.
7. 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 (pág. 286) en el servidor vCenter Server o ESXi.
8. 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 (pág. 286) en el servidor vCenter Server o ESXi.

6. Haga clic en **Configurar** para guardar los cambios.

2.6.3 Instalación de agentes localmente

2.6.3.1 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 Backup.
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 seleccione si el equipo participará en el Programa de experiencia del cliente (PEC) de Acronis.
4. Seleccione **Instalar un agente de copias de seguridad**.
5. Realice una de las siguientes operaciones:
   - Haga clic en **Instalar Acronis Backup**.

     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
     - Monitorización de copias de seguridad
   - 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" (pág. 42).
   - 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" (pág. 73).
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. Puede usar las credenciales de sesión de Windows actuales o especificar explícitamente el nombre de usuario y la contraseña.

      Aunque no sea administrador del servidor de gestión, puede registrar el equipo si selecciona la opción **Conectar sin autenticación**. Esto funciona siempre que el servidor de gestión admita registrarse de forma anónima, opción que puede estar deshabilitada (pág. 332).

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 la sección "Administradores y unidades" (pág. 333).
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 de copias de seguridad, 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 buzones de correo" (pág. 247).

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 Backup.
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 seleccione si el equipo participará en el Programa de experiencia del cliente (PEC) de Acronis.
4. Seleccione **Instalar un agente de copias de seguridad** 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 Backup 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. Puede usar las credenciales de sesión de Windows actuales o especificar explícitamente el nombre de usuario y la contraseña.

      Aunque no sea administrador del servidor de gestión, puede registrar el equipo si selecciona la opción **Conectar sin autenticación**. Esto funciona siempre que el servidor de gestión admita registrarse de forma anónima, opción que puede estar deshabilitada (pág. 332).
   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 la sección "Administradores y unidades" (pág. 333).
9. [Opcional] Cambie otros ajustes de la instalación según se describe en "Personalización de los ajustes de instalación" (pág. 42).
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" (pág. 50).
13. [Solo al instalar Agent for Exchange] Abra la consola de copias de seguridad, 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 buzones de correo" (pág. 247).

2.6.3.2 Instalación en Linux

Preparación

1. 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`.
2. Asegúrese de que los paquetes de Linux (pág. 31) necesarios se han instalado en el equipo.

Instalación

Para instalar Agente para Linux

1. Como usuario raíz, ejecute el archivo de instalación apropiado (un archivo .i686 o un archivo .x86_64).
2. Acepte los términos del contrato de licencia.
3. Especifique los componentes que desee instalar:
   a. Desmarque la casilla de verificación **Acronis Backup Management Server**.
   b. Seleccione las casillas de verificación de los agentes que desea instalar. Los agentes disponibles son los siguientes:
      - **Agente para Linux**
      - **Agent for 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, o seleccione el registro anónimo.

      Especificar las credenciales es útil si su organización tiene unidades y desea añadir el equipo a la unidad gestionada por un administrador específico. Con el registro anónimo, el equipo siempre se añade a la organización. Para obtener más información, consulte la sección "Administradores y unidades" (pág. 333).

      Es necesario especificar las credenciales si la opción de registro anónimo en el servidor de gestión está deshabilitada (pág. 332).
   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. Cuando haya terminado la instalación, haga clic en **Salir**.

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

2.6.3.3 Instalación en macOS

Para instalar Agente para Mac

1. Haga doble clic en 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, o seleccione el registro anónimo.

      Especificar las credenciales es útil si su organización tiene unidades y desea añadir el equipo a la unidad gestionada por un administrador específico. Con el registro anónimo, el equipo siempre se añade a la organización. Para obtener más información, consulte la sección "Administradores y unidades" (pág. 333).

      Es necesario especificar las credenciales si la opción de registro anónimo en el servidor de gestión está deshabilitada (pág. 332).
   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**.

2.6.4 Instalación o desinstalación sin supervisión

2.6.4.1 Instalación o desinstalación sin supervisión en Windows

En esta sección se describe cómo instalar o desinstalar Acronis Backup en el modo sin supervisión 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" (pág. 73)).

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. Los paquetes de instalación de estos componentes se extraerán del programa de instalación.
4. Compruebe o modifique el resto de la configuración de instalación que se añadirá al archivo .mst.
5. 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

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

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 de instalación o desinstalación sin supervisión" (pág. 55).

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=ru
ACEP_AGREEMENT=1 AMS_USE_SYSTEM_ACCOUNT=1 AMS_PUBLIC_ADDRESS=10.10.1.1
```

- Instalación del Agente para Windows, la herramienta de línea de comandos y el monitor de copia de seguridad. 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,TrayMonito
r TARGETDIR="C:\Program Files\Acronis" REBOOT=ReallySuppress CURRENT_LANGUAGE=en
ACEP_AGREEMENT=1 MMS_CREATE_NEW_ACCOUNT=1 MANAGEMENT_SERVER_ADDRESS=10.10.1.1
```

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=<lista de componentes>

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
MonitoringServer	AcronisCentralizedManagementServer	32 bits / 64 bits	Servicio de monitorización
ComponentRegisterFeature	AcronisCentralizedManagementServer	32 bits / 64 bits	Componentes para la instalación remota
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	Agent for 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 for 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	Agent for Hyper-V
ESXVirtualAppliance		32 bits / 64 bits	Agente para VMware (dispositivo virtual)
CommandLineTool		32 bits / 64 bits	Herramienta de línea de comandos
TrayMonitor	BackupAndRecoveryAgent	32 bits / 64 bits	Monitorización de copias de seguridad
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=<ruta>

La carpeta donde se instalará el producto.

REBOOT=ReallySuppress

Si se especifica el parámetro, se prohíbe el reinicio del equipo.

CURRENT_LANGUAGE=<ID de idioma>

El idioma del producto. Los valores disponibles son los siguientes: **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 (PEC) de Acronis.

REGISTRATION_ADDRESS=<nombre de servidor o dirección IP>:<puerto>

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).

Si está deshabilitada (pág. 332) la opción de registro anónimo en el servidor de gestión, 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 de copias de seguridad, como se describe en Implementación de agentes mediante la directiva de grupo (pág. 73).

REGISTRATION_LOGIN=<nombre de usuario>, **REGISTRATION_PASSWORD=**<contraseña>

Nombre de usuario y contraseña del administrador del servidor de gestión.

REGISTRATION_TENANT=<ID de unidad>

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 de copias de seguridad haga clic en **Configuración** > **Administradores**, seleccione la unidad y haga clic en **Detalles**.

Este parámetro no funciona sin **REGISTRATION_TOKEN** ni sin **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 falla. Si el valor es **0**, la instalación se lleva a cabo correctamente, aunque el componente no esté registrado.

REGISTRATION_CA_SYSTEM={0,1}|REGISTRATION_CA_BUNDLE={0,1}|REGISTRATION_PINNED_PUBLIC_KEY={0,1}

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, el paquete de la CA proporcionado con el producto o la clave pública anclada, como corresponda. 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.

PINNED_PUBLIC_KEY=<valor de clave pública>

Valor de la clave pública anclada. Este parámetro se debe especificar junto con el parámetro **REGISTRATION_PINNED_PUBLIC_KEY** o en lugar de este.

/l*v <archivo de registro>

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=<número de puerto>

El puerto que utilizarán los navegadores web para acceder al servidor de gestión. El valor predeterminado es 9877.

AMS_ZMQ_PORT=<número de puerto>

El puerto que se utilizará para la comunicación entre los componentes del producto. El valor predeterminado es 7780.

SQL_INSTANCE=<instancia>

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=<nombre de usuario> y **SQL_PASSWORD=**<contraseña>

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=**<nombre de usuario> y **AMS_SERVICE_PASSWORD=**<contraseña>

  Se utilizará la cuenta especificada.

Parámetros de instalación del agente

HTTP_PROXY_ADDRESS=<dirección IP> y **HTTP_PROXY_PORT=**<puerto>

Servidor proxy HTTP que utilizará el agente. Sin estos parámetros, no se utilizará ningún servidor proxy.

HTTP_PROXY_LOGIN=<nombre de usuario> y **HTTP_PROXY_PASSWORD=**<contraseña>

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

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" (pág. 50).

Si el valor es **1**, especifique los parámetros siguientes:

ESX_HOST=<nombre de servidor o dirección IP>

El nombre del servidor o dirección IP del vCenter Server o servidor ESXi.

ESX_USER=<nombre de usuario> y **ESX_PASSWORD=**<contraseña>

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=**<nombre de usuario> y **MMS_SERVICE_PASSWORD=**<contraseña>

  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=**<nombre de usuario> y **ASN_SERVICE_PASSWORD=**<contraseña>

  Se utilizará la cuenta especificada.

Parámetros de desinstalación

REMOVE={<lista de componentes>**|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.

2.6.4.2 Instalación o desinstalación sin supervisión en Linux

Esta sección describe cómo instalar o desinstalar Acronis Backup en el modo sin supervisión en un equipo que ejecute Linux, o mediante la 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).

Parámetros de instalación

Parámetros comunes

{-i |--id=}<lista de componentes>

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
MonitoringServer	Servicio de monitorización

Sin este parámetro, se instalarán todos los componentes anteriores.

--language=<ID de idioma>

El idioma del producto. Los valores disponibles son los siguientes: **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=}<número de puerto>

El puerto que utilizarán los navegadores web para acceder al servidor de gestión. El valor predeterminado es 9877.

--ams-tcp-port=<número de puerto>

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 registre el agente en el servidor de gestión.
- **{-C |--ams=}**<nombre de servidor o dirección IP>

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**.

Si está deshabilitada (pág. 332) la opción de registro anónimo en el servidor de gestión, debe especificar el parámetro **token**, o los parámetros **login** y **password**.

--token=<token>

Token de registro que se generó en la consola de copias de seguridad, como se describe en Implementación de agentes mediante la directiva de grupo (pág. 73).

{-g |--login=}<nombre de usuario> y **{-w |--password=}**<contraseña>

Credenciales de un administrador del servidor de gestión.

--unit=<ID de unidad>

La unidad dentro de la organización. El agente se añadirá a esta unidad.

Para averiguar el ID de una unidad, en la consola de copias de seguridad haga clic en **Configuración** > **Administradores**, 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=<valor de clave pública>

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=**<dirección IP> y **--http-proxy-port=**<puerto>

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

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

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

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.

```
./AcronisBackup_12.5_64-bit.x86_64 -a -i AcronisCentralizedManagementServer
```

- Instalación del servidor de gestión y el servicio de supervisión. Especificación de puertos personalizados.

```
./AcronisBackup_12.5_64-bit.x86_64 -a -i
AcronisCentralizedManagementServer,MonitoringServer --web-server-port 6543
--ams-tcp-port 8123
```

- Instalación del Agente para Linux y su registro en el servidor de gestión especificado.

```
./AcronisBackup_12.5_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.

```
./AcronisBackup_12.5_64-bit.x86_64 -a -i BackupAndRecoveryAgent --ams 10.10.1.1
--login root --password 123456 –unit 01234567-89AB-CDEF-0123-456789ABCDEF
```

2.6.5 Buscar actualizaciones de software

Esta funcionalidad solo está disponible para administradores de la organización (pág. 333).

Cada vez que inicie sesión en la consola de copias de seguridad, Acronis Backup busca nuevas versiones disponibles en el sitio web de Acronis. En ese caso, la consola de copias de seguridad muestra un enlace de descarga de la nueva versión en la parte inferior de cada página en las pestañas **Dispositivos**, **Planes** y **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** (pág. 332).

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**.

2.6.6 Gestión de licencias

Las licencias de Acronis Backup se basan en el número de equipos físicos y hosts de virtualización de los que se ha realizado la copia de seguridad. Se pueden utilizar tanto la licencia de suscripción como la licencia perpetua. El periodo de caducidad de la suscripción comienza cuando la registra en el sitio de Acronis.

Para comenzar a utilizar Acronis Backup, 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 copias de seguridad.

Las licencias también pueden asignarse y revocarse manualmente. Las operaciones manuales con licencias solo están disponibles para administradores de la organización (pág. 333).

Para acceder a la página Licencias

1. Realice uno de los siguientes procedimientos:
   - Haga clic en **Configuración**.
   - Haga clic en el icono de la cuenta en la esquina superior derecha.
2. Haga clic en **Licencias**.

Para añadir una clave de licencia

1. Haga clic en **Añadir claves**.
2. Introduzca las claves de licencia.
3. Haga clic en **Agregar**.
4. Para activar una suscripción, debe haber iniciado sesión. Si ha introducido al menos una clave de suscripción, especifique la dirección de correo electrónico y la contraseña de su cuenta de Acronis y, a continuación, haga clic en **Iniciar sesión**. Si solo ha introducido claves perpetuas, omita este paso.
5. Haga clic en **Realizado**.

Consejo *Si ya ha registrado las claves de suscripción, el servidor de gestión podrá importarlas desde su cuenta de Acronis. Para sincronizar las claves de suscripción, haga clic en* ***Sincronizar*** *e inicie sesión.*

Gestión de licencias perpetuas

Para asignar una licencia perpetua a un equipo

1. Seleccione una licencia perpetua.

   El software muestra las claves de licencia que corresponden a la licencia seleccionada.
2. Seleccione la clave que se debe asignar.
3. Haga clic en **Asignar**.

   El software muestra los equipos a los que se puede asignar la clave seleccionada.
4. Seleccione el equipo y haga clic en **Finalizado**.

Para revocar una licencia perpetua de un equipo

1. Seleccione una licencia perpetua.

   El software muestra las claves de licencia que corresponden a la licencia seleccionada. El equipo al que está asignada la clave se muestra en la columna **Asignada a**.
2. Seleccione la clave de licencia que se debe revocar.
3. Haga clic en **Revocar**.
4. Confirme su decisión.

   La clave revocada permanecerá en la lista de claves de licencia. Se podrá asignar a otro equipo.

Gestión de licencias de suscripción

Para asignar una licencia de suscripción a un equipo

1. Seleccione una licencia de suscripción.

   El software muestra los equipos a los que la licencia seleccionada ya está asignada.
2. Haga clic en **Asignar**.

El software muestra los equipos a los que la licencia seleccionada se puede asignar.

3. Seleccione el equipo y haga clic en **Finalizado**.

Para revocar una licencia de suscripción de un equipo

1. Seleccione una licencia de suscripción.

   El software muestra los equipos a los que la licencia seleccionada ya está asignada.
2. Seleccione el equipo al que se debe revocar la licencia.
3. Haga clic en **Revocar licencia**.
4. Confirme su decisión.

2.7 Implementación en la nube

2.7.1 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 active 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 de copias de seguridad.** Utilícelo para acceder a la consola en el futuro. El usuario y la contraseña son los mismos que en el paso anterior.

2.7.2 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 la sección "Componentes" (pág. 18).

Paso 2

Descargue 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 de interacción, por ejemplo, a través de la directiva de grupo. Este escenario avanzado se describe en "Implementación de agentes a través de la directiva de grupo" (pág. 73).

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

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 copias de seguridad. 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 siguiente puertos TCP:

- **443** y **8443** Se usan estos puertos para el acceder a la consola de copias de seguridad, registrar los agentes, descargar los certificados, obtener la autorización del usuario y descargar archivos del almacenamiento en la cloud.
- **7770...7800** Los agentes usan estos puertos para comunicarse con el servidor de gestión de copias de seguridad.
- **44445** Los agentes usan este puerto para transferir datos durante la realización de copias de seguridad y durante la recuperación.

Si hay un servidor proxy habilitado en la red, consulte la sección "Configuración del servidor proxy" (pág. 66) para saber si debe configurar estos valores en cada equipo que ejecute un agente de copia de seguridad.

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.

2.7.3 Configuración del servidor proxy

Los agentes de copia de seguridad 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.

En Windows

Si se configura un servidor proxy en Windows (**Panel de control** > **Opciones de Internet** > **Conexiones**), el programa de instalación lee la configuración del servidor proxy del registro y la usa automáticamente. También puede especificar la configuración del servidor proxy durante la instalación, o bien hacerlo antes mediante el procedimiento que se describe a continuación. Para modificar la configuración del servidor proxy durante la instalación, siga el mismo procedimiento.

Para especificar la configuración del servidor proxy en Windows:

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 de copias de seguridad aún no está instalado, ahora puede instalarlo. De lo contrario, haga lo siguiente para reiniciar el agente:
   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
```

En Linux

Ejecute el archivo de instalación con estos parámetros: **`--http-proxy-host`**=DIRECCIÓN **`--http-proxy-port`**=PUERTO **`--http-proxy-login`**=INICIO DE SESIÓN **`--http-proxy-password`**=CONTRASEÑA. Para modificar la configuración del servidor proxy durante la instalación, siga el procedimiento que se describe a continuación.

Para cambiar la configuración del servidor proxy en Linux:

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, 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>`**.
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. Reinicie el agente ejecutando el comando siguiente en cualquier directorio:

```
sudo service acronis_mms restart
```

En macOS

Puede especificar la configuración del servidor proxy durante la instalación, o bien hacerlo antes mediante el procedimiento que se describe a continuación. Para modificar la configuración del servidor proxy durante la instalación, siga el mismo procedimiento.

Para especificar la configuración del servidor proxy en macOS:

1. Cree el archivo **/Library/Application Support/Acronis/Registry/Global.config** y ábralo con un editor de texto, como por ejemplo, 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 de copias de seguridad aún no está instalado, ahora puede instalarlo. De lo contrario, haga lo siguiente para reiniciar el agente:
   a. Vaya a **Aplicaciones** > **Utilidades** > **Terminal**.
   b. Ejecute los siguientes comandos:

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

2.7.4 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:
   - 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.
   - Cambiar la ruta de acceso de instalación.
   - Cambiar la cuenta para el servicio de agente.
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 (pág. 286) en el servidor vCenter Server o ESXi.
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.
7. Espere a que se muestre la pantalla de registro.
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 de copia de seguridad, 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**.

Consejo *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 de copia de seguridad.

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=INICIO DE SESIÓN **--http-proxy-password=**CONTRASEÑA.
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. Espere a que se muestre la pantalla de registro.
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 de copia de seguridad, 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**.

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 de copia de seguridad.

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 copia de seguridad**, 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 de copia de seguridad, 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**.

   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 de copia de seguridad.

2.8 Implementación del Agente para VMware (dispositivo virtual) desde una plantilla de OVF

2.8.1 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. Le recomendamos que aumente estos recursos a 8 GB de RAM y 4 vCPU 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) para mejorar el rendimiento de copia de seguridad.

Las unidades de disco virtual del propio dispositivo no ocupan más de 6 GB. No importa si el formato del disco es ligero o denso, ya que esto no afecta al rendimiento del dispositivo.

¿Cuántos agentes necesito?

Aunque un dispositivo virtual puede proteger todo un entorno vSphere, lo mejor es implementar un dispositivo virtual por clúster vSphere (o por host, si no hay clústeres). Esto provoca que las copias de seguridad sean más rápidas porque el dispositivo puede adjuntar los discos de los que se ha realizado la copia mediante el transporte HotAdd y, por tanto, la transferencia de datos de la copia de seguridad se dirige desde un disco local a otro.

Es normal usar tanto el dispositivo virtual como el agente para VMware (Windows) a la vez, siempre que estén conectados al mismo vCenter Server *o* a diferentes hosts ESXi. Evite los casos en los que un agente se conecte a un ESXi directamente y otro se conecte al vCenter Server que gestione este ESXi.

No le recomendamos usar un almacenamiento conectado localmente (es decir, almacenar copias de seguridad en discos virtuales añadidos al dispositivo virtual) si tiene más de un agente. Para obtener más detalles, consulte Utilización de un almacenamiento conectado localmente.

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**.

2.8.2 Implementación de la plantilla de 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 de 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 en una instalación, seleccione una red que incluya el servidor de gestión.

2.8.3 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. Busque la siguiente sección:

```
<key name="HttpProxy">
    <value name="Enabled" type="Tdword">"0"</value>
    <value name="Host" type="TString">"DIRECCIÓN"</value>
    <value name="Port" type="Tdword">"PUERTO"</value>
    <value name="Login" type="TString">"INICIO DE SESIÓN"</value>
    <value name="Password" type="TString">"CONTRASEÑA"</value>
</key>
```

d. Sustituya **0** por **1**.

e. Reemplace DIRECCIÓN por el nombre del host o la dirección IP del servidor proxy y PUERTO por el valor decimal del número de puerto.

f. 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.

g. Guarde el archivo.

h. Ejecute el comando **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 (pág. 286) en el servidor vCenter Server o ESXi.

   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 copia de seguridad. 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 el cloud, indique el nombre de usuario y la contraseña para el servicio de copias de seguridad. 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 programadas 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.

2.8.4 Actualización de Agent for VMware (Virtual Appliance)

En las implementaciones locales, use el mismo procedimiento de actualización que para el resto de los agentes (pág. 75).

En las implementaciones en el cloud, use el siguiente procedimiento.

Pasos para actualizar el Agente para VMware (dispositivo virtual) en implementaciones en el cloud

1. Elimine Agente para VMware (dispositivo virtual), tal como se describe en "Desinstalación del producto (pág. 76)". En el paso 5, elimine el agente de **Configuración** > **Agentes** aunque tenga previsto volver a instalarlo.
2. Implemente Agente para VMware (dispositivo virtual), tal como se describe en "Implementación de la plantilla OVF".
3. Configure Agente para VMware (dispositivo virtual), tal como se describe en "Configuración del dispositivo virtual".

   Si quiere reconstruir el almacenamiento adjunto de forma local, haga lo siguiente en el paso 7:

   a. Añada el disco que contenga el almacenamiento local al dispositivo virtual.
   b. Haga clic en **Actualizar** > **Crear almacenamiento** > **Montar**.
   c. El software mostrará la **letra** y la **etiqueta** originales del disco. No las modifique.
   d. Haga clic en **Aceptar**.

   Como resultado, los planes de copias de seguridad aplicados al agente anterior se volverán a aplicar automáticamente al agente nuevo.
4. Los planes con la copia de seguridad que detecta aplicaciones activada requieren que se vuelvan a introducir las credenciales del SO invitado. Edite estos planes y vuelva a introducir las credenciales.
5. Los planes que incluyen la copia de seguridad de la configuración ESXi requieren que se vuelva a introducir la contraseña "raíz". Edite estos planes y vuelva a introducir la contraseña.

2.9 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 de copias de seguridad.

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 de copia de seguridad. Esto le permite registrar cualquier número de equipos usando su cuenta. Para más seguridad, los tokens tienen una duración limitada.

Para generar un token de registro:

1. Inicie sesión en la consola de copia de seguridad 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 2: 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**.

2.10 Actualización de agentes

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

Puede actualizar agentes al repetir su instalación de cualquier modo disponible. Para actualizar varios agentes simultáneamente, siga el procedimiento indicado a continuación.

Para actualizar agentes mediante la pestaña Agentes

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" (pág. 46) > "Paquetes de instalación".
3. Haga clic en **Ajustes** > **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**.

   [Solo en implementaciones locales] El progreso de la actualización aparece en la pestaña **Actividades**.

2.11 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.

Aviso *En implementaciones en una instalación, no desinstale el servidor de gestión por error. Si lo hace, la consola de copia de seguridad dejará de estar disponible. Ya no podría realizar copias de seguridad ni recuperaciones en todos los equipos que están registrados en el servidor de gestión.*

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 Backup** > **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 de copia de seguridad y las copias de seguridad del antiguo equipo podrían no asociarse al nuevo equipo.
4. Confirme su decisión.
5. Si tiene previsto volver a instalar el agente, omita este paso. En caso contrario, en la consola de copia de seguridad, haga clic en **Configuración** > **Agentes**, seleccione el equipo donde se instaló el agente y, a continuación, haga clic en **Eliminar**.

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 de copia de seguridad y las copias de seguridad del antiguo equipo podrían no asociarse al nuevo equipo.

3. Confirme su decisión.
4. Si tiene previsto volver a instalar el agente, omita este paso. En caso contrario, en la consola de copia de seguridad, haga clic en **Configuración** > **Agentes**, seleccione el equipo donde se instaló el agente y, a continuación, haga clic en **Eliminar**.

En OS X

1. Haga doble clic en 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.
6. Si tiene previsto volver a instalar el agente, omita este paso. En caso contrario, en la consola de copia de seguridad, haga clic en **Configuración** > **Agentes**, seleccione el equipo donde se instaló el agente y, a continuación, haga clic en **Eliminar**.

Eliminación de Agente para VMware (dispositivo virtual)

1. Abra vSphere Client e inicie sesión en vCenter Server.
2. Si el dispositivo virtual (VA) está encendido, haga clic sobre él con el botón derecho y luego elija **Activar** > **Apagar**. Confirme su decisión.
3. Si el VA utiliza un almacenamiento conectado localmente en una unidad de disco virtual y desea conservar los datos en ese disco, haga lo siguiente:
   a. Haga clic con el botón derecho en el VA y después 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 VA.
4. Haga clic con el botón derecho en el VA y haga clic en **Eliminar del disco**. Confirme su decisión.
5. Si tiene previsto volver a instalar el agente, omita este paso. En caso contrario, en la consola de copia de seguridad, haga clic en **Configuración** > **Agentes**, seleccione el dispositivo virtual y, a continuación, haga clic en **Eliminar**.

3 Acceso a la consola de copia de seguridad

Para acceder a la consola de copia de seguridad, 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 en una instalación

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 (pág. 42). El puerto predeterminado es 9877.

Puede configurar el servidor de gestión (pág. 84) para prohibir el acceso a la consola de copias de seguridad 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 de copia de seguridad.

- 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 (pág. 78). Si no lo hace, el navegador le solicitará un nombre de usuario y una contraseña.
- 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" (pág. 333).

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" (pág. 333).

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.

3.1 Configuración de un navegador web para autenticación integrada de Windows

La autenticación integrada de Windows es posible si accede a la consola de copia de seguridad desde un equipo con Windows y cualquier navegador admitido.

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.

Configuración de Internet Explorer, Microsoft Edge, Opera y Google Chrome

Si el equipo con el navegador se encuentra en el mismo dominio de Active Directory que el equipo con el servidor de gestión, añada la página de inicio de sesión de la consola a la lista de sitio de la **intranet local**.

Si no, añada la página de inicio de sesión de la consola a la lista de **Sitios de confianza** y active el ajuste **Inicio de sesión automático con el nombre y la contraseña actual del usuario**.

Se ofrecen instrucciones detalladas más adelante en esta sección. Como estos navegadores utilizan la configuración de Windows, también es posible configurarlos utilizando la política de grupos de un dominio de Active Directory.

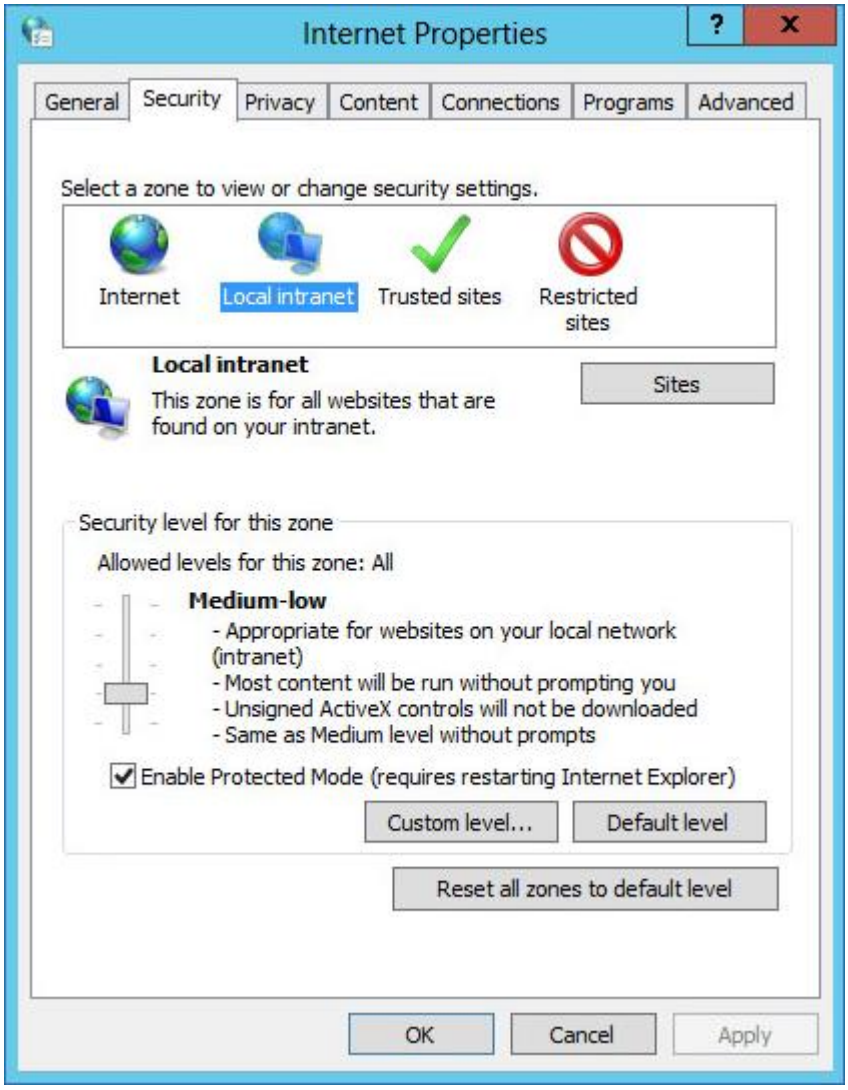
Configuración de Mozilla Firefox

1. En Firefox, navegue hasta la URL `about:config` y, a continuación, haga clic en el botón **Acepto los riesgos**.
2. En el campo **Búsqueda**, busque la preferencia `network.negotiate-auth.trusted-uris`.
3. Haga doble clic en la preferencia y, a continuación, introduzca la dirección de la página de inicio de la consola de copia de seguridad.
4. Repita los pasos 2-3 para la preferencia `network.automatic-ntlm-auth.trusted-uris`.
5. Cierre la ventana `about:config`.

3.1.1 Incorporación de la consola a la lista de sitios de la intranet local

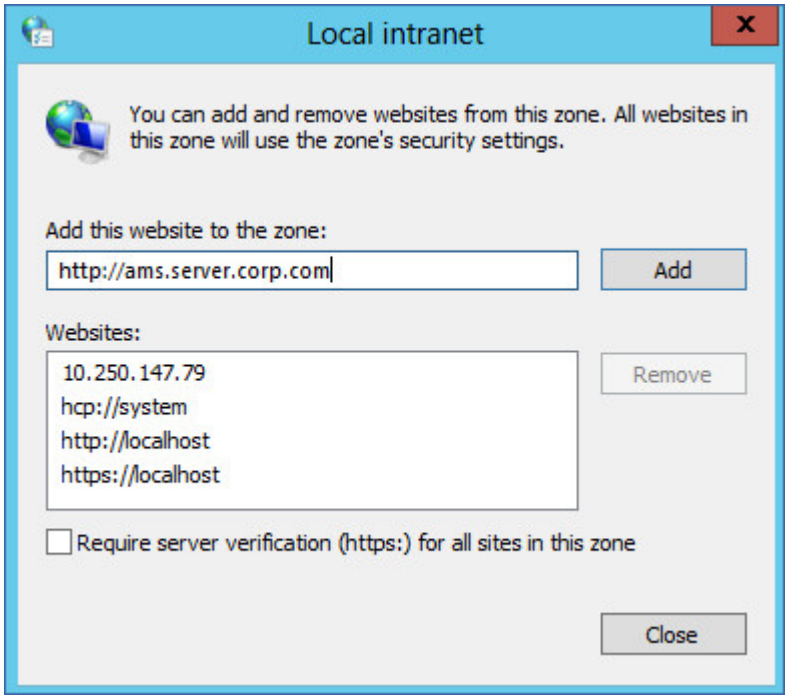
1. Vaya al **Panel de control** > **Opciones de Internet**.

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 de copia de seguridad y, a continuación, haga clic en **Añadir**.

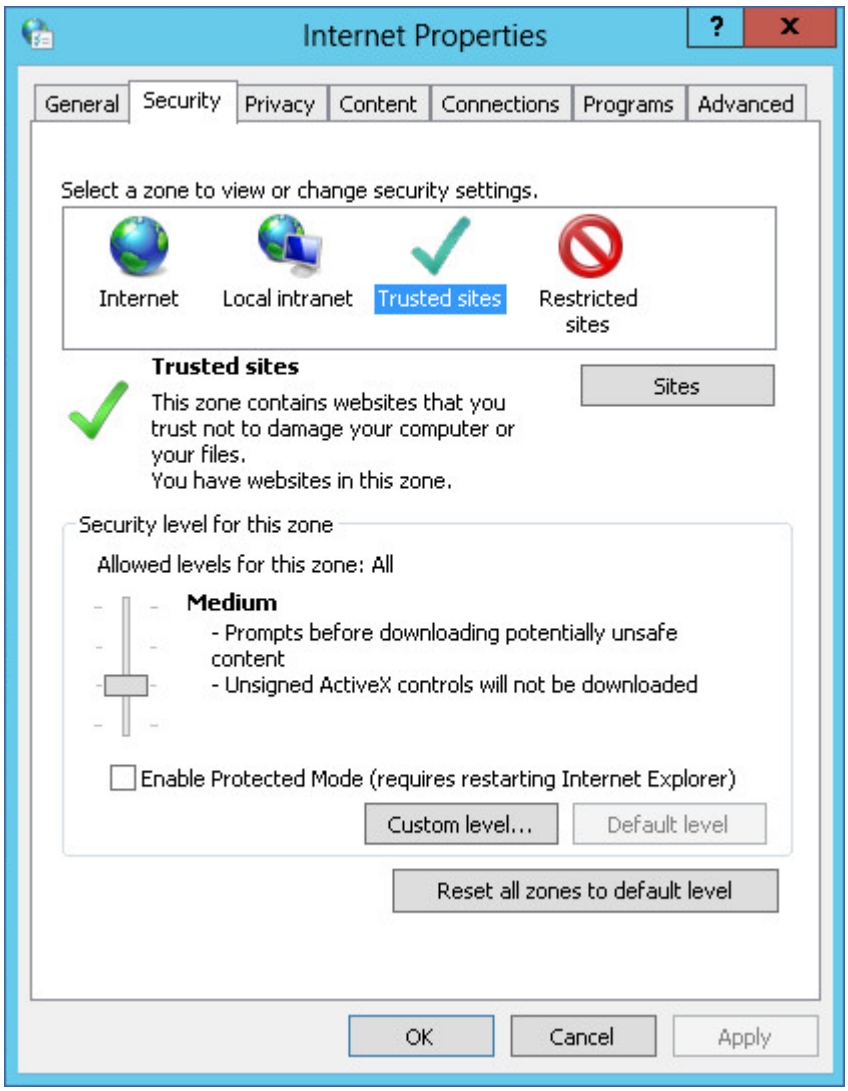


5. Haga clic en **Cerrar**.
6. Haga clic en **Aceptar**.

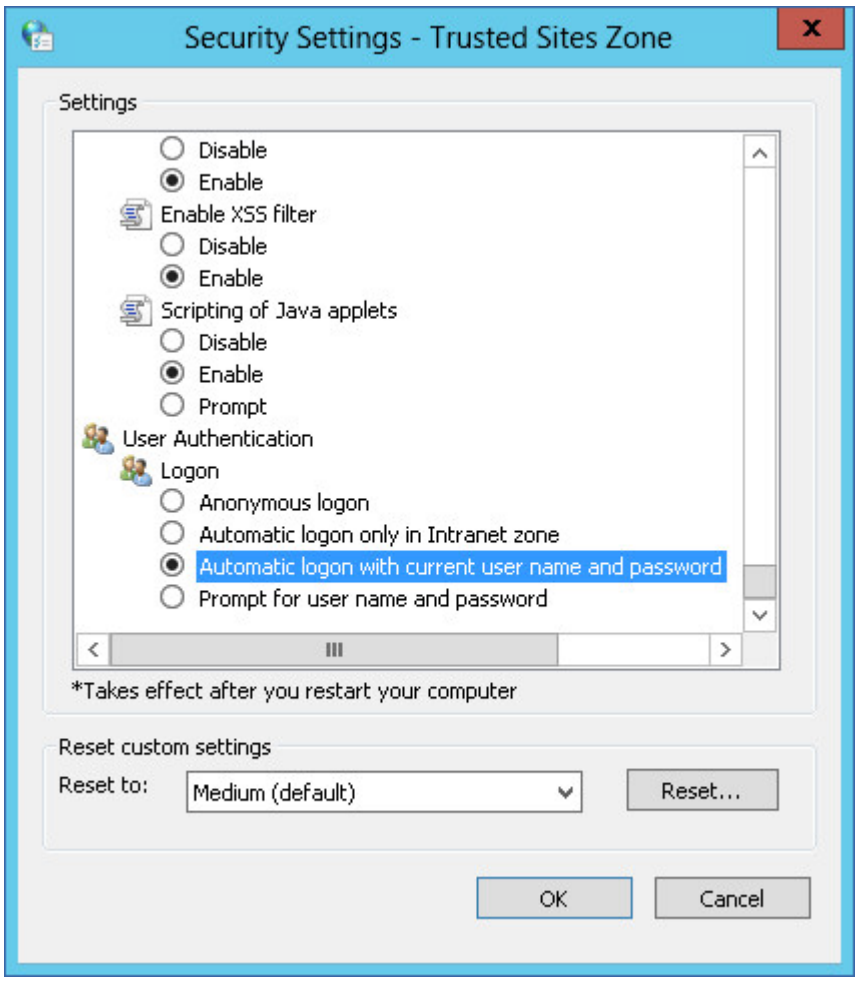
3.1.2 Incorporación de la consola a la lista de sitios de confianza

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**.

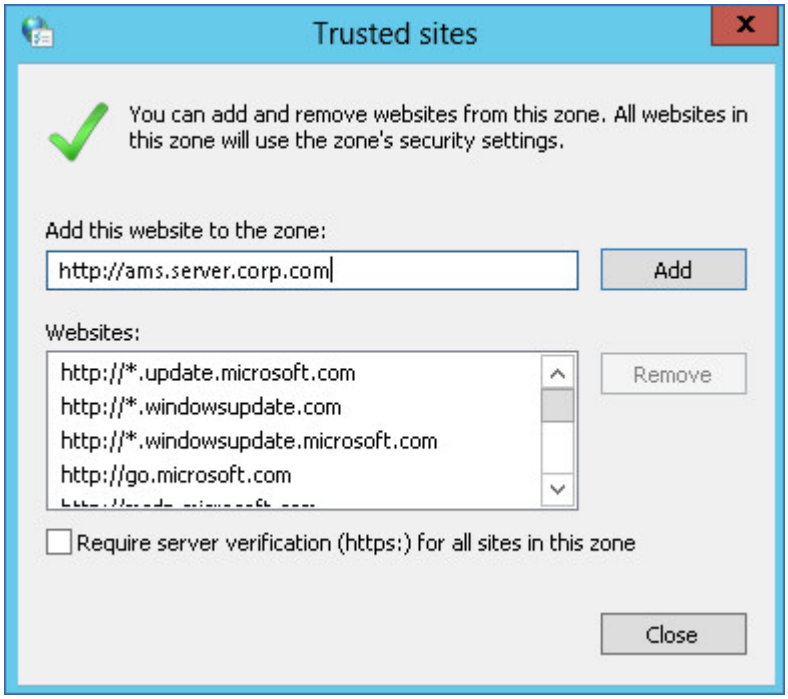


3. En **Iniciar sesión**, seleccione **Inicio de sesión automático con el usuario y la contraseña actuales** y, a continuación, haga clic en **Aceptar**.



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 de copia de seguridad y, a continuación, haga clic en **Añadir**.



6. Haga clic en **Cerrar**.
7. Haga clic en **Aceptar**.

3.2 Cambio de la configuración del certificado SSL

Esta sección describe cómo cambiar el certificado Secure Socket Layer (SSL) autofirmado generado por el servidor de gestión por un certificado emitido por una autoridad 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 de copias de seguridad mediante el protocolo HTTPS.

Opcionalmente, puede configurar el servidor de gestión, así como prohibir el acceso a la consola de copias de seguridad mediante HTTP y redirigir a todos los usuarios a la versión HTTPS.

Para cambiar la configuración del certificado SSL

1. Asegúrese de tener lo siguiente:
   - El archivo del certificado (.pem, .cert u otro formato)
   - El archivo con la clave privada para el certificado (generalmente, .key)
   - La frase de contraseña de clave privada, si la clave está cifrada
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": "",
    "auto_redirect": false
}
```

5. Entre las comillas de la línea **"cert_file"**, especifique la ruta completa al archivo de certificado. Por ejemplo:
   - En Windows (tenga en cuenta las barras diagonales): **"cert_file": "C:/certificate/local-domain.ams.cert"**
   - En Linux: **"cert_file": "/home/user/local-domain.ams.cert"**
6. Entre las comillas de la línea **"key_file"**, especifique la ruta completa al archivo de clave privada. Por ejemplo:
   - En Windows (tenga en cuenta las barras diagonales): **"key_file": "C:/certificate/private.key"**
   - En Linux: **"key_file": "/home/user/private.key"**
7. Si la clave privada está cifrada, especifique la frase de contraseña de la clave privada entre las comillas de la línea **"passphrase"**. Por ejemplo: **"passphrase": "my secret passphrase"**
8. Si desea prohibir el acceso a la consola de copias de seguridad mediante HTTP redirigiendo a todos los usuarios a la versión HTTPS, cambie el valor de **"auto_redirect"** de **false** a **true**. De lo contrario, omita este paso.
9. Guarde el archivo **api_gateway.json**.

Importante *Tenga cuidado de no eliminar accidentalmente comas, paréntesis o comillas en el archivo de configuración.*

10. Reinicie Acronis Service Manager Service como se describe continuación.

Para reiniciar Acronis Service Manager Service 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
```

Para reiniciar Acronis Service Manager Service en Linux

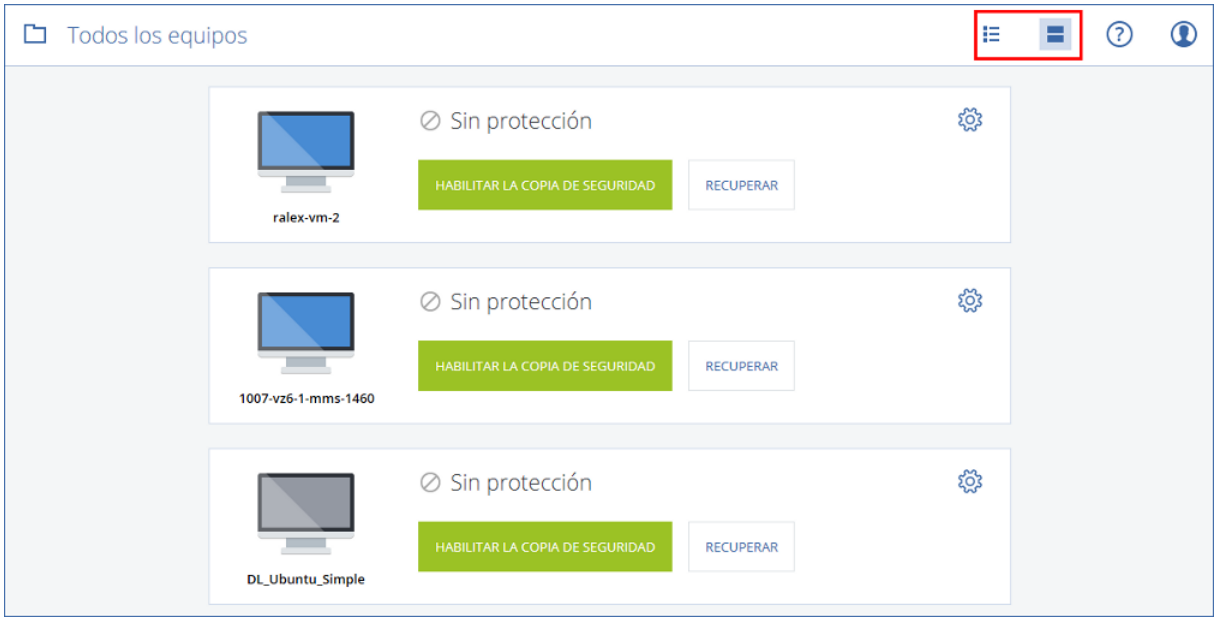
1. Abra el **Terminal**.
2. Ejecute el comando siguiente en cualquier directorio:

```
sudo service acronis_asm restart
```

4 Vistas de la consola de copias de seguridad

La consola de copias de seguridad 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.

5 Copia de seguridad

Un plan de copias de seguridad es una serie de reglas que especifica cómo se protegerán los datos en un equipo determinado.

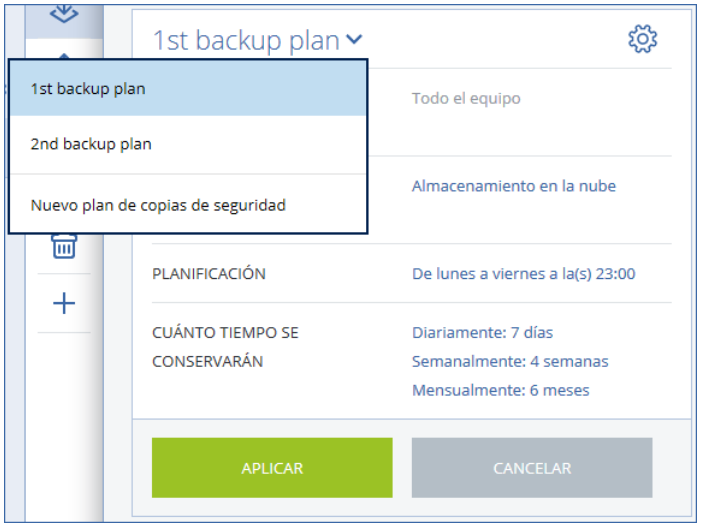
Cuando cree un plan de copias de seguridad, puede aplicarlo a múltiples equipos en ese momento o más adelante.

Nota *En las implementaciones en una instalación, si solo están presentes las licencias estándar en el servidor de gestión, no se puede aplicar un plan de copias de seguridad a varios equipos físicos. Cada equipo físico debe tener su propio plan de copias de seguridad.*

Para crear el primer plan de copias de seguridad

1. Seleccione los equipos que desea incluir en la copia de seguridad.
2. Haga clic en **Copia de seguridad**.

El software muestra una nueva plantilla de plan de copias de seguridad.

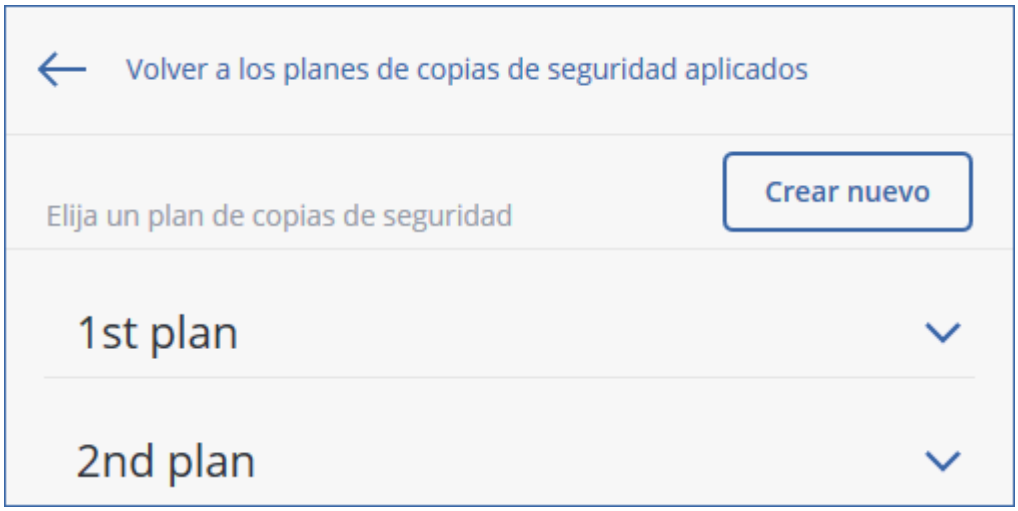


3. [Opcional] Para modificar el nombre del plan de copias de seguridad, haga clic en el nombre predeterminado.
4. [Opcional] Para modificar los parámetros del plan, haga clic en la sección correspondiente del panel del plan de copias de seguridad.
5. [Opcional] Para modificar las opciones de copia de seguridad, haga clic en el icono de engranaje.
6. Haga clic en **Crear**.

Para aplicar un plan de copias de seguridad existente

1. Seleccione los equipos que desea incluir en la copia de seguridad.
2. Haga clic en **Copia de seguridad**. Si ya se aplica un plan de copias de seguridad común a los equipos seleccionados, haga clic en **Agregar plan de copias de seguridad**.

   El software muestra planes de copias de seguridad creados previamente.



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

5.1 Apuntes del plan de copias de seguridad

Importante *Algunas de las funciones descritas en esta sección se introdujeron en la versión 12.5, que afecta solo a las implementaciones en una instalación. Estas funciones todavía no están disponibles en las implementaciones en la nube. Para obtener más información, consulte* *"Novedades en Acronis Backup" (pág. 8).*

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

DE QUÉ REALIZAR COPIAS DE SEGURIDAD	ELEMENTOS PARA INCLUIR EN LA COPIA DE SEGURIDAD Métodos de selección	DÓNDE REALIZAR COPIAS DE SEGURIDAD	PLANIFICAR Esquemas de copia de seguridad (no para la cloud)	CUÁNTO TIEMPO GUARDARLAS
Discos/volúmenes (equipos físicos)	Selección directa (pág. 93) Normas de directiva (pág. 93) Filtros de archivo (pág. 136)	Nube (pág. 97) Carpeta local (pág. 97) Carpeta de red (pág. 97) Servidor SFTP (pág. 97)* NFS (pág. 97)* Secure Zone (pág. 97)* Ubicación gestionada (pág. 97)* Dispositivo de cintas (pág. 97)*	Siempre incremental (archivo único) (pág. 103)* Siempre completas (pág. 103) Completa semanal, incremental diaria (pág. 103) Completa mensual, diferencial semanal, incremental diaria (GFS) (pág. 103) Personalizadas (F-D-I) (pág. 103)	Por antigüedad de las copias de seguridad (norma única/por conjunto de copias de seguridad) (pág. 113) Por número de copias de seguridad (pág. 113) Por tamaño total de las copias de seguridad (pág. 113)* Guardar indefinidamente (pág. 113)
Discos/volúmenes (equipos virtuales)	Normas de directiva (pág. 93) Filtros de archivo (pág. 136)	Nube (pág. 97) Carpeta local (pág. 97) Carpeta de red (pág. 97) Servidor SFTP (pág. 97)* NFS (pág. 97)* Ubicación gestionada (pág. 97)* Dispositivo de cintas (pág. 97)*		
Archivos (sólo equipos físicos)	Selección directa (pág. 91) Normas de directiva (pág. 91) Filtros de archivo (pág. 136)	Nube (pág. 97) Carpeta local (pág. 97) Carpeta de red (pág. 97) Servidor SFTP (pág. 97)* NFS (pág. 97)* Secure Zone (pág. 97)* Ubicación gestionada (pág. 97)* Dispositivo de cintas (pág. 97)	Siempre completas (pág. 103) Completa semanal, incremental diaria (pág. 103) Completa mensual, diferencial semanal, incremental diaria (GFS) (pág. 103) Personalizadas (F-D-I) (pág. 103)	
Configuración de ESXi	Selección directa (pág. 96)	Carpeta local (pág. 97) Carpeta de red (pág. 97) Servidor SFTP (pág. 97) NFS (pág. 97)*		

<table>
<tr><th>DE QUÉ REALIZAR COPIAS DE SEGURIDAD</th><th>ELEMENTOS PARA INCLUIR EN LA COPIA DE SEGURIDAD
Métodos de selección</th><th>DÓNDE REALIZAR COPIAS DE SEGURIDAD</th><th>PLANIFICAR
Esquemas de copia de seguridad
(no para la cloud)</th><th>CUÁNTO TIEMPO GUARDARLAS</th></tr>
<tr><td>Estado del sistema (solo en implementaciones en la nube)</td><td>Selección directa (pág. 93)</td><td>Nube (pág. 97)
Carpeta local (pág. 97)
Carpeta de red (pág. 97)</td><td rowspan="3">Siempre completas (pág. 103)
Completas semanalmente, incrementales diariamente (pág. 103)
Personalizadas (F-I) (pág. 103)</td><td rowspan="3"></td></tr>
<tr><td>Bases de datos SQL</td><td>Selección directa (pág. 241)</td><td rowspan="2">Nube (pág. 97)
Carpeta local (pág. 97)
Carpeta de red (pág. 97)
Ubicación gestionada (pág. 97)*
Dispositivo de cintas (pág. 97)</td></tr>
<tr><td>Bases de datos de Exchange</td><td>Selección directa (pág. 241)</td></tr>
<tr><td>Buzones de correo de Exchange</td><td>Selección directa (pág. 248)</td><td rowspan="2">Nube (pág. 97)
Carpeta local (pág. 97)
Carpeta de red (pág. 97)
Ubicación gestionada (pág. 97)*</td><td rowspan="2">Siempre incremental (archivo único) (pág. 103)</td><td></td></tr>
<tr><td>Buzones de correo de Office 365</td><td>Selección directa (pág. 262)</td><td>Por antigüedad de las copias de seguridad (norma única/por conjunto de copias de seguridad) (pág. 113)
Por número de copias de seguridad (pág. 113)
Guardar indefinidamente (pág. 113)</td></tr>
</table>

* Consulte las limitaciones a continuación.

Limitaciones

Servidor SFTP y dispositivo de cintas

- Estas ubicaciones no pueden ser un destino de copias de seguridad a nivel de disco de 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.

Secure Zone

- Secure Zone no se puede crear en un Mac.

Ubicación gestionada

- Una ubicación gestionada no puede ser un destino si el esquema de copias de seguridad está configurado como **Siempre incremental (archivo único)** y el cifrado está habilitado en el plan de copias de seguridad.
- 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 Office 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 (un archivo)

- 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.

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.

5.2 Seleccionar los datos que se incluirán en la copia de seguridad

5.2.1 Seleccionar archivos/carpetas

La copia de seguridad a nivel de archivos está disponible para los equipos físicos.

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.

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 (pág. 136).

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 copias de seguridad:
   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 copias de seguridad. 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 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 de archivos de programa (por ejemplo, **C:\Program Files**).
  - **`%WINDIR%`** selecciona la carpeta en la que 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 de 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**.

5.2.2 Seleccionar un estado del sistema

La copia de seguridad del estado del sistema está disponible para los equipos que ejecutan de Windows Vista en adelante.

Para realizar copias de seguridad del estado del sistema, en **De qué realizar copias de seguridad**, seleccione **Estado del sistema**.

La copia de seguridad de un estado del sistema está formada por los siguientes archivos:

- Configuración del programador de tareas
- Almacenamiento de metadatos de VSS
- Información de configuración del contador de rendimiento
- Servicio MSSearch
- Background Intelligent Transfer Service (BITS)
- El registro
- Windows Management Instrumentation (WMI)
- Base de datos del registro de Component Services Class

5.2.3 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.

Hay dos maneras de seleccionar discos/volúmenes: directamente en cada equipo o usando las normas de política. Puede excluir archivos de la copia de seguridad de un disco activando los filtros de archivo (pág. 136).

Selección directa

La selección directa está disponible únicamente para los equipos físicos.

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 copias de seguridad, seleccione las casillas 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 política

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 política**.
4. Seleccione cualquiera de las normas predefinidas, escriba sus propias normas o combine las dos.

   Las normas de política se aplicarán a todos los equipos incluidos en el plan de copias de seguridad. 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 OS X

- **`[All volumes]`**seleccione todos los volúmenes en los equipos que ejecutan Windows y todos los volúmenes incorporados en los equipos que ejecutan Linux o OS X.

Normas para Windows

- La letra de unidad (por ejemplo: **C:**) selecciona el volumen con la letra de unidad especificada.
- **`[Fixed Volumes (Physical machines)]`** seleccione 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 del sistema y de arranque. Esta combinación es el conjunto mínimo de datos que garantiza la recuperación del sistema operativo desde la copia de seguridad.
- **`[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 duro IDE.
- **`/dev/sda1`** selecciona el primer volumen en el primer disco duro SCSI.
- **`/dev/md1`** selecciona el primer disco duro 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, especifique su nombre junto con el nombre del grupo del volumen. Por ejemplo, para realizar copias de seguridad de dos volúmenes lógicos, **lv_root** y **lv_bin**, que pertenecen al grupo de volumen **vg_mymachine**, especifique:

```
/dev/vg_mymachine/lv_root
/dev/vg_mymachine/lv_bin
```

Normas para OS X

- **`[Disk 1]`** selecciona el primer disco del equipo, incluidos todos los volúmenes de ese disco. Para seleccionar otro disco, escriba el número correspondiente.

5.2.3.1 ¿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 no se les realizan copias de seguridad en los sistemas operativos Windows Vista, puntos de restauración de Windows.
  - Si se habilita la opción de copia de seguridad **Servicio de instantáneas de volumen (VSS)** (pág. 154), 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.

5.2.4 Selección de la configuración de ESXi

Una copia de seguridad de una configuración de servidor ESXi permite recuperar un servidor ESXi desde cero. La recuperación se lleva a cabo con un dispositivo de arranque.

Los equipos virtuales que se ejecutan en el servidor no se incluyen en la copia de seguridad. Se puede hacer una copia de seguridad de ellos y se pueden recuperar por separado.

Una copia de seguridad de una configuración de servidor ESXi incluye:

- Las particiones del cargador de arranque y el banco de arranque del servidor.
- El estado del servidor (configuración del almacenamiento y las redes virtuales, claves SSL, ajustes de la red del servidor e información del usuario local).
- Extensiones o parches instalados o montados en el servidor.
- Archivos de registro.

Requisitos previos

- SSH debe estar habilitado en el **Perfil de seguridad** de la configuración del servidor ESXi.
- Tiene que conocer la contraseña de la cuenta "raíz" alojada en el servidor ESXi.

Para seleccionar una configuración de ESXi

1. Haga clic en **Dispositivos** > **Todos los equipos** 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.

5.3 Seleccionar un destino

Importante *Algunas de las funciones descritas en esta sección se introdujeron en la versión 12.5, que afecta solo a las implementaciones en una instalación. Estas funciones todavía no están disponibles en las implementaciones en la nube. Para obtener más información, consulte* *"Novedades en Acronis Backup" (pág. 8).*

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, `\\example.company.com\shared\files`.

  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.

  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 "Información sobre Acronis Cyber Infrastructure" (pág. 102).

- **Carpeta NFS** (disponible para equipos que ejecutan Linux o macOS)

  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" (pág. 99).

- **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

Nota *Esta funcionalidad solo está disponible con la licencia de Acronis Backup Advanced.*

- **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 copias de seguridad, 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 **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.

  Ejemplo. El siguiente script de JScript da como resultado la ubicación de copia de seguridad de un equipo en el formato **\\bkpsrv**<nombre del equipo>:

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

  De ese modo, las copias de seguridad de cada equipo se guardarán en una carpeta con el mismo nombre en el servidor **bkpsrv**.

- **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" (pág. 322).

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 ANS de Acronis**

  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" (pág. 314).

5.3.1 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.

Motivos para 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.
- Secure Zone no admite el formato de copia de seguridad de archivo único (pág. 341). Al cambiar el destino a Secure Zone en un plan de copias de seguridad que tiene el esquema de copias de seguridad **Siempre incremental (archivo único)**, este cambia a **Completas semanalmente, incrementales diariamente**.

Cómo la creación de Secure Zone transforma el disco

- Secure Zone siempre se crea al final del disco duro.
- 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.*

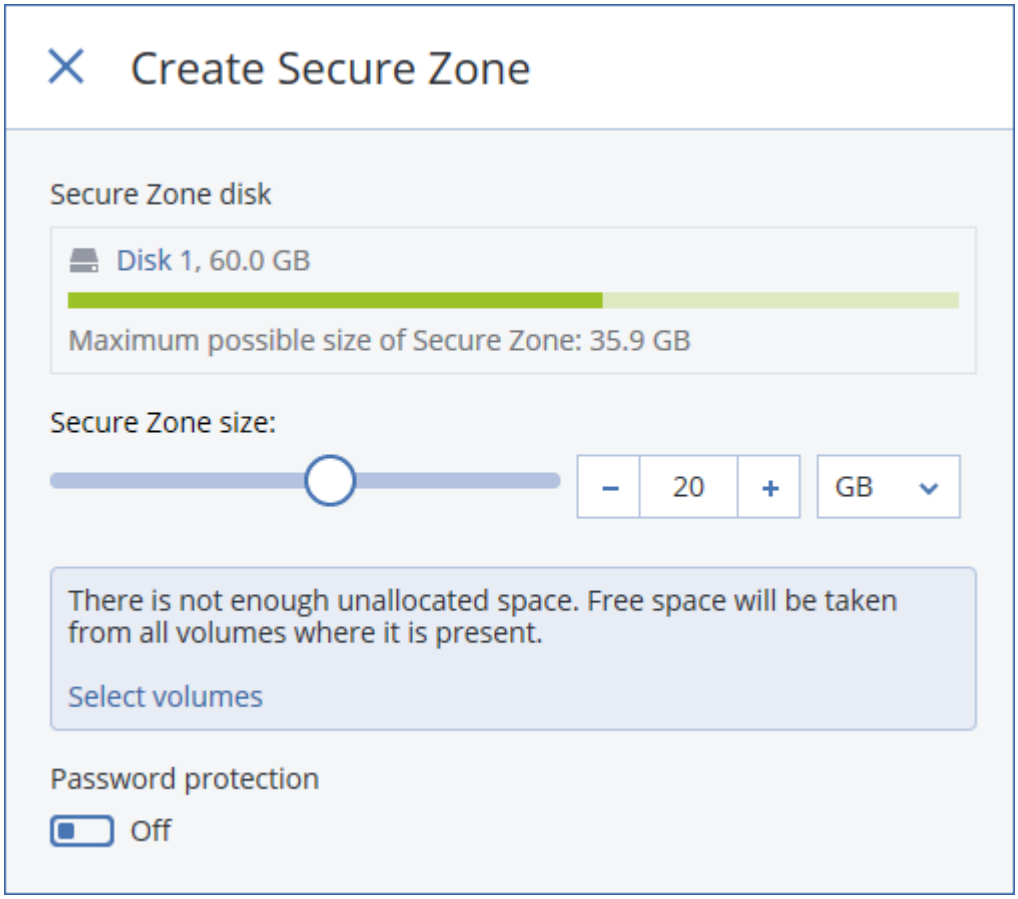
Cómo crear Secure Zone

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. Indique el tamaño de Secure Zone o arrastre el deslizador para seleccionarlo 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 dispositivo 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 copias de seguridad.

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 después, haga clic en **Eliminar**.
4. [Opcional] Seleccione los volúmenes a los que desea agregar el espacio liberado de la zona. De manera predeterminada, se seleccionan todos los volúmenes.

   El espacio se distribuirá a partes iguales entre los volúmenes seleccionados. Si no selecciona ningún volumen, el espacio liberado se convertirá en espacio sin asignar.

   Para cambiar el tamaño del volumen desde el que se arranca el sistema, es necesario reiniciar.

5. Haga clic en **Eliminar**.

Como resultado, se eliminan Secure Zone y todas las copias de seguridad almacenadas en ella.

5.3.2 Acerca de Acronis Cyber Infrastructure

Acronis Backup 12.5, a partir de la actualización 2, admite la integración con Acronis Storage 2.3, o sus versiones posteriores, llamadas Acronis Cyber Infrastructure.

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 una 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 Backup. 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 Acronis 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 (pág. 228) y gestiónelo mediante la consola de copia de seguridad.

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 cloud. La única diferencia es que las copias de seguridad pueden replicarse *desde* Acronis Cyber Infrastructure durante la ejecución de un plan de copias de seguridad.

Documentación

Toda la documentación de Acronis Cyber Infrastructure está disponible en el sitio web deAcronis.

5.4 Programar

Importante *Algunas de las funciones descritas en esta sección se introdujeron en la versión 12.5, que afecta solo a las implementaciones en una instalación. Estas funciones todavía no están disponibles en las implementaciones en la nube. Para obtener más información, consulte "Novedades en Acronis Backup" (pág. 8).*

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 copias de seguridad 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 la sección "Programar por eventos" (pág. 105).

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 copias de seguridad que incluye la planificación de copias de seguridad y los métodos de copias de seguridad.

En el **esquema de copias de seguridad**, seleccione una de las siguientes opciones:

- [Solo para copias de seguridad a nivel de disco] **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 (pág. 341).

Este esquema no está disponible al hacer una copia de seguridad en un dispositivo de cintas, un servidor SFTP o Secure Zone.

- **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.

  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 de planes de copias de seguridad.

- **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 la sección "Programar por eventos" (pág. 105).

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 la sección "Condiciones de inicio" (pág. 107).
- 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.

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 copias de seguridad en el equipo y permanece igual hasta que se edita el plan de copias de seguridad y se modifica el valor máximo de demora.

Nota: *Esta opción está habilitada de forma predeterminada en las implementaciones en la cloud, 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.*

- 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 en equipos que ejecuten Windows. Esta opción no se aplica si el equipo está apagado, es decir, no utiliza la funcionalidad Wake-on-LAN.

5.4.1 Planificación por eventos

Cuando se configura una programación para un plan de copias de seguridad, 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 copias de seguridad. Puede especificar la duración.
- **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 (pág. 106).

En la siguiente tabla se muestran los eventos disponibles para diversos datos en Windows, Linux y macOS.

DE QUÉ REALIZAR COPIAS DE SEGURIDAD	En 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 Office 365	Windows	–	–	–	–	Windows
Buzones de correo y bases de datos de Exchange	Windows	–	–	–	–	Windows
Bases de datos SQL	Windows	–	–	–	–	Windows

5.4.1.1 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 copia de seguridad 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 duro.

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 suceso

Especifica el origen del suceso que, por lo general, indica qué programa o componente del sistema generó el suceso. Por ejemplo: **disco**

Tipo de suceso

Especifica el tipo de suceso: **Error**, **Advertencia**, **Información**, **Auditoría correcta** o **Error en auditoría**.

Id. suceso

Especifica el número del suceso, que suele identificar los tipos de sucesos en particular entre sucesos del mismo origen.

Por ejemplo, un suceso **Error** con Origen de suceso **disco** e Id. suceso **7** ocurre cuando Windows descubre un bloque dañado en un disco, mientras que un suceso **Error** con Origen de suceso **disco** e Id. suceso **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 copia de seguridad para copiar datos del disco duro 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****.*

5.4.2 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 copias de seguridad.

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 (pág. 131). 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 Office 365	Buzones de correo y bases de datos de Exchange	Bases de datos SQL
El usuario está inactivo (pág. 108)	Windows	–	–	–	–	–
El servidor de la ubicación de copia de seguridad está disponible (pág. 109)	Windows, Linux y macOS	Windows, Linux	Windows, Linux	Windows	Windows	Windows
Los usuarios cerraron la sesión (pág. 109)	Windows	–	–	–	–	–
Se adapta al intervalo de tiempo (pág. 110)	Windows, Linux y macOS	Windows, Linux	–	–	–	–
Ahorrar batería (pág. 110)	Windows	–	–	–	–	–
No iniciar con conexiones de uso medido (pág. 111)	Windows	–	–	–	–	–
No iniciar con conexiones a las siguientes redes Wi-Fi (pág. 112)	Windows	–	–	–	–	–
Comprobar dirección IP del dispositivo (pág. 112)	Windows	–	–	–	–	–

5.4.2.1 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.

5.4.2.2 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.

5.4.2.3 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.

5.4.2.4 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.

5.4.2.5 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 (pág. 131), 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.

5.4.2.6 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.

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

5.4.2.8 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**: `<inicio del intervalo de direcciones IP de VPN>`, **A**: `<fin del intervalo de direcciones IP de VPN>`.
- Condiciones de inicio de la copia de seguridad: **Esperar hasta que se cumplan las condiciones**.

Como resultado:

(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.

5.5 Reglas de retención

Importante *Algunas de las funciones descritas en esta sección se introdujeron en la versión 12.5, que afecta solo a las implementaciones en una instalación. Estas funciones todavía no están disponibles en las implementaciones en la nube. Para obtener más información, consulte "Novedades en Acronis Backup" (pág. 8).*

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 copias de seguridad. De manera predeterminada, las reglas de retención se especifican para cada conjunto de copias de seguridad (pág. 341) 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 almacenamiento en la nube, 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**

     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

- Se conservará siempre la última copia de seguridad creada mediante el plan de copias de seguridad, incluso aunque se detecte una violación a una regla de retención. No intente borrar la única copia de seguridad de la que dispone al aplicar las reglas de retención antes de realizar la copia de seguridad.
- 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" (pág. 126).
- Las reglas de retención son parte del plan de copia de seguridad. Dejan de funcionar en las copias de seguridad del equipo cuando se revoca o elimina el plan de copias de seguridad 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" (pág. 203).

5.6 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 hay forma posible de recuperar las copias de seguridad cifradas si pierde u olvida la contraseña.*

Cifrado en un plan de copias de seguridad

Para habilitar el cifrado, especifique los valores de cifrado al crear un plan de copias de seguridad. Después de aplicar un plan de copias de seguridad, los valores de cifrado ya no se pueden modificar. Para usar valores de cifrado diferentes, cree un nuevo plan de copias de seguridad.

Para especificar los valores de cifrado en un plan de copias de seguridad

1. En el panel del plan de copias de seguridad, 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 copias de seguridad, 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 copias de seguridad de la manera siguiente:

- **Planes de copias de seguridad que ya se han aplicado al equipo.** Si los ajustes de cifrado en un plan de copias de seguridad son diferentes, las copias de seguridad fallarán.
- **Planes de copias de seguridad que se aplicarán al equipo más adelante.** Los ajustes de cifrado guardados en un equipo reemplazarán los valores de cifrado en un plan de copias de seguridad. Todas las copias de seguridad se cifrarán, incluso si el cifrado está deshabilitado en la configuración de los planes de copias de seguridad.

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 copias de seguridad 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 copias de seguridad. De manera predeterminada, la ruta es **%ProgramFiles%\BackupClient** para las implementaciones en la cloud 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 copias de seguridad. De manera predeterminada, la ruta es **%ProgramFiles%\BackupClient** para las implementaciones en la cloud y **%ProgramFiles%\Acronis** para las implementaciones locales.
   - En Linux: **/usr/sbin/acropsh -m manage_creds --reset**

Para cambiar la configuración de cifrado mediante Backup Monitor:

1. Inicie sesión como administrador en Windows o macOS.
2. Haga clic en el icono de **Backup Monitor** en el área de notificación (en Windows) o en la barra de 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 copias de seguridad**.
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.

5.7 Notarización

Importante *Esta función se introdujo en la versión 12.5, que afecta solo a las implementaciones en una instalación. Esta función todavía no está disponible en las implementaciones en la nube. Para obtener más información, consulte "Novedades en Acronis Backup" (pág. 8).*

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 notarización 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 copias de seguridad.

Al configurar la recuperación, los archivos notarizados se marcarán con un icono especial y podrá verificar la autenticidad del archivo (pág. 168).

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.

5.8 Conversión a equipo virtual

Importante *Algunas de las funciones descritas en esta sección se introdujeron en la versión 12.5, que afecta solo a las implementaciones en una instalación. Estas funciones todavía no están disponibles en las implementaciones en la nube. Para obtener más información, consulte "Novedades en Acronis Backup" (pág. 8).*

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 copias de seguridad** (pág. 119)

    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** (pág. 209)

    Este método permite especificar una planificación de la conversión independiente.

- **Recuperación a un nuevo equipo virtual** (pág. 159)

  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 (pág. 289)).

5.8.1 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 o Hyper-V, necesitará un servidor ESXi o Hyper-V, y un agente de copia de seguridad (Agente para VMware o Agente para Hyper-V).

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	Agent for VMware	Agent for Hyper-V	Agente para Windows	Agente para Linux	Agente para Mac
VMware ESXi	+	–	–	–	–
Microsoft Hyper-V	–	+	–	–	–
VMware Workstation	+	+	+	+	–
Archivos VHDX	+	+	+	+	–

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 (pág. 209).
- Las copias de seguridad almacenadas en Secure Zone únicamente pueden convertirse mediante el agente que se ejecute en el mismo equipo.
- Las copias de seguridad que contienen volúmenes lógicos (LVM) de Linux se pueden convertir únicamente si las ha creado Agente para VMware o Agente para Hyper-V 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. El equipo solo puede ser permanente en ESXi.

5.8.2 Conversión a un equipo virtual en un plan de copias de seguridad

Puede configurar la conversión a un equipo virtual desde cualquier ubicación de copia de seguridad o replicación presente en un plan de copias de seguridad. 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" (pág. 117).

Pasos para configurar una conversión a un equipo virtual en un plan de copias de seguridad

1. Decida desde qué ubicación de copia de seguridad desea realizar la conversión.
2. En el panel del plan de copias de seguridad, 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**.

5.8.3 Cómo funciona la conversión regular a equipos virtuales

La forma en la que las conversiones repetidas funcionan depende de en dónde decide crear el equipo virtual.

- **Si escoge guardar el equipo virtual como un conjunto de archivos:** cada conversión recrea el equipo virtual desde cero.

- **Si escoge crear el equipo virtual en un servidor de virtualización:** al convertir una copia de seguridad incremental o diferencial, el software actualiza 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.

5.9 Replicación

Importante *Algunas de las funciones descritas en esta sección se introdujeron en la versión 12.5, que afecta solo a las implementaciones en una instalación. Estas funciones todavía no están disponibles en las implementaciones en la nube. Para obtener más información, consulte "Novedades en Acronis Backup" (pág. 8).*

En esta sección se describe la réplica de copia de seguridad como una parte del plan de copias de seguridad. Para obtener más información acerca de la creación de un plan de replicación independiente, consulte "Procesamiento de datos fuera del host" (pág. 205).

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 de 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 copias de seguridad, haga clic en **Añadir ubicación**.

   El control **Añadir ubicación** solo se muestra si la replicación es compatible *con* la última ubicación 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" (pág. 113).
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" (pág. 117).
5. [Opcional] Repita los pasos del 1 al 4 para todas las ubicaciones en que desee replicar las copias de seguridad. Se admiten hasta cinco ubicaciones consecutivas (incluyendo la principal).

5.9.1 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" (pág. 205).

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.

5.10 Iniciar una copia de seguridad manualmente

1. Seleccione un equipo que tenga como mínimo un plan de copias de seguridad aplicado.
2. Haga clic en **Copia de seguridad**.
3. Si se le aplica más de un plan de copia de seguridad, seleccione el plan de copias de seguridad.
4. Realice uno de los siguientes procedimientos:
   - Para ejecutar una copia de seguridad incremental, haga clic en **Ejecutar ahora**. Esta es la única opción si el destino de la copia de seguridad es el almacenamiento en la nube.
   - Para ejecutar una copia de seguridad completa, haga clic en la flecha del botón **Ejecutar ahora** y, a continuación, seleccione **Completa**.
   - Para ejecutar una copia de seguridad diferencial, haga clic en la flecha del botón **Ejecutar ahora** y seleccione **Diferencial**. Esta opción solo aparece si se cumplen las siguientes condiciones simultáneamente:
     - El esquema de copias de seguridad es **Personalizada** o Abuelo-Padre-Hijo (**GFS**).

- No se ha configurado ninguna replicación al almacenamiento en la cloud.

La primera copia de seguridad creada por un plan de copias de seguridad siempre es completa.

El progreso de la copia de seguridad se muestra en la columna **Estado** del equipo.

5.11 Opciones de copia de seguridad

Importante *Algunas de las funciones descritas en esta sección se introdujeron en la versión 12.5, que afecta solo a las implementaciones en una instalación. Estas funciones todavía no están disponibles en las implementaciones en la nube. Para obtener más información, consulte "Novedades en Acronis Backup" (pág. 8).*

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 copias de seguridad 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	Windows
Alertas (pág. 126)	+	+	+	+	+	+	+	+	+
Consolidación de la copia de seguridad (pág. 126)	+	+	+	+	+	+	+	+	-
Nombre del archivo de la copia de seguridad (pág. 127)	+	+	+	+	+	+	+	+	+
Formato de la copia de seguridad (pág. 130)	+	+	+	+	+	+	+	+	+
Validación de la copia de seguridad (pág. 131)	+	+	+	+	+	+	+	+	+
Condiciones de inicio de la copia de seguridad (pág. 131)	+	+	-	+	+	-	+	+	+
Seguimiento de bloques modificados (CBT) (pág. 132)	+	-	-	-	-	-	+	+	+
Modo de copia de seguridad de clústeres (pág. 132)	-	-	-	-	-	-	-	-	+
Tasa de compresión (pág. 134)	+	+	+	+	+	+	+	+	+
Notificaciones por correo electrónico (pág. 134)	+	+	+	+	+	+	+	+	+
Manejo de errores (pág. 135)									
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 (pág. 136)	+	+	+	-	-	-	-	-	-
Filtros de archivo (pág. 136)	+	+	+	+	+	+	+	+	-
Instantánea de la copia de seguridad a nivel de archivo (pág. 138)	-	-	-	+	+	+	-	-	-
Truncamiento de registros (pág. 138)	-	-	-	-	-	-	+	+	Solo SQL
Toma de instantáneas de LVM (pág. 139)	-	+	-	-	-	-	-	-	-

	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	Windows
Puntos de montaje (pág. 139)	-	-	-	+	-	-	-	-	-
Instantánea multivolumen (pág. 140)	+	+	-	+	+	-	-	-	-
Ventana de copia de seguridad y rendimiento (pág. 140)	+	+	+	+	+	+	+	+	+
Envío de datos físicos (pág. 143)	+	+	+	+	+	+	+	+	-
Comandos previos/posteriores (pág. 144)	+	+	+	+	+	+	+	+	+
Comandos previos o posteriores a la captura de datos (pág. 146)	+	+	+	+	+	+	-	-	+
Instantáneas de hardware SAN (pág. 148)	-	-	-	-	-	-	+	-	-
Planificación (pág. 149)									
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 (pág. 149)	+	+	-	-	-	-	+	+	-
División (pág. 150)	+	+	+	+	+	+	+	+	+
Gestión de cintas (pág. 150)	+	+	+	+	+	+	+	+	+
Manejo de fallos de la tarea (pág. 153)	+	+	+	+	+	+	+	+	+
Volume Shadow Copy Service (VSS) (pág. 154)	+	-	-	+	-	-	-	+	+
Volume Shadow Copy Service (VSS) para equipos virtuales (pág. 155)	-	-	-	-	-	-	+	+	-
Copia de seguridad semanal (pág. 155)	+	+	+	+	+	+	+	+	+
Registro de eventos de Windows (pág. 155)	+	-	-	+	-	-	+	+	+

5.11.1 Alertas

No se realizan copias de seguridad correctamente durante un número especificado de días

El preajuste es: **Deshabilitado**.

Esta opción determina si se debe crear una alerta cuando el plan de copias de seguridad no ha realizado una copia 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.

5.11.2 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: **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 (pág. 130) 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 la 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.

5.11.3 Nombre del archivo de la copia de seguridad

Esta opción define los nombres de los archivos de copia de seguridad creados por el plan de copias de seguridad.

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 copias de seguridad crea un archivo o varios en la ubicación de la copia de seguridad, dependiendo de qué esquema de copias de seguridad y qué formato de copia de seguridad (pág. 130) se utilice. La tabla que aparece a continuación incluye los archivos que se pueden crear por equipo o buzón de correo.

	Siempre incremental (un archivo)	**Otros esquemas de copia de seguridad**
Formato de copia de seguridad **versión 11**	Un archivo .tib y otro archivo de metadatos .xml	Varios archivos .tib y un archivo de metadatos .xml (formato 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 copias de seguridad.

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 el programa del plan de copias de seguridad.

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 **Copias de seguridad**.

¿Dónde se ven los nombres del archivo de copia de seguridad?

Seleccione la pestaña **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 **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

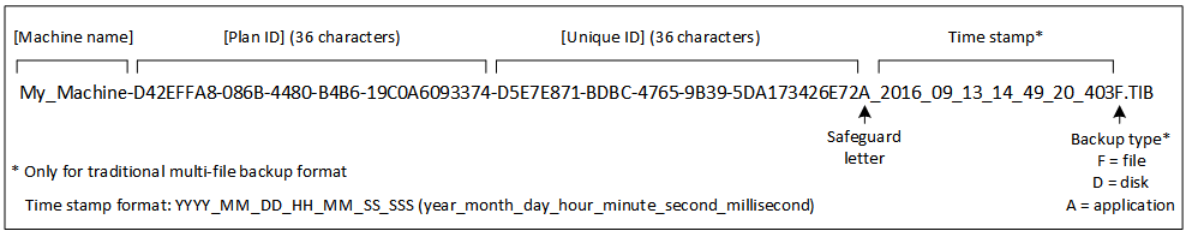
Se restaurará copia de seguridad file name is **`[Machine Name]-[Plan ID]-[Unique ID]A`**.

Se restaurará copia de seguridad file name for buzón de correo copia de seguridad is **`[Mailbox ID]_mailbox_[Plan ID]A`**.

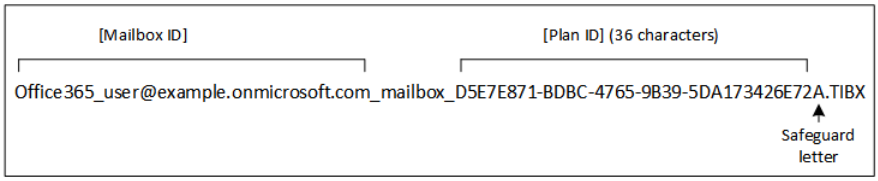
El nombre consta de las variables siguientes:

- **`[Machine Name]`** Esta variable se sustituye por el nombre del equipo (el mismo nombre que aparece en la consola de copia de seguridad) para todos los tipos de datos incluidos en la copia de seguridad, salvo los buzones de correo de Office 365. En el caso de los buzones de correo de Office 365, se sustituye por el nombre principal del usuario del buzón de correo (UPN, por sus siglas en inglés).
- **`[Plan ID]`** Este variable is replaced con a único identificador of a plan de copias de seguridad. 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 seleccionado. Si se cambia el nombre del equipo o el UPN del buzón de correo, el valor no cambiará.
- **`[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 copias de seguridad.

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 Acronis Backup. 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

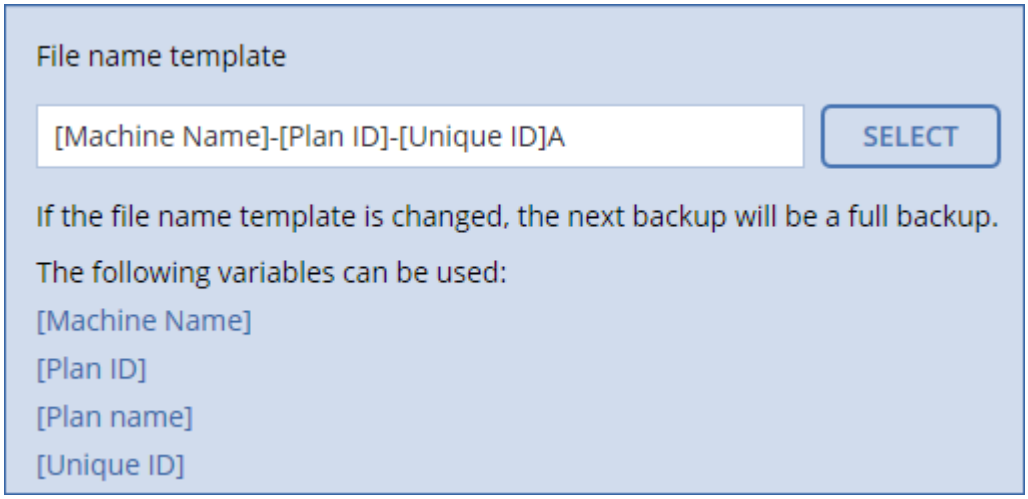
- **Ver nombres de archivo sencillos**

  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 copias de seguridad a un solo equipo y tiene que eliminar este equipo de la consola de copia de seguridad, o bien 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 copia de seguridad para que continúe realizando la misma copia de seguridad o la secuencia de copias de seguridad. Simplemente elija esta opción, haga clic en **Seleccionar** y seleccione la copia de seguridad pertinente.

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 copias de seguridad. No es posible buscar nada fuera de esta ubicación.



- **Actualizar desde las versiones de productos anteriores**

  Si durante la actualización un plan de copias de seguridad no se migra de forma automática, 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.

5.11.4 Formato de la copia de seguridad

Esta opción define el formato de las copias de seguridad creadas por el plan de copias de seguridad. Puede elegir entre el nuevo formato (**versión 12**), diseñado para realizar copias de seguridad y recuperarlas más rápidamente, y el formato antiguo (**versión 11**), que se conserva para la compatibilidad con versiones anteriores y los casos especiales. Después de aplicar un plan de copias de seguridad, no se puede modificar esta opción.

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: **Selección automática**.

Puede seleccionar una de las siguientes opciones:

- **Selección automática**

  Se usará la versión 12, salvo que el plan de copias de seguridad 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**

Se utilizará un formato antiguo en un nuevo plan de copias de seguridad que añada copias de seguridad a las ya creadas por las versiones de productos 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 la copia de seguridad (o un destino de replicación) es una ubicación gestionada con la deduplicación habilitada. Si cambia el formato a la **versión 12**, no será posible realizar las copias de seguridad.

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 (pág. 127). La tabla que aparece a continuación incluye los archivos que se pueden crear por equipo o buzón de correo.

	Siempre incremental (un archivo)	**Otros esquemas de copia de seguridad**
Formato de copia de seguridad **versión 11**	Un archivo .tib y otro archivo de metadatos .xml	Varios archivos .tib y un archivo de metadatos .xml (formato 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)	

5.11.5 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 copias de seguridad se valida justo después de su creación.

El valor predeterminado es: **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 (pág. 267) en el entorno de ESXi o Hyper-V.

5.11.6 Condiciones de inicio de la copia de seguridad

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 de copia de seguridad 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" (pág. 107).

El valor predeterminado es: **Esperar hasta que se cumplan las condiciones**.

Esperar hasta que se cumplan las condiciones

Con esta configuración, el programador empieza a supervisar las condiciones e inicia la copia de seguridad en cuanto se cumplan las condiciones. Si nunca se cumplen las condiciones, jamás se iniciará 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. Marque la casilla de verificación **Iniciar la copia de seguridad de todos modos después de** y especifique el intervalo de tiempo. La copia de seguridad comenzará tan pronto como se cumplan las condiciones o pase el período máximo de tiempo, lo que suceda primero.

Omitir la copia de seguridad planificada

El retraso de una copia de seguridad puede ser inadmisible, por ejemplo, cuando necesite realizar una copia de seguridad estrictamente a la hora especificada. Parece lógico omitir la copia de seguridad en lugar de esperar a que se cumplan las condiciones, especialmente si las copias de seguridad se producen con relativa frecuencia.

5.11.7 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: **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.

5.11.8 Modo de copia de seguridad de clústeres

Esta opción es eficaz para las copias de seguridad de nivel de la base de datos de Microsoft SQL Server y Microsoft Exchange Server.

Estas opciones son eficaces solo si se selecciona el propio clúster (Grupos de disponibilidad de AlwaysOn de Microsoft SQL Server [AAG] o el grupo de disponibilidad de base de datos de Microsoft Exchange Server [DAG]) para la copia de seguridad, en lugar de los nodos concretos o las bases de datos que tiene. Si selecciona elementos concretos del clúster, la copia de seguridad no será compatible con el clúster y solo se incluirán en la copia de seguridad las copias seleccionadas de los elementos.

Microsoft SQL Server

Esta opción determina el modo de copia de seguridad para los grupos de disponibilidad de AlwaysOn (AAG) de SQL Server. Para que se realice la operación, Agent for SQL debe estar instalado en todos los nodos de los AAG. Para obtener más información acerca de cómo realizar la copia de seguridad de los grupo de disponibilidad de AlwaysOn, consulte "Protección de los grupos de disponibilidad AlwaysOn (AAG)" (pág. 242).

El valor predeterminado es: **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 desactivadas, 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 desconectadas, 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 desconectada, 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)" (pág. 244).

El valor predeterminado es: **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 del servidor Exchange 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.

5.11.9 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** y **Alto**.

El preajuste es: **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.

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.

5.11.10 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: **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" (pág. 329).

Importante *El hecho de cambiar la configuración del sistema afecta a todos los planes de copias de seguridad que usan esta configuración.*

Antes de habilitar esta opción, asegúrese de que se han configurado los ajustes del **Servidor de correo electrónico** (pág. 330).

Para personalizar las notificaciones por correo electrónico en un plan de copias de seguridad

1. Seleccione **Personalizar los ajustes de este plan de copias de seguridad**.
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 la 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 a la 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.

5.11.11 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 preajuste es: **Habilitado. Cantidad 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 sea exitosa 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 sólo 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 nube

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 preajuste es: **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 preajuste es: **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 preajuste es: **Habilitado. Cantidad 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 sea exitosa o se realice el número de intentos especificados, lo que suceda primero.

5.11.12 Copias de seguridad incrementales/diferenciales rápidas

Esta opción es eficaz para las copias de seguridad incrementales y diferenciales a nivel de disco.

El valor predeterminado: **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.

5.11.13 Filtros de archivo

Los filtros de archivo determinan los archivos y las carpetas que se van a excluir durante el proceso de 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.

Para habilitar los filtros de archivo:

1. Seleccione los datos de los cuales quiere realizar la copia de seguridad.
2. Haga clic en el icono de engranaje que se encuentra al lado del nombre del plan de la copia de seguridad y, a continuación, haga clic en **Opciones de copia de seguridad**.
3. Seleccione **Filtros de archivo**.
4. Use cualquiera de las opciones que se especifican a continuación.

Excluya los archivos que cumplan con 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*** *(pág. 130) y el destino de la copia de seguridad no es un almacenamiento en la cloud.*

- **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**).

- **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**.

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**).

Consejo: *Puede ver los atributos de los archivos o carpetas en las propiedades de archivo/carpeta o usando el comando attrib. Para obtener más información, consulte el Centro de Soporte Técnico y Ayuda de Windows.*

5.11.14 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 *La copia de seguridad de los archivos almacenados en las redes compartidas siempre se realiza uno a uno.*

El valor predeterminado es:

- 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.

5.11.15 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: **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.

5.11.16 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: **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.

5.11.17 Puntos de montaje

Esta opción es solo eficaz en Windows para la copia de seguridad a nivel de archivos de un origen de datos que incluye volúmenes montados o volúmenes de clúster compartido.

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 **(pág. 177)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 **(pág. 177)Puntos de montaje**.

El valor predeterminado: **Deshabilitado**.

Consejo. *Puede realizar copias de seguridad de equipos virtuales de Hyper-V virtual en un volumen de clúster compartido al realizar la copia de seguridad de los archivos necesarios o de todo el volumen con la copia de seguridad a nivel de archivos. 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 crear una copias de seguridad 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 **(pág. 177)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 ara 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**.

5.11.18 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" (pág. 138) 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:

- 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 copias de seguridad 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.

5.11.19 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 copias de seguridad. 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 copias de seguridad (validación y conversión a un equipo virtual) se ejecutarán independientemente de si esta opción está habilitada.

El valor predeterminado es:**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.

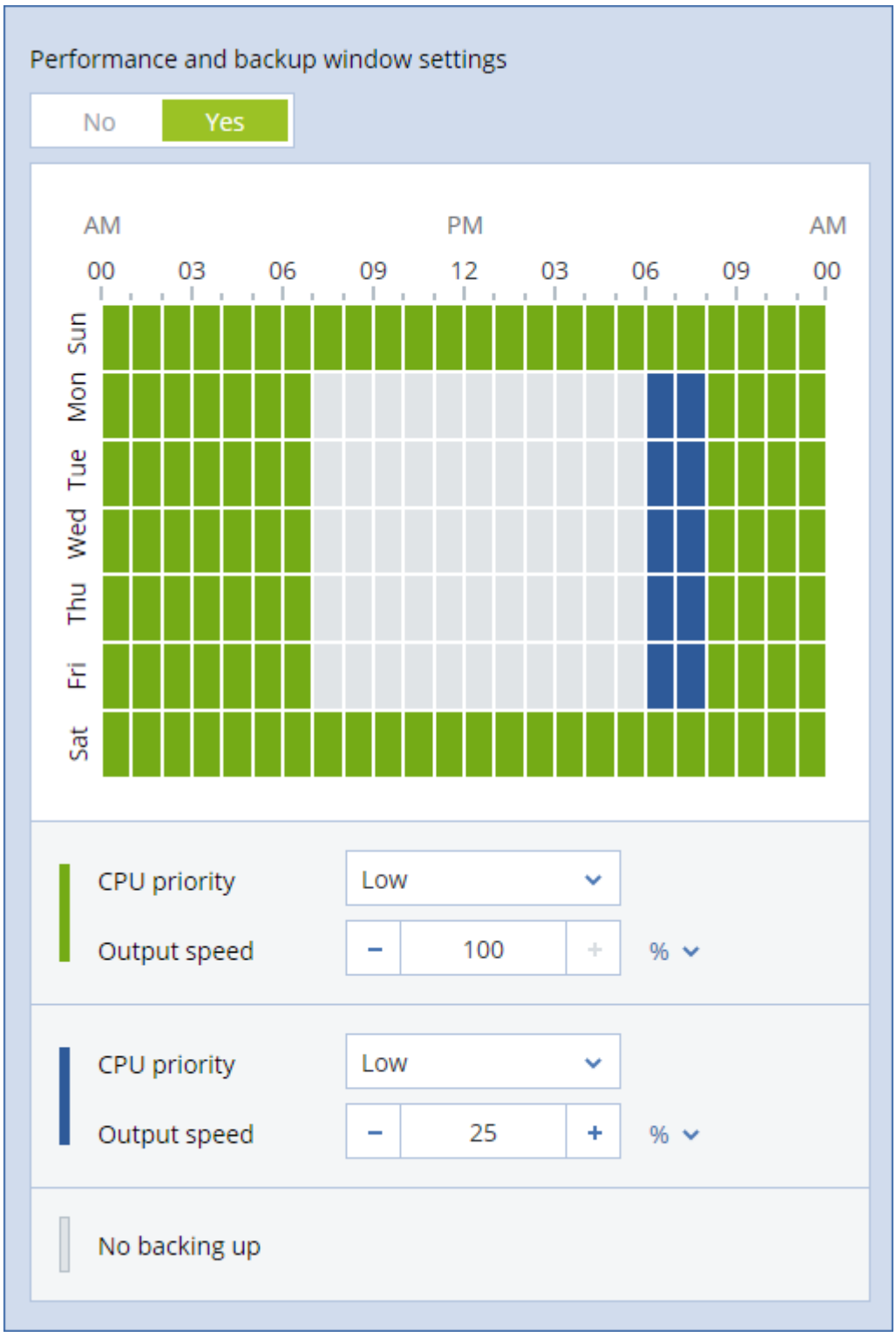
Ventana de copias de seguridad

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

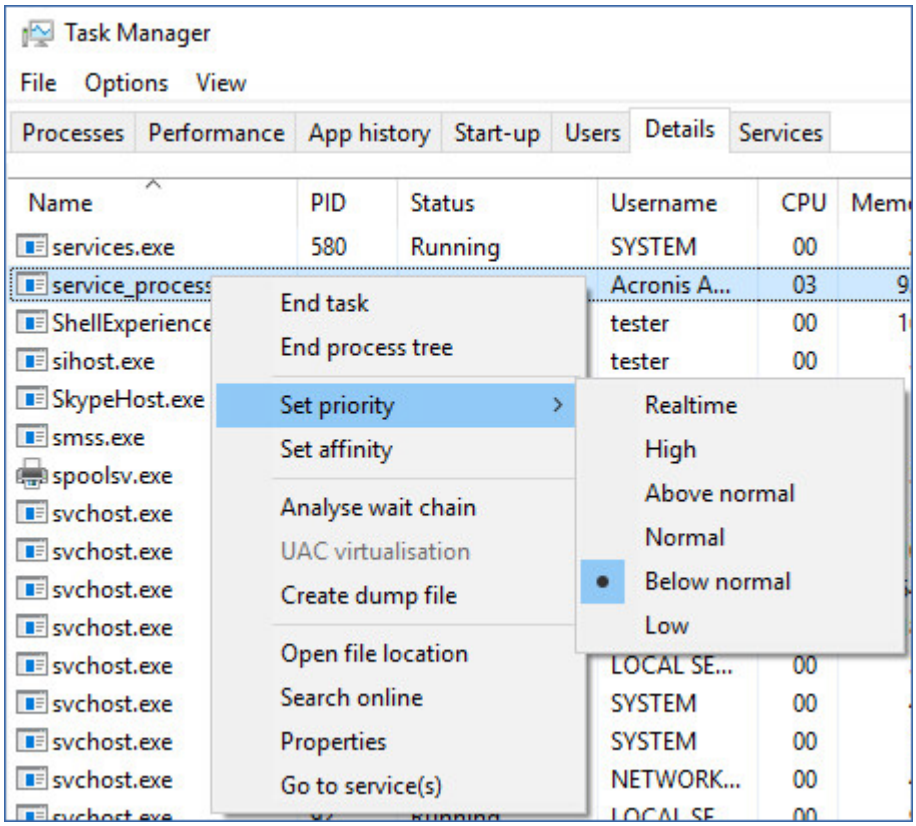
Este parámetro define la prioridad del proceso de copia de seguridad en el sistema operativo.

Los ajustes disponibles son: **Baja**, **Normal**, **Alta**.

La prioridad de un proceso que se ejecute en un sistema determina la cantidad de uso de la CPU y los recursos del sistema que se asignan a dicho proceso. La disminución de la prioridad de la copia de

seguridad liberará más recursos para otras aplicaciones. El aumento de la prioridad podría acelerar el proceso de copia de seguridad al solicitar que el sistema operativo asigne más recursos, como CPU, a la aplicación de copia de seguridad. Sin embargo, el efecto resultante dependerá del uso total de CPU y otros factores, como la velocidad de salida o entrada del disco, o el tráfico en la red.

Esta opción define la prioridad de un proceso de copia de seguridad (**service_process.exe)** en Windows y la perfección de este proceso (**service_process)** en Linux y en 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).

5.11.20 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 (pág. 130) está establecido en la **Versión 12**.

Esta opción se aplica a las copias de seguridad de discos y archivos creadas por el agente para Windows, Linux, Mac, VMware, Hyper-V y Virtuozzo. 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 copias de seguridad se enviará al almacenamiento en la cloud 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: **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 (pág. 333) en implementaciones locales y administradores en implementaciones en el cloud.

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. Crear un nuevo plan de copia de seguridad. 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 copias de seguridad. Cualquier otro plan de copias de seguridad, 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 que siga 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.

5.11.21 Comandos pre/post

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	Crear 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 copias de seguridad copia *todas* las copias de seguridad a ubicaciones posteriores.

El agente realiza la replicación *después* de ejecutar el comando posterior a la copia de seguridad.

El programa no admite comandos interactivos, es decir, comandos que requieran la intervención del usuario (por ejemplo, “pause”).

5.11.21.1 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, “pause”).
3. En el campo **Directorio de trabajo**, especifique una ruta en donde se ejecutará el comando o archivo 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.

5.11.21.2 Comando de Post-copia de seguridad

Para especificar un comando o archivo que se ejecute después de completar la copia de seguridad

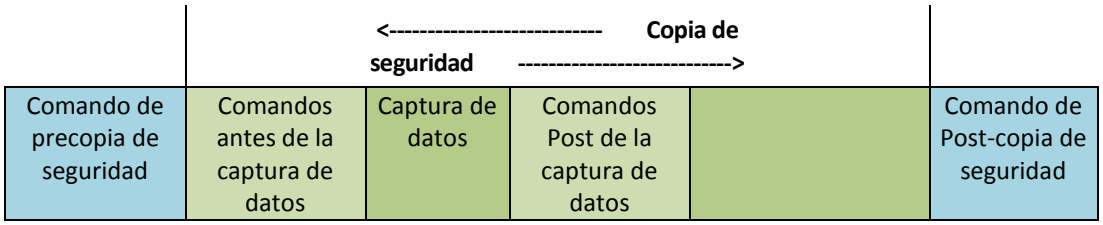
1. Habilite el conmutador **Ejecutar un comando tras la copia de seguridad**.
2. En el campo **Comando...**, escriba un comando o busque un archivo de proceso por lotes.
3. En el campo **Directorio de trabajo**, especifique la ruta del directorio donde se ejecutará el comando o archivo de proceso por 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**.

5.11.22 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.



Si la opción (pág. 154) 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:

Los comandos "Antes de la captura de datos" -> Suspensión VSS -> captura de datos -> Reanudación VSS -> comando "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.

5.11.22.1 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, "pause").
3. En el campo **Directorio de trabajo**, especifique una ruta en donde se ejecutará el comando o archivo 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 del comando.	Realizar la captura de datos después de que se ejecute el comando a pesar del éxito o fallo de la ejecución	N/D	Realizar la captura de datos al mismo tiempo que se ejecuta el comando, independientemente del resultado de la ejecución del comando.

* Un comando se considerará fallido si su código de salida no es igual a cero.

5.11.22.2 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, “pause”).
3. En el campo **Directorio de trabajo**, especifique una ruta en donde se ejecutará el comando o archivo 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 ejecute el comando correctamente.	Continúe la copia de seguridad después de que se ejecute el comando a pesar del éxito o fallo de su ejecución.	N/D	Continuar la copia de seguridad al mismo tiempo que se ejecuta el comando, independientemente del resultado de la ejecución del comando.

* Un comando se considerará fallido si su código de salida no es igual a cero.

5.11.23 Instantáneas de hardware SAN

Esta opción es eficaza para copias de seguridad de equipos virtuales VMware ESXi.

El valor predeterminado es: **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" (pág. 278).

5.11.24 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.

El preajuste es:

- Implementación en una instalación: **Iniciar todas las copias de seguridad según lo planificado.**
- Implementación 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 copias de seguridad en el equipo y permanece igual hasta que se edita el plan de copias de seguridad 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**

  Esta opción solo está disponible cuando un plan de copias de seguridad se aplica a varios equipos virtuales. Esta opción define cuántos equipos virtuales puede incluir el agente en la copia de seguridad simultáneamente al ejecutar el plan de copias de seguridad dado.

  Si, según el plan de copias de seguridad, el agente tiene que comenzar la copia de seguridad de múltiples equipos a la vez, escogerá dos equipos. (Para optimizar el rendimiento de la copia de seguridad, el agente intenta hacer coincidir los equipos almacenados en diferentes almacenamientos.) Una vez que haya finalizado las dos copias de seguridad, el agente escogerá el tercer equipo y así sucesivamente.

  Puede cambiar la cantidad de equipos virtuales que un agente incluirá en la copia de seguridad simultáneamente. El valor máximo es 10. Sin embargo, si el agente ejecuta varios planes de copias de seguridad que se superponen en el tiempo, se sumarán los números especificados en las opciones. Puede limitar el número total de equipos virtuales (pág. 290) que un agente puede incluir en la copia de seguridad al mismo tiempo, independientemente de cuántos planes de copias de seguridad se estén ejecutando.

  Las copias de seguridad de los equipos físicos empezarán exactamente según la planificación.

5.11.25 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: **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" (pág. 134) se define 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.

5.11.26 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: **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.

5.11.27 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: **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 (pág. 319), eliminan (pág. 320) 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 Vista 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 (pág. 317) 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: **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 copias de seguridad, 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: **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 copias de seguridad, 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: **Deshabilitado**.

La opción se aplica solo a unidades de cintas autónomas. Cuando esta opción está habilitada, una cinta insertada en una unidad 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 copia de seguridad.

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 copia de seguridad 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 copia de seguridad 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 copias de seguridad 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.

Usar juego de cintas en el grupo de cintas seleccionado para realizar copias de seguridad

El valor predeterminado es: **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 copias de seguridad.

También puede especificar juegos de cintas (pág. 320) 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 copias de seguridad. 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 el día respectivo de la semana.

5.11.28 Manejo de fallos de la tarea

Esta acción determina el comportamiento del programa cuando falle la ejecución planificada de un plan de copias de seguridad. Esta opción no se aplica si se inicia un plan de copias de seguridad manualmente.

Si esta opción está habilitada, el programa intentará ejecutar de nuevo el plan de copias de seguridad. 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: **Deshabilitado**.

5.11.29 Volume Shadow Copy Service (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.

El preajuste es: **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 (pág. 146) 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 preajuste es: **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 (pág. 138).

5.11.30 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: **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" (pág. 135) 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.

5.11.31 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: **Lunes**.

5.11.32 Registro de sucesos 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 eventos que quiere recopilar.

El valor predeterminado: **Deshabilitado**.

6 Recuperación

6.1 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 (pág. 157) Uso de dispositivos de arranque (pág. 162)
Equipo físico (Mac)	Uso de dispositivos de arranque (pág. 162)
Equipo virtual (VMware o Hyper-V)	Uso de la interfaz web (pág. 161) Uso de dispositivos de arranque (pág. 162)
Configuración de ESXi	Uso de dispositivos de arranque (pág. 171)
Archivos/Carpetas	Uso de la interfaz web (pág. 166) Descargar archivos del almacenamiento en la cloud (pág. 167) Uso de dispositivos de arranque (pág. 169) Extraer archivos de copias de seguridad locales (pág. 170)
Estado del sistema	Uso de la interfaz web (pág. 171)
Bases de datos SQL	Uso de la interfaz web (pág. 248)
Bases de datos de Exchange	Uso de la interfaz web (pág. 252)
Buzones de correo de Exchange	Uso de la interfaz web (pág. 254)
Buzones de correo de Office 365	Uso de la interfaz web (pág. 262)
Bases de datos de Oracle	Uso de la herramienta Oracle Explorer (pág. 264)

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.

6.2 Creación de dispositivos de inicio

El dispositivo de arranque 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 arranque es recuperar un sistema operativo que no se pueda iniciar.

Recomendamos especialmente que cree y compruebe un dispositivo de arranque en cuanto empiece a usar copias de seguridad a nivel de discos. Además, es conveniente volver a crear el dispositivo después de cada actualización importante del Agente de copias de seguridad.

Puede recuperar tanto Windows como Linux con el mismo dispositivo. Para recuperar macOS, cree un dispositivo independiente en un equipo que ejecute macOS.

Para crear dispositivos de arranque en Windows o Linux

1. Descargue el archivo ISO del 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 (pág. 210).

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 arranque.

   Aviso *Se borrará toda la información del disco.*
3. Haga clic en **Crear**.
4. Espere mientras el software crea el dispositivo de arranque.

6.3 Recuperar un equipo

6.3.1 Equipo físico

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

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

- 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.

La recuperación de un sistema operativo requiere que se reinicie. Puede elegir si reiniciar el equipo automáticamente o asignarle el estado **Interacción necesaria**. El sistema operativo recuperado se conecta a Internet automáticamente.

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 copias de seguridad (pág. 199).
- Recupere el equipo como se describe en "Recuperar discos usando dispositivos de inicio" (pág. 162).

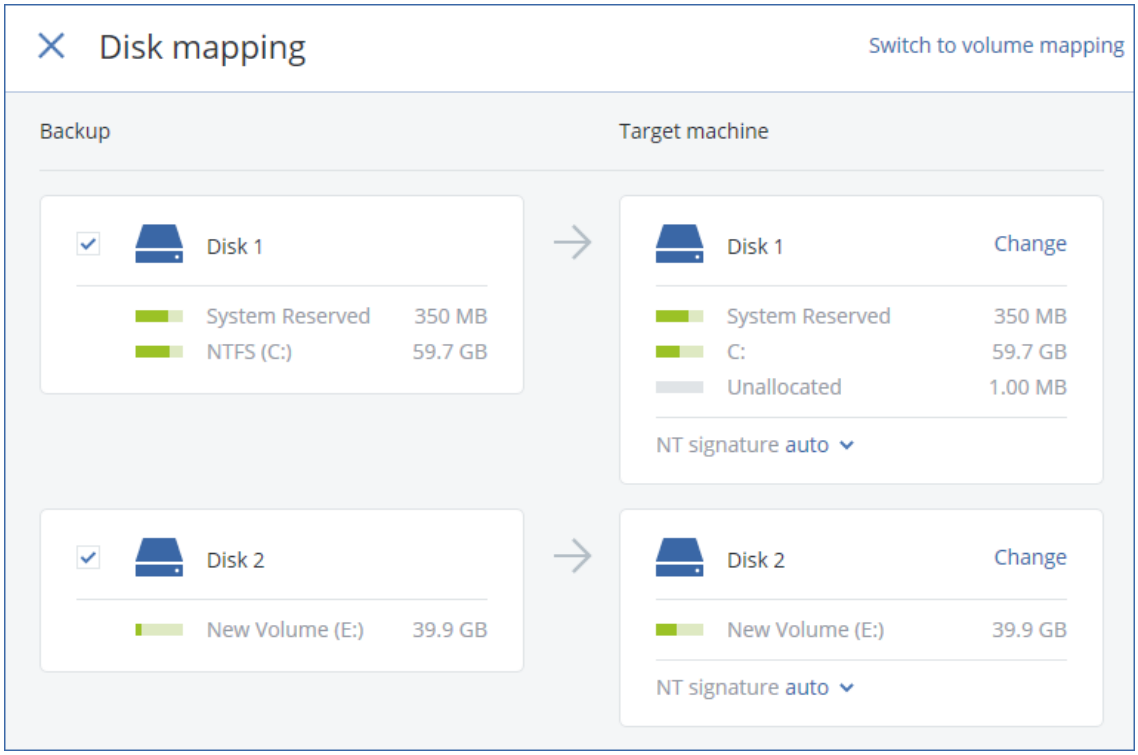
4. Haga clic en **Recuperar** > **Todo el equipo**.

   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.

La sección de asignación también permite elegir los discos individuales o volúmenes para la recuperación. Podrá cambiar entre recuperar discos y volúmenes utilizando el enlace **Cambiar a...** ubicado en la esquina posterior derecha.



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.

El proceso de recuperación se muestra en la pestaña **Actividades**.

6.3.2 De equipo físico a virtual

En esta sección se describe la recuperación de un equipo físico como equipo virtual mediante la interfaz web. Esta operación se puede realizar si hay instalado y registrado por lo menos un Agente para VMware o un Agente para Hyper-V.

Para más información sobre la migración P2V, consulte "Migración de equipos" (pág. 289).

Para recuperar un equipo físico como un equipo virtual

1. Seleccione el equipo del que se ha realizado la copia de seguridad.
2. Haga clic en **Recuperación**.
3. Seleccione un punto de recuperación. Tenga en cuenta que los puntos de recuperación se filtran por ubicación.

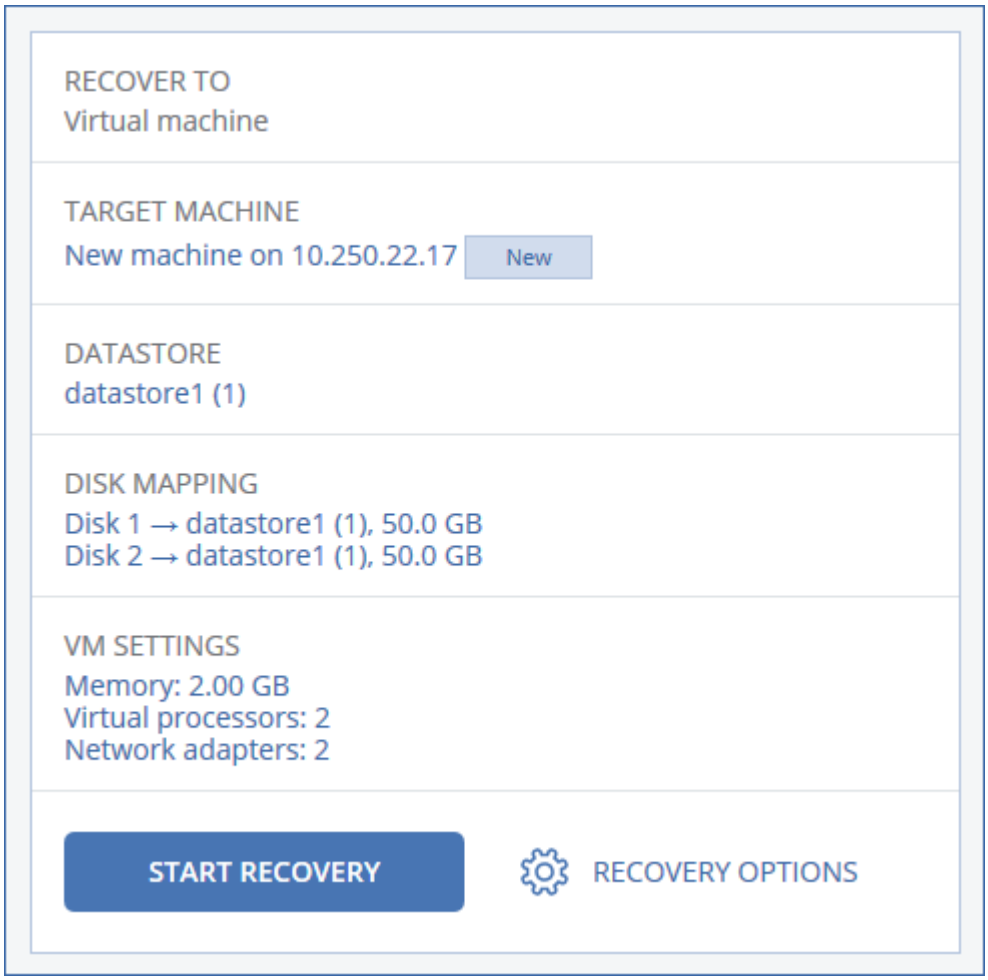
   Si el equipo no está conectado a Internet, no se muestran los puntos de recuperación. Realice una de las siguientes operaciones:

   - Si la copia de seguridad se encuentra en el almacenamiento compartido o en la cloud (es decir, otros agentes pueden acceder a ella), haga clic en **Seleccionar equipo**, seleccione un equipo que tenga conexión a Internet y, a continuación, seleccione un punto de recuperación.
   - Seleccione un punto de recuperación en la pestaña de copias de seguridad (pág. 199).

- Recupere el equipo como se describe en "Recuperar discos usando dispositivos de inicio" (pág. 162).

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 (**VMware ESXi** o **Hyper-V**).

      Debe estar instalado por lo menos un Agente para VMware o un Agente para Hyper-V.
   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. [Opcional] Al recuperar en un equipo nuevo, 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.
   - Haga clic en **Asignación de discos** para seleccionar el almacén de datos (almacenamiento), interfaz y modo de aprovisionamiento para cada unidad de disco virtual. La sección de asignación también permite elegir discos individuales para la recuperación.
   - 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 **Iniciar recuperación**.
9. Al realizar la recuperación en un equipo virtual existente, confirme que desea sobrescribir los discos.

El proceso de recuperación se muestra en la pestaña **Actividades**.

6.3.3 Equipo virtual

Durante la recuperación en un equipo virtual, éste debe permanecer detenido. El software detiene el equipo sin previo aviso. Cuando se complete la recuperación, debe iniciar el equipo manualmente.

Este comportamiento se puede cambiar utilizando la opción de recuperación de gestión de energía de VM (haga clic en **Opciones de recuperación** > **Gestión de energía de VM**).

Para recuperar un equipo virtual

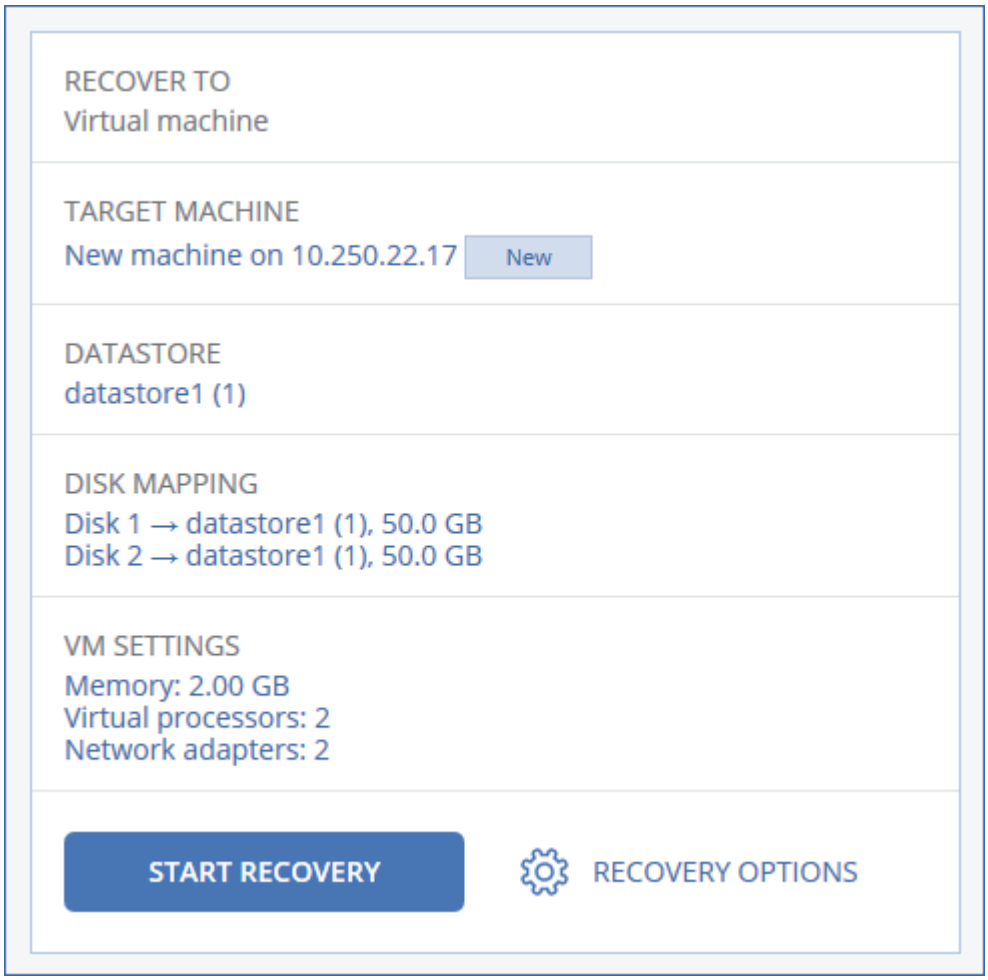
1. Realice uno de los siguientes procedimientos:
   - Seleccione un equipo incluido en la copia de seguridad, haga clic en **Recuperación** y luego seleccione un punto de recuperación.
   - Seleccione un punto de recuperación en la pestaña de copias de seguridad (pág. 199).
2. Haga clic en **Recuperar** > **Todo el equipo**.
3. Si desea recuperar el equipo virtual en un equipo físico, seleccione **Equipo físico** en **Recuperar en**. De lo contrario, omita este paso.

   La recuperación en un equipo físico solo es posible si la configuración de disco del equipo de destino coincide exactamente con la configuración de disco de la copia de seguridad.

   En caso afirmativo, siga con el paso 4 de la sección "Equipo físico" (pág. 157). En caso contrario, le recomendamos que realice la migración V2P mediante un dispositivo de arranque (pág. 162).
4. El software selecciona automáticamente el equipo original como equipo de destino.

   Para recuperar el equipo virtual en otro equipo virtual, haga clic en **Equipo de destino** y, a continuación, haga lo siguiente:
   a. Seleccione el hipervisor (**VMware ESXi** o **Hyper-V**).
   b. Seleccione si desea realizar la recuperación en un equipo nuevo o en otro ya existente.
   c. Seleccione el servidor y especifique el nuevo nombre de equipo, o bien seleccione un equipo de destino existente.
   d. Haga clic en **Aceptar**.
5. [Opcional] Al recuperar en un equipo nuevo, 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.
   - Haga clic en **Asignación de discos** para seleccionar el almacén de datos (almacenamiento), interfaz y modo de aprovisionamiento para cada unidad de disco virtual. La sección de asignación también permite elegir discos individuales para la recuperación.

- 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. Haga clic en **Iniciar recuperación**.
7. Al realizar la recuperación en un equipo virtual existente, confirme que desea sobrescribir los discos.

El proceso de recuperación se muestra en la pestaña **Actividades**.

6.3.4 Recuperar discos usando dispositivos de arranque

Para obtener información sobre cómo crear dispositivos de inicio, consulte "Crear dispositivos de arranque" (pág. 156).

Para recuperar discos usando dispositivos de arranque.

1. Inicie el equipo de destino usando dispositivos de arranque.
2. [Solo cuando se recupera un Mac] Si recupera volúmenes o discos con formato APFS a un equipo no original o en una recuperación completa, vuelva a crear la configuración del disco original manualmente:
   a. Haga clic en **Disk Utility**.
   b. 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**.

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 los discos que desea recuperar. Haga clic en **Aceptar** para confirmar su selección.
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.

    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. [Al recuperar un equipo Linux] Si el equipo incluido en la copia de seguridad tenía volúmenes lógicos (LVM) y quiere reproducir la estructura LVM original:
    a. Asegúrese de que el número y capacidad de los discos en el equipo de destino igualan o exceden los del equipo original. A continuación, haga clic en **Aplicar RAID/LVM**.
    b. Revise la estructura de volumen y luego haga clic en **Aplicar RAID/LVM** para crearla.
12. [Opcional] Haga clic en **Opciones de recuperación** para especificar configuraciones adicionales.
13. Haga clic en **Aceptar** para comenzar la recuperación.

6.3.5 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 (pág. 164).
5. Haga clic en **Aceptar**.

6.3.5.1 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 dispositivo 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 y, una vez encontrado, transmite al sistema operativo la ruta de ese controlador. 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.

6.3.5.2 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.

6.4 Recuperación de archivos

6.4.1 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 copias de seguridad (pág. 199).
   - Descargue los archivos desde el almacenamiento en la cloud (pág. 167).
   - Use dispositivos de arranque (pág. 169).
4. Haga clic en **Recuperar** > **Archivos/carpetas**.
5. Vaya hasta la carpeta requerida o utilice la 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" (pág. 136).

   Nota *Buscar no está disponible para las copias de seguridad a nivel de disco que se guardan en el almacenamiento en la nube.*
6. Seleccione los archivos que desea recuperar.
7. Si desea guardar los archivos en un archivo .zip, haga clic en **Descargar**, seleccione la ubicación en la que se guardarán los datos y, a continuación, haga clic en **Guardar**. De lo contrario, omita este paso.

   La acción de descarga no está disponible si su selección incluye carpetas o si el tamaño total de los archivos seleccionados supera los 100 MB.
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 o Agente para Hyper-V (si los archivos proceden de un equipo virtual ESXi o Hyper-V).

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
   - Una carpeta de red accesible desde el equipo de destino
10. Haga clic en **Iniciar recuperación**.
11. Seleccione una de las opciones de sobrescritura 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**.

6.4.2 Descarga de archivos desde el almacenamiento en la nube

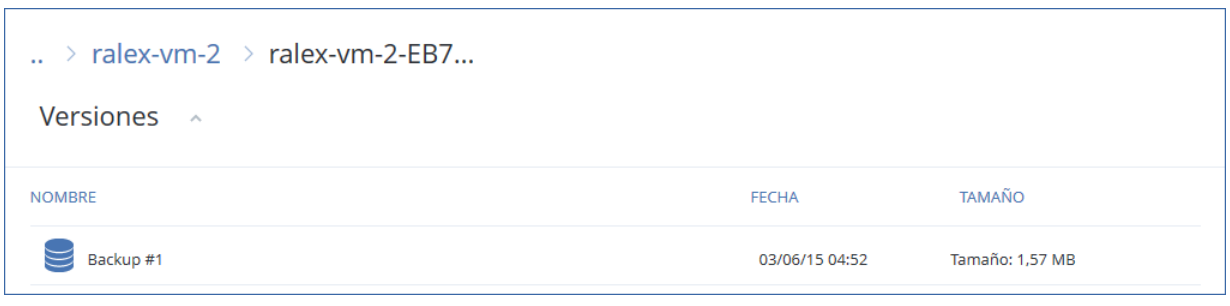
Puede explorar el almacenamiento en la nube, ver el contenido de las copias de seguridad y descargar los archivos que necesite.

Limitaciones

- No se puede explorar el estado del sistema de las copias de seguridad, las bases de datos de SQL y las bases de datos de Exchange.
- Para disfrutar de una mejor experiencia de descarga, no baje más de 100 MB a la vez. Para recuperar grandes cantidades de datos del cloud rápidamente, siga el procedimiento de recuperación de archivos (pág. 166).

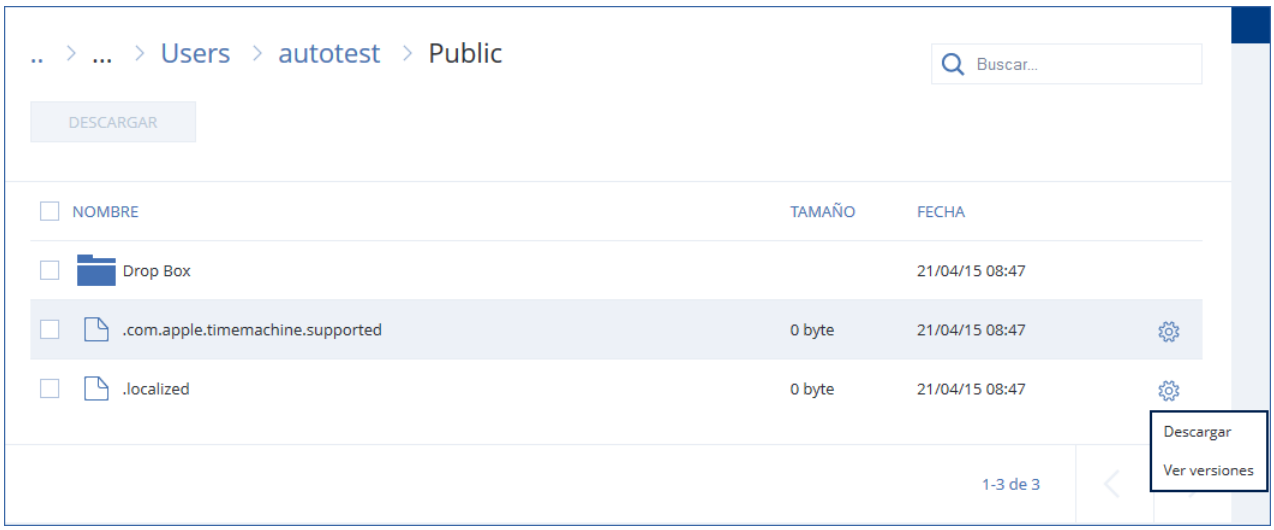
Para descargar archivos del almacenamiento en la nube

1. Seleccione un equipo del que se haya realizado una copia de seguridad.
2. Haga clic en **Recuperar** > **Otros métodos de recuperación...** > **Descargar archivos**.
3. Especifique las credenciales de la cuenta a la que está asignado el equipo del que se hizo la copia de seguridad.
4. [Cuando explore copias de seguridad a nivel de discos] En **Versiones**, haga clic en la copia de seguridad de la que desea recuperar los archivos.



[Cuando explore copias de seguridad a nivel de archivos] Puede seleccionar la fecha y hora de la copia de seguridad en el siguiente paso, bajo el icono de engranaje que se encuentra a la derecha del archivo seleccionado. De manera predeterminada, los archivos se recuperan de la última copia de seguridad.

5. Vaya hasta la carpeta requerida o utilice la búsqueda para obtener la lista de los archivos deseados.



6. Seleccione la casilla de verificación de los elementos que quiere recuperar y, a continuación, haga clic en **Descargar**.

   Si selecciona un archivo único, se descargará como tal. En cualquier otro caso, los datos seleccionados se combinan en un archivo .zip.
7. Seleccione la ubicación en la que guardar los datos y, a continuación, haga clic en **Guardar**.

6.4.3 Verificar la autenticidad del archivo con Notary Service

Si se ha habilitado la notarización durante la copia de seguridad (pág. 116), 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 web" (pág. 166).
2. Asegúrese de que el archivo seleccionado esté marcado con el icono siguiente:  . 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.

6.4.4 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" (pág. 166).
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.

6.4.5 Recuperación de archivos usando dispositivos de arranque

Para obtener información sobre cómo crear dispositivos de arranque, consulte "Crear dispositivos de arranque" (pág. 156).

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.

6.4.6 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 copias de seguridad 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:

   `<nombre del equipo> - <GUID del plan de copias de seguridad>`
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.

6.5 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**.

6.6 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" (pág. 156).

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.

6.7 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 y Hyper-V	Windows
Validación de la copia de seguridad (pág. 174)	+	+	+	+	+	+	+	+	+
Modo de arranque (pág. 174)	+	-	-	-	-	-	-	+	-
Fecha y hora de los archivos (pág. 175)	-	-	-	+	+	+	+	-	-
Manejo de errores	+	+	+	+	+	+	+	+	+
Exclusiones de archivos (pág. 176)	-	-	-	+	+	+	+	-	-
Seguridad a nivel de archivo (pág. 176)	-	-	-	+	-	-	-	-	-
Flashback (pág. 176)	+	+	+	-	-	-	-	+	-
Recuperación de ruta completa (pág. 177)	-	-	-	+	+	+	+	-	-
Puntos de montaje (pág. 177)	-	-	-	+	-	-	-	-	-
Rendimiento (pág. 177)	+	+	-	+	+	+	-	+	+
Comandos previos/posteriores (pág. 178)	+	+	-	+	+	+	-	+	+
Cambios en el identificador de seguridad (SID) (pág. 179)	+	-	-	-	-	-	-	-	-
Gestión de energía de VM (pág. 179)	-	-	-	-	-	-	-	+	-
Registro de eventos de Windows (pág. 180)	+	-	-	+	-	-	-	Solo Hyper-V	+

6.7.1 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.

El valor predeterminado: **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.

6.7.2 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: **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 Vista SP1
  - 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.

6.7.3 Fecha y hora de los archivos

Esta opción solo sirve al recuperar archivos.

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: **Habilitado**.

6.7.4 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: **Habilitado. Cantidad 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 sea exitosa 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: **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: **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.

6.7.5 Exclusiones de archivos

Esta opción solo sirve al recuperar archivos.

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.*

6.7.6 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: **Habilitado**.

Puede elegir entre recuperar los permisos o permitir que los archivos hereden los permisos NTFS de la carpeta desde donde se recuperan.

6.7.7 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 a 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**.

6.7.8 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: **Deshabilitado**.

6.7.9 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 (pág. 139) habilitada.

El valor predeterminado es: **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.*

6.7.10 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: **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.

6.7.11 Comandos pre/post

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, “pause”).

No se ejecutará un comando de recuperación posterior si la recuperación sucede como reinicio.

6.7.11.1 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, “pause”).
3. En el campo **Directorio de trabajo**, especifique una ruta en donde se ejecutará el comando o archivo 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.

6.7.11.2 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 la ruta del directorio 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.*

6.7.12 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 o Agente para Hyper-V realizan la recuperación en un equipo virtual.

El valor predeterminado es: **Deshabilitado**.

El software puede generar un identificador de seguridad único (SID del equipo) para el sistema operativo recuperado. Solo necesita esta opción para asegurar la operatividad del software de terceros que dependa del SID del equipo.

Microsoft no admite oficialmente cambios en el SID en un sistema recuperado o implementado. De modo que deberá utilizar esta opción por su cuenta y riesgo.

6.7.13 Gestión de energía de VM

Estas opciones funcionan cuando Agente para VMware o Agente para Hyper-V realizan la recuperación en un equipo virtual.

Apagar los equipos virtuales de destino al iniciar la recuperación

El valor predeterminado es: **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: **Deshabilitado**.

Después de recuperar un equipo con una copia de seguridad en otro equipo, es posible que la réplica del equipo existente aparezca en la red. Para tener seguridad, encienda el equipo virtual manualmente, después de tomar las precauciones necesarias.

6.7.14 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 eventos que quiere recopilar.

El valor predeterminado es: **Deshabilitado**.

7 Recuperación ante desastres

Importante *Esta opción está disponible solamente en las implementaciones en el cloud de Acronis Backup. Todavía no está disponible para implementaciones en una instalación.*

La funcionalidad de recuperación ante desastres le permite contar con un equipo virtual en la cloud. En el caso de que se produzca algún desastre, la carga de trabajo se puede conmutar instantáneamente (conmutada por error) desde un equipo corrupto al equipo virtual en la cloud.

Para incluir el equipo virtual en su red TCP/IP local, tiene que ampliar la red a la cloud mediante un túnel de VPN seguro. Esto se puede hacer fácilmente si se instala el dispositivo VPN que se va a usar en dos variantes: para VMware ESXi y para Hyper-V.

Una vez que la conexión VPN esté configurada y el equipo virtual, creado en la cloud, podrá acceder al equipo virtual directamente desde la consola de la copia de seguridad. También puede utilizar la conexión por escritorio remoto y SSH.

La función de recuperación ante desastres solo está disponible para el administradores de la empresa. Los administradores son los responsables de proporcionar a los usuarios acceso al equipo virtual en la cloud y de indicarles cómo acceder a equipo en caso de se produzca un desastre.

Recursos de pago controlados por cuotas

Al tener un equipo virtual en la cloud, no tendrá que preocuparse por el hardware adicional, pero sí tendrá que pagar por los recursos informáticos que consuma el equipo virtual. Entre ellos se incluyen la CPU y la RAM calculadas en puntos del equipo, el espacio del almacén de datos ocupado por los archivos del equipo virtual y una dirección IP pública, en caso necesario.

El espacio del almacén de datos se denomina "almacenamiento de recuperación ante desastres". Este rápido almacenamiento es más caro que el almacenamiento en la cloud normal en el que se almacenan las copias de seguridad. El coste del almacenamiento de recuperación ante desastres también incluye el coste de la infraestructura que se necesita para la recuperación ante desastres.

Servidores de recuperación

El equipo virtual en la cloud puede ser una copia de su servidor local, basada en las copias de seguridad del servidor almacenadas en la cloud. Este equipo se llama **servidor de recuperación**.

Un servidor de recuperación se detiene la mayoría de las veces. Lo inicia solo para probar o cuando sea necesario realizar una conmutación por error. Como los recursos de la CPU y la RAM se consumen en un periodo de tiempo relativamente corto, paga sobre todo por el almacenamiento en la cloud, en el que las copias de seguridad se conservan y sirven como reserva del almacenamiento de la recuperación ante desastres. Otras de las ventajas que ofrece un servidor de recuperación son las siguientes:

- No es necesario tener mucho conocimiento sobre el software instalado en el servidor.
- Retención de datos a largo plazo. Puede volver a un punto de recuperación que sea de hace varios años y ver los cambios en los datos o acceder a datos eliminados.
- Capacidades de recuperación adicionales. Puede recuperar el equipo o llevar a cabo una recuperación granular desde la misma copia de seguridad que se usa para la recuperación ante desastres.

Servidores principales

Otro tipo de equipo virtual en la cloud es el **servidor principal**. Es, simplemente, un servidor adicional de su red. Con este servicio puede crear un equipo virtual basado en una de las plantillas proporcionadas. La realización de un mantenimiento adicional es su responsabilidad.

Normalmente, se usa un servidor principal para la replicación de datos en tiempo real en servidores que ejecuten aplicaciones fundamentales. La replicación la configura usted mismo con herramientas nativas de la aplicación. Por ejemplo, la replicación de Active Directory o de SQL se puede configurar entre los servidores locales y el principal.

Como alternativa, un servidor principal se puede incluir en un grupo de disponibilidad AlwaysOn (AGG) o un grupo de disponibilidad de base de datos (DAG).

Ambos métodos requieren un profundo conocimiento de la aplicación y los derechos del administrador. Un servidor principal consume constantemente recursos informáticos y espacio del almacenamiento rápido de recuperación ante desastres. Necesita mantenimiento por su parte, como el control de la replicación, la instalación de actualizaciones de software y la realización de copias de seguridad. Las ventajas son los RPO y RTO mínimos con una carga mínima del entorno de producción (en comparación con la realización de copias de seguridad de servidores completos en la cloud).

Limitaciones

La recuperación ante desastres no se admite en los siguientes casos:

- Para equipos virtuales y contenedores Virtuozzo
- Para equipos Mac
- Para equipos Linux con volúmenes lógicos (LVM) o volúmenes formateados con el sistema de archivos XFS o discos sin una tabla de particiones
- Para equipos Windows con discos dinámicos
- Si las copias de seguridad del equipo original están cifradas

Un servidor de recuperación tiene una interfaz de red. Si el equipo original tiene varias interfaces de red, solo se emula una.

Los servidores en la cloud no se cifran.

7.1 Requerimientos de software

Sistemas operativos compatibles

La protección con un servidor de recuperación se ha probado para los siguientes sistemas operativos:

- Centos 6.6, 7.1, 7.2, 7.3, 7.4, 7.5 y 7.6
- Debian 9
- Ubuntu 16.04, 18.04
- Windows Server 2008/2008 R2
- Windows Server 2012/2012 R2
- Windows Server 2016 (todas las opciones de instalación, excepto Nano Server)

Los sistemas operativos de los equipos de escritorio Windows no son compatibles con las condiciones de los productos de Microsoft.

Es posible que este software funcione con otros sistemas operativos de Windows y distribuciones Linux, pero no se lo podemos asegurar.

Plataformas de virtualización compatibles

La protección de equipos virtuales con un servidor de recuperación se ha probado para las siguientes plataformas de virtualización:

- VMware ESXi 5.1, 5.5, 6.0, 6.5
- Windows Server 2008 R2 con Hyper-V
- Windows Server 2012/2012 R2 con Hyper-V
- Microsoft Hyper-V Server 2012/2012 R2
- Windows Server 2016 con Hyper-V: todas las opciones de instalación, excepto Nano Server
- Microsoft Hyper-V Server 2016
- Equipos virtuales basados en Kernel (KVM)
- Red Hat Enterprise Virtualization (RHEV) 3.6
- Red Hat Virtualization (RHV) 4.0
- Citrix XenServer: 6.5, 7.0, 7.1, 7.2
- Equipos virtuales de Azure

El dispositivo VPN se ha probado para las siguientes plataformas de virtualización:

- VMware ESXi 5.1, 5.5, 6.0, 6.5
- Windows Server 2008 R2 con Hyper-V
- Windows Server 2012/2012 R2 con Hyper-V
- Microsoft Hyper-V Server 2012/2012 R2
- Windows Server 2016 con Hyper-V: todas las opciones de instalación, excepto Nano Server
- Microsoft Hyper-V Server 2016

Puede que este software funcione con otras plataformas de virtualización y versiones distintas, pero no se lo podemos asegurar.

7.2 Configuración de una conexión VPN

Antes de crear un servidor de recuperación o uno principal, se debe establecer una conexión VPN en el sitio web de recuperación en la cloud. La conexión VPN usa dos equipos virtuales:

- Un dispositivo VPN, situado en sus instalaciones.
- Un servidor VPN, ubicado en el sitio web de recuperación en la cloud.

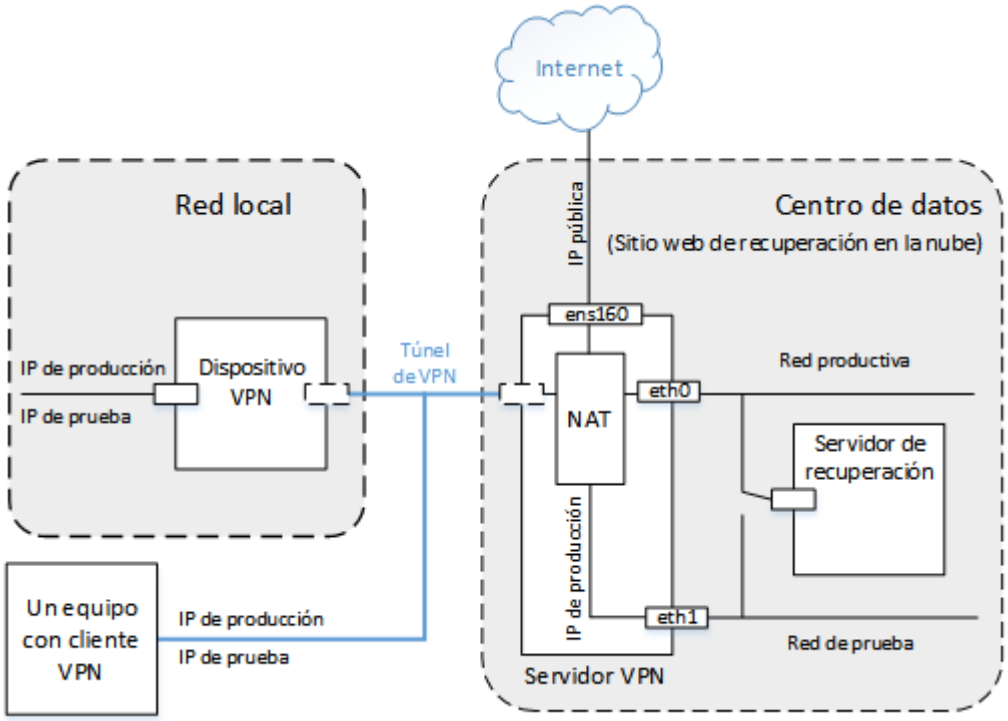
El dispositivo VPN habilita la conexión entre el sitio de recuperación en la cloud y su red local. En el caso de que la red local esté caída, podrá conectarse directamente al servidor VPN.

En el diagrama que aparece a continuación se muestran los métodos de conexión al sitio de recuperación en la cloud y las direcciones IP públicas en los modos de conmutación por error y conmutación por error de prueba.

- En el modo de conmutación por error (como se muestra), un servidor de recuperación se conecta a la red de producción y asigna la dirección IP pública.
- En el modo de conmutación por error de prueba, un servidor de recuperación se conecta a la red de prueba aislada y asigna la dirección IP pública. Sin embargo, para acceder al servidor

mediante la VPN, debe usar la dirección IP de prueba. El servidor VPN sustituye la dirección IP de prueba por la dirección IP de producción en la red de prueba.

- Si el servidor de recuperación cuenta con una dirección IP pública, también se traslada a la dirección IP de producción tanto en el modo de conmutación por error como en el de conmutación por error de prueba.



7.2.1 Requisitos del dispositivo VPN

Requisitos del sistema

- 1 CPU
- 1 GB DE RAM
- 8 GB de espacio de disco

Puertos

- TCP 443 (salida): para conexión VPN
- TCP 80 (salida): para actualizar el dispositivo automáticamente (pág. 186)

Asegúrese de que sus cortafuegos y otros componentes del sistema de seguridad de la red permiten las conexiones a través de estos puertos a cualquier dirección IP.

7.2.2 Conexión mediante el dispositivo VPN

El dispositivo VPN amplía su red local a la cloud mediante un túnel de VPN seguro. Este tipo de conexión se suele llamar conexión "de sitio a sitio" (S2S).

Pasos para configurar una conexión mediante el dispositivo VPN

1. Haga clic en **Dispositivos** > **Sitio de recuperación en la cloud**.
2. Haga clic en **Iniciar** en la página de bienvenida.

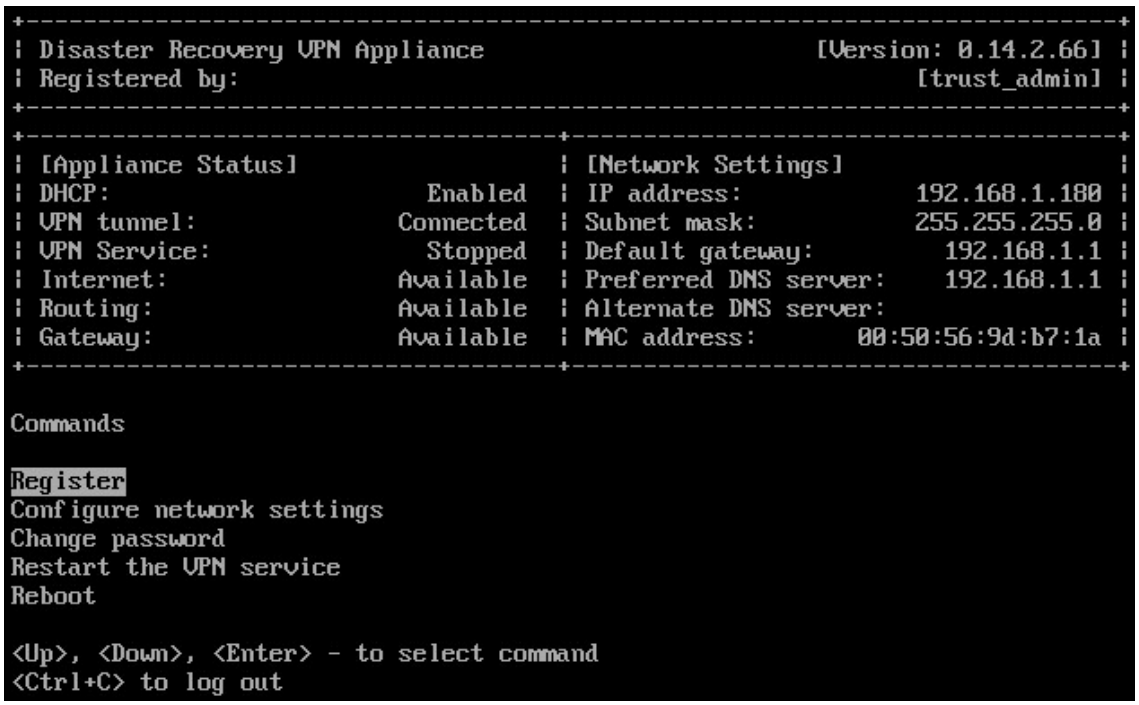
   El sistema empieza a implementar el servidor VPN en la cloud. Este proceso tardará cierto tiempo; mientras tanto, puede continuar con el siguiente paso.

Nota *El servidor VPN se proporciona sin ningún cargo adicional. Se eliminará si la funcionalidad de recuperación ante desastres no se usa, es decir, si no hay ningún servidor principal ni de recuperación en la cloud durante siete días.*

3. En función de la plataforma de virtualización que use, descargue el dispositivo VPN de VMware vSphere o Microsoft Hyper-V.
4. Implemente el dispositivo y conéctelo a la red de producción.

   En vSphere, asegúrese de que esté activado el modo **Promiscuous** y establezca en **Aceptar** todos los conmutadores virtuales que conecten el dispositivo VPN a la red de producción. Para acceder a esta configuración, en vSphere Client, seleccione el host > **Resumen** > **Red** y, a continuación, seleccione el conmutador > **Editar configuración...** > **Seguridad**.

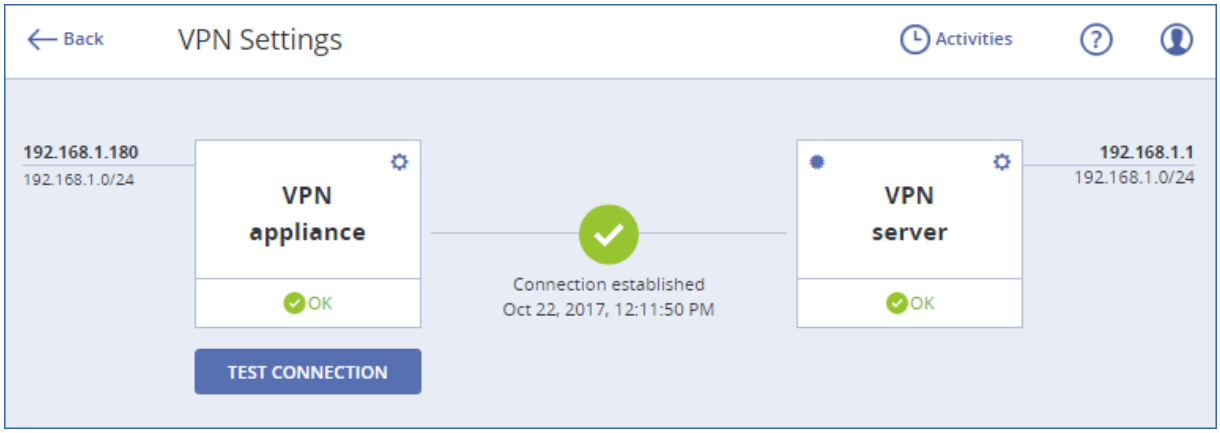
   En Hyper-V, cree un equipo virtual de 1.ª generación con 1024 MB de memoria. También le recomendamos habilitar la memoria dinámica del equipo. Cuando haya creado el equipo, vaya a **Configuración** > **Hardware** > **Adaptador de red**> **Funciones avanzadas** y marque la casilla de verificación **Habilitar el redireccionamiento de direcciones MAC**.
5. Encienda el dispositivo.
6. Abra la consola del dispositivo e inicie sesión con el usuario y la contraseña "admin"/"admin".



7. [Opcional] Cambie la contraseña.
8. [Opcional] Cambie la configuración de red. Es posible que quiera asignar el dispositivo a la dirección IP estática.
9. Use las credenciales del administrador de la empresa para registrar el dispositivo en el servicio de copias de seguridad.

   Estas credenciales solo se usan una vez para recuperar el certificado. La URL del centro de datos viene predefinida.

El dispositivo se conecta al servidor VPN. Una vez finalizada la configuración, el equipo mostrará el estado **Correcto**.



Pasos para probar la conexión VPN

1. Haga clic en **Dispositivos** > **Sitio de recuperación en la cloud**.
2. Haga clic en **Configuración de la VPN**.
3. Asegúrese de que el estado del dispositivo VPN y el servidor VPN sea **Correcto**.
4. Haga clic en **Probar**.

   El dispositivo VPN comprueba la conectividad al servidor VPN. Aparecerá la lista de pruebas que se están realizando y sus resultados.

7.2.3 Operaciones con un dispositivo VPN

En la consola de copia de seguridad (**Dispositivos** > **> Sitio de recuperación en la cloud** > **Configuración de la VPN**), puede llevar a cabo las siguientes acciones:

- Conectar o desconectar el dispositivo
- Eliminando el dispositivo del registro

Para acceder a esta configuración, haga clic en el ícono de engranaje de la imagen del dispositivo VPN:

En la consola del dispositivo puede realizar lo siguiente:

- Cambiar la contraseña del dispositivo
- Ver y cambiar la configuración de la red
- Registrar la cuenta o cambiar su registro (repitiéndolo)
- Reiniciar el servicio VPN
- Reinicie el dispositivo
- Enviar un ping a una dirección de red para solucionar los problemas

Actualización del dispositivo VPN

El dispositivo VPN busca actualizaciones automáticamente una vez al día. Cuando se detecta una nueva versión, se aplica la actualización automáticamente, sin reiniciar el servicio VPN ni detenerlo.

7.2.4 Conexión de punto a sitio

El dispositivo VPN habilita la conexión entre el sitio de recuperación en la cloud y su red local. En el caso de que la red local esté caída, podrá conectarse directamente al sitio de recuperación en la

cloud. Este tipo de conexión se suele llamar conexión "de punto a sitio" (P2S), en comparación con la conexión "de sitio a sitio" (S2S).

Pasos para establecer el nombre de usuario y la contraseña de la conexión de punto a sitio

1. En la consola de copia de seguridad (**Dispositivos** > **> Sitio de recuperación en la cloud** > **Configuración de la VPN**), haga clic en el ícono de engranaje de la imagen del servidor VPN.
2. Haga clic en **Cambiar credenciales**.
3. Cree y escriba el nombre de usuario.
4. Cree y escriba la contraseña.
5. Confirme la contraseña
6. Haga clic en **Aceptar**.

Pasos para establecer la conexión de punto a sitio

1. Instale el cliente OpenVPN en el equipo que quiera conectar al sitio de recuperación en la cloud.

   Las versiones del cliente OpenVPN admitidas son la 2.4.0 y posteriores.
2. En la consola de copia de seguridad, haga clic en **Dispositivos** > **> Sitio de recuperación en la cloud** > **Configuración de la VPN**.
3. Haga clic en el ícono de engranaje de la esquina superior derecha del servidor VPN.
4. Haga clic en **Descargar configuración para OpenVPN**.
5. Importe la configuración de OpenVPN.
6. Cuando se inicie la conexión, introduzca el nombre de usuario y la contraseña que haya establecido como se ha descrito anteriormente.

7.2.5 Parámetros de la conexión de punto a sitio

En la consola de copia de seguridad (**Dispositivos** > **> Sitio de recuperación en la cloud** > **Configuración de la VPN**), haga clic en el ícono de engranaje de la imagen del servidor VPN. El software muestra el nombre de usuario que se ha establecido para la conexión de punto a sitio y los siguientes elementos del menú.

Descargar configuración para OpenVPN

Así se descargará el archivo de configuración del cliente OpenVPN, que requiere el establecimiento de una conexión de punto a sitio al sitio web de recuperación en la cloud (pág. 186).

Cambiar credenciales

Puede cambiar el nombre de usuario o la contraseña que se usen para la conexión del punto a sitio.

Esta acción es obligatoria en los siguientes casos:

- Durante la configuración inicial de la conexión de punto a sitio (pág. 186).
- Para llevar a cabo un cambio de contraseña planificado según la política de seguridad establecida por su organización.
- Para restringir el acceso al sitio de recuperación en la cloud a ciertos usuarios (por ejemplo, antiguos empleados).

Cuando las credenciales se hayan cambiado, asegúrese de informar a los usuarios de que tienen que usar unas credenciales diferentes.

Regeneración del archivo de configuración

Puede volver a generar el archivo de configuración del cliente OpenVPN.

Esta acción es obligatoria en los siguientes casos:

- Si el certificado del cliente VPN está a punto de caducar. Para ver la fecha de caducidad, haga clic en el icono (i) de la imagen de servidor VPN.
- Si cree que el archivo de configuración está en riesgo.

En cuanto se actualice el archivo de configuración, no se podrá llevar a cabo la conexión a través de archivo anterior. Asegúrese de distribuir el nuevo archivo entre los usuarios a los que se les permita usar la conexión de punto a sitio.

7.3 Trabajar con un servidor se recuperación

7.3.1 Creación de un servidor de recuperación

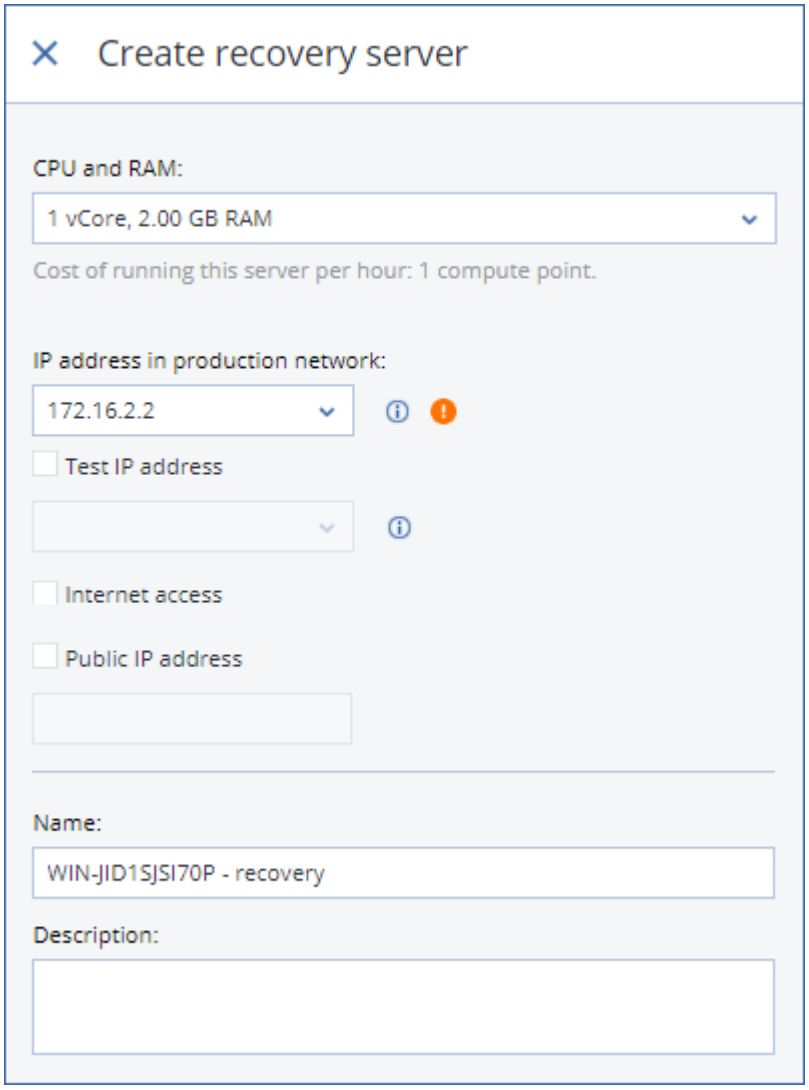
Requisitos previos

- Los planes de copias de seguridad se deben aplicar al equipo que quiera proteger.
  - Puede realizar copias de seguridad de todo el equipo o únicamente de los discos necesarios para iniciarlo y proporcionar los servicios necesarios.
  - Se debe seleccionar el almacenamiento en la cloud como destino.
  - El cifrado de las copias de seguridad debe estar deshabilitado.
  - Le recomendamos que ejecute el plan de copias de seguridad al menos una vez antes de crear el servidor de recuperación para asegurarse de que las copias de seguridad en la cloud se crean correctamente.
- Se debe establecer una conexión VPN en el sitio web de recuperación en la cloud.

Pasos para crear un servidor de recuperación

1. Seleccione el equipo que desea proteger.

2. Haga clic en **Recuperación ante desastres** y, luego, en **Crear recuperar servidor**.



3. Seleccione el número de núcleos virtuales y el tamaño de la RAM.

   Tenga en cuenta los puntos del equipo que se encuentran junto a cada opción. El número de puntos del equipo indican el coste de funcionamiento del servidor de recuperación por hora.

4. Especifique la dirección IP que tendrá el servidor en la red de producción. La dirección IP del equipo original se establece de forma predeterminada.

   Nota *Si usa un servidor DHCP, agregue esta dirección IP a la lista de exclusión de servidores para evitar conflictos con la dirección IP.*

5. [Opcional] Marque la casilla de verificación de **dirección IP de prueba** y, a continuación, especifique la dirección IP.

   Así, podrá conectarse al servidor de recuperación mediante el escritorio remoto o SHH durante una conmutación por error de prueba. En el modo de conmutación por error de prueba, el servidor VPN sustituirá la dirección IP de prueba por la dirección IP de producción mediante el protocolo NAT.

   Si deja la casilla de verificación desmarcada, la consola será la única forma de acceder al servidor durante una conmutación por error de prueba.

   Nota *Si usa un servidor DHCP, agregue esta dirección IP a la lista de exclusión de servidores para evitar conflictos con la dirección IP.*

Puede seleccionar una de las direcciones IP propuestas o escribir otra.

6. [Opcional] Marque la casilla de verificación de **acceso a Internet**.

   De esta forma, el servidor de recuperación tendrá acceso a Internet durante una conmutación por error de prueba o real.

7. [Opcional] Marque la casilla de verificación de **dirección IP pública**.

   El hecho de que el servidor de recuperación cuente con una dirección IP pública conlleva que se pueda acceder a él desde Internet durante una conmutación por error de prueba o real. Si deja la casilla de verificación desmarcada, el servidor solo estará disponible en su red de producción.

   La dirección IP pública se mostrara cuando finalice la configuración. Los siguientes puertos se abren para realizar conexiones de entrada a direcciones IP públicas:

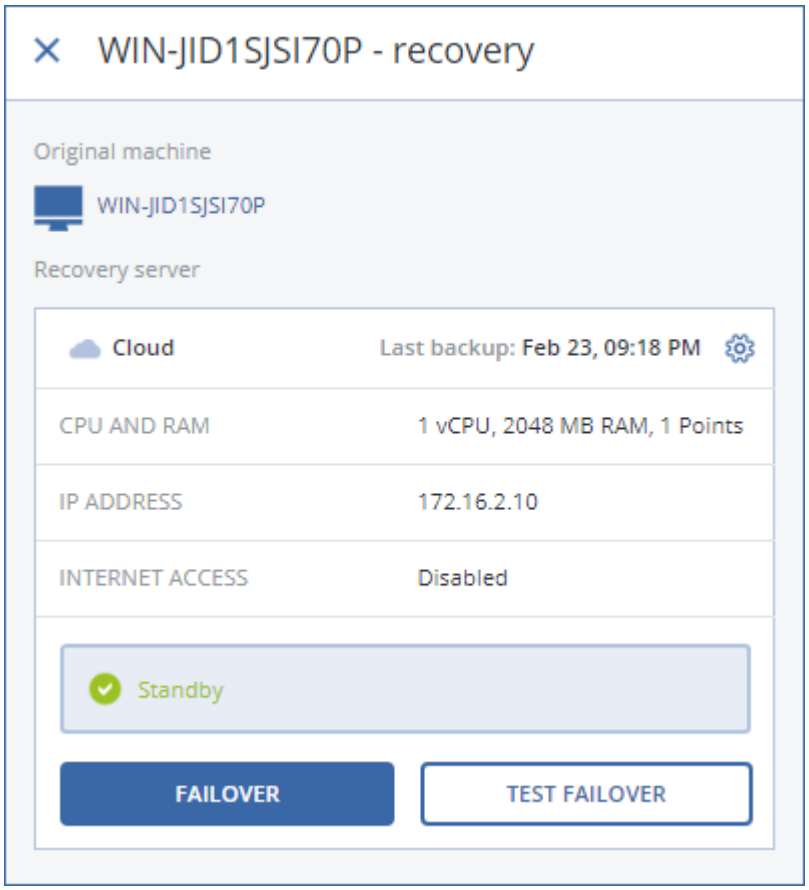
   TCP: 80, 443, 8088, 8443

   UDP: 1194

   Si necesita que se abran otros puertos, póngase en contacto con el equipo de soporte técnico.

8. [Opcional] Cambie el nombre del servidor de recuperación.
9. [Opcional] Escriba una descripción para el servidor de recuperación.
10. Haga clic en **Realizado**.

El servidor de recuperación aparece en la sección **Sitio web de recuperación en la cloud** de la consola de copia de seguridad. También puede acceder a su configuración si selecciona el equipo original y hace clic en **Recuperación ante desastres**.



7.3.2 Cómo funciona la conmutación por error

El funcionamiento de la conmutación por error emplea la funcionalidad "ejecutar un equipo virtual desde una copia de seguridad" (pág. 267).

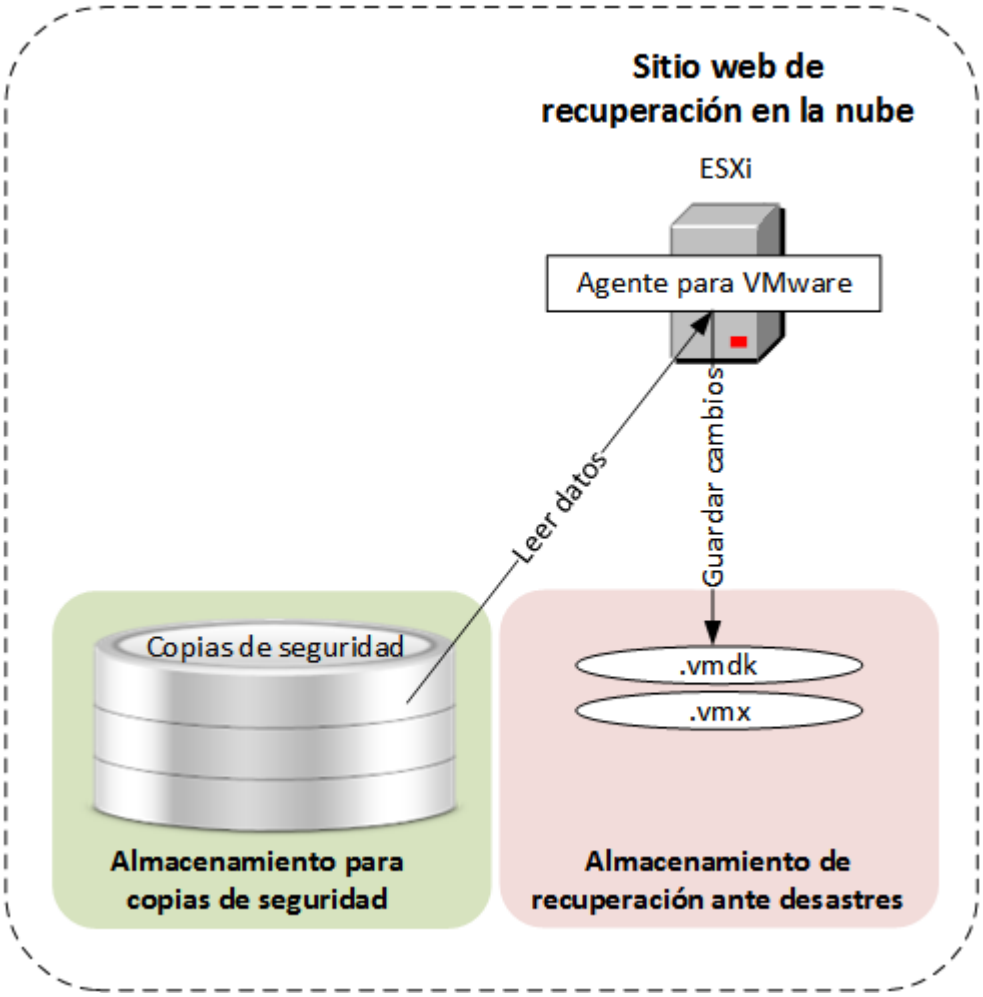
Cuando se dice que "un servidor de recuperación se inicia", significa que un equipo virtual con parámetros predefinidos se ejecuta desde una de las copias de seguridad del equipo original.

Durante una **conmutación por error de prueba**, el equipo virtual no se apaga. Esto significa que el agente lee el contenido de los discos virtuales directamente desde la copia de seguridad, es decir, accede aleatoriamente a varias partes de ella. Por lo tanto, el servidor puede funcionar más lento, pero ocupa menos espacio en el almacén de datos (almacenamiento de recuperación ante desastres).

Durante una **conmutación por error real**, el equipo virtual se apaga lo antes posible para conseguir el mejor rendimiento. Cuando el servidor de recuperación se inicia, su estado cambia a **Finalización**. Este proceso consiste en transferir las unidades de disco virtual del servidor desde la copia de seguridad hasta el almacenamiento de recuperación ante desastres. De hecho, la recuperación del equipo virtual tiene lugar durante su ejecución. Debido a este procedimiento, el servidor puede funcionar más lentamente. Cuando la finalización se completa, el rendimiento del servidor alcanza su valor normal. El estado del servidor cambia a **Conmutación por error**.

Si el servidor de recuperación cuenta con un agente de copia de seguridad en su interior, el servicio de agente se detiene para evitar que se produzca una actividad no deseada, como el inicio de una copia de seguridad o la creación de informes sobre estados desactualizados al servicio de copia de seguridad.

En el siguiente diagrama se muestra la ejecución de un servidor de recuperación, incluido el consumo del almacenamiento.



7.3.3 Prueba de una conmutación por error

Probar una conmutación por error implica iniciar un servidor de recuperación en la VLAN de prueba que esté aislada de su red de producción. Puede probar varios servidores de recuperación a la vez para comprobar su interacción. En la red de prueba, los servidores se comunican mediante sus direcciones IP de producción, pero no pueden iniciar las conexiones TCP o UDP en los equipos de su red local.

Aunque el proceso de prueba de una conmutación por error es opcional, le recomendamos que lo haga habitualmente con la frecuencia que considere adecuada, teniendo en cuenta el coste y la seguridad. Una práctica recomendada es un runbook, un conjunto de instrucciones en las que se describe la forma de iniciar el entorno de producción en la cloud.

Pasos para ejecutar una conmutación por error de prueba

1. Seleccione el equipo original o el servidor de recuperación que quiera probar.
2. Haga clic en **Recuperación ante desastres**.

   Se abre la descripción del servidor de recuperación.
3. Haga clic en **Probar conmutación por error de prueba**.
4. Seleccione el punto de recuperación y haga clic en **Probar conmutación por error**.

Cuando el servidor de recuperación se inicia, su estado cambia a **Probando conmutación por error**.

5. Use uno de los siguientes métodos para probar el servidor de recuperación:
   - En la consola de copias de seguridad, haga clic en **Dispositivos** > **Sitio de recuperación en la cloud**, seleccione el servidor de recuperación y, luego, haga clic en **Consola** en el panel de la derecha.
   - Use el equipo remoto o SSH para conectarse al servidor de recuperación y a la dirección IP de prueba que especificó al crear el servidor de recuperación. Pruebe la conexión tanto desde el interior de la red de producción como de exterior (como se describe en "Conexión de punto a sitio" (pág. 186).
   - Ejecute una secuencia de comandos en el servidor de recuperación.

     Con ella se puede comprobar la pantalla de inicio, si as aplicaciones se han iniciado, la conexión a Internet y la capacidad de otros equipos de conectarse al servidor de recuperación.
   - Si el servidor de recuperación tiene acceso a Internet y a una IP pública, puede que quiera usar TeamViewer.
6. Cuando la prueba haya terminado, haga clic en **Detener prueba** en la consola de copia de seguridad.

   El servidor de recuperación se detiene. Todos los cambios realizados en el servidor de recuperación durante la prueba de conmutación por error se pierden.

7.3.4 Realización de una conmutación por error

La conmutación por error es un proceso que consiste en mover una carga de trabajo a la cloud, además del estado en el que la carga de trabajo permanece en la cloud.

Al iniciar una recuperación por error, el servidor de recuperación se inicia en la red de producción. Todos los planes de copias de seguridad se revocarán desde el equipo original. Se ha creado y aplicado automáticamente un nuevo plan de copias de seguridad al servidor de recuperación.

Pasos para llevar a cabo una conmutación por error

1. Asegúrese de que el equipo original no esté disponible en la red.
2. En la consola de copias de seguridad, seleccione el equipo original o el servidor de recuperación que corresponda al equipo.
3. Haga clic en **Recuperación ante desastres**.

   Se abre la descripción del servidor de recuperación.
4. Haga clic en **Conmutación por error**.
5. Seleccione el punto de recuperación y haga clic en **Conmutación por error**.

   Cuando el servidor de recuperación se inicia, su estado cambia a **Finalización** y, después de un tiempo, cambia a **Conmutación por error**. Entender que el servidor está disponible en ambos estados es fundamental, a pesar de que el indicador de progreso cambie. Para obtener información detallada, consulte la sección Cómo funciona la conmutación por error (pág. 191).
6. Mire la consola del servidor de recuperación para asegurarse de que se ha iniciado. Haga clic en **Dispositivos** > **> Sitio de recuperación en la cloud**, seleccione el servidor de recuperación y, luego, haga clic en **Consola** en el panel de la derecha.
7. Asegúrese de que se pueda acceder al servidor de recuperación mediante la IP de producción que haya especificado al crearlo.

Cuando el servidor de recuperación se haya apagado, se crea y se aplica automáticamente un nuevo plan de copias de seguridad. Este plan de copias de seguridad se basa en el que se usó para crear el servidor de recuperación, con ciertas limitaciones. En este plan, puede cambiar únicamente la planificación y las reglas de retención. Para obtener más información, consulte "Realización de copias de seguridad de servidores en la cloud" (pág. 196).

La única forma de salir del estado de conmutación por error es llevar a cabo una conmutación por recuperación.

7.3.5 Realización de una conmutación por recuperación

La conmutación por recuperación es un proceso que consiste en volver a mover la carga de trabajo desde la cloud a sus instalaciones.

Durante este proceso, el servidor no está disponible. La duración de la ventana de mantenimiento es aproximadamente igual a la de una copia de seguridad y la posterior recuperación del servidor.

Pasos para llevar a cabo una conmutación por recuperación

1. Seleccione un servidor de recuperación cuyo estado sea **conmutación por error**.
2. Haga clic en **Recuperación ante desastres**.

   Se abre la descripción del servidor de recuperación.
3. Haga clic en **Preparar conmutación por recuperación**.

   El servidor de recuperación se detendrá y se realizará una copia de seguridad en el almacenamiento en la cloud. Espere hasta que el proceso de creación de la copia de seguridad termine.

   En ese momento, puede llevar a cabo dos acciones: **Cancelar la conmutación por recuperación** y **Ejecutar la conmutación por recuperación**. Si hace clic en **Cancelar conmutación por recuperación**, el servidor de recuperación se iniciará y la conmutación por error continuará.
4. Recupere el servidor desde esta copia de seguridad al hardware o a un equipo virtual situado en sus instalaciones.
   - Al usar un dispositivo de arranque, proceda como se describe en "Recuperar discos usando dispositivos de arranque" (pág. 162). Asegúrese de que inicia sesión en la cloud con la cuenta para la que se registró el servidor, así como de que haya seleccionado la copia de seguridad más reciente.
   - Si el equipo de destino está en línea o es un equipo virtual, puede usar la consola de copia de seguridad. En la pestaña **Copias de seguridad**, seleccione el almacenamiento en la cloud. En **Equipo desde el cual examinar**, seleccione el equipo físico de destino, o bien el equipo que esté ejecutando el agente si el equipo de destino es virtual. El equipo seleccionado debe estar registrado para la misma cuenta para la que se registró el servidor. Busque la copia de seguridad más reciente del servidor, haga clic en **Recuperar todo el equipo** y configure otros parámetros de recuperación. Para obtener instrucciones detalladas, consulte la sección "Recuperación de un equipo" (pág. 157).

   Asegúrese de que la recuperación se complete y de que el equipo recuperado funcione correctamente.
5. Vuelva al servidor de recuperación de la consola de copias de seguridad y, a continuación, haga clic en **Ejecutar conmutación por recuperación**.

   El servidor y los puntos de recuperación estarán listos para una nueva conmutación por error. Para crear puntos de recuperación nuevos, aplique el plan de copias de seguridad a un nuevo servidor local.

7.4 Trabajar con un servidor principal

7.4.1 Creación de un servidor principal

Requisitos previos

- Se debe establecer una conexión VPN en el sitio web de recuperación en la cloud.

Pasos para crear un servidor principal

1. Haga clic en **Dispositivos** > **Cloud**.
2. Haga clic en **Nuevo**.
3. Seleccione una plantilla para el nuevo equipo virtual.
4. Seleccione el número de núcleos virtuales y el tamaño de la RAM.

   Preste atención a los puntos del equipo que se encuentran junto a cada opción. El número de puntos del equipo indican el coste de funcionamiento del servidor principal por hora.
5. Especifique la dirección IP que tendrá el servidor en la red de producción. La primera dirección IP libre de su red de producción se establece de forma predeterminada.

   Nota *Si usa un servidor DHCP, agregue esta dirección IP a la lista de exclusión de servidores para evitar conflictos con la dirección IP.*
6. [Opcional] Marque la casilla de verificación de **acceso a Internet**.

   De esta forma, el servidor principal tendrá acceso a Internet.
7. [Opcional] Marque la casilla de verificación de **dirección IP pública**.

   El hecho de que el servidor principal cuente con una dirección IP pública conlleva que se pueda acceder a él desde Internet. Si deja la casilla de verificación desmarcada, el servidor solo estará disponible en su red de producción.

   La dirección IP pública se mostrara cuando finalice la configuración. Los siguientes puertos se abren para realizar conexiones de entrada a direcciones IP públicas:

   TCP: 80, 443, 8088, 8443

   UDP: 1194

   Si necesita que se abran otros puertos, póngase en contacto con el equipo de soporte técnico.
8. [Opcional] Cambie el tamaño de las unidades de discos virtuales. Si necesita más de un disco rígido, haga clic en **Agregar disco** y, a continuación, especifique el nuevo disco.
9. Cree y escriba el nombre del servidor principal.
10. [Opcional] Escriba una descripción para el servidor principal.
11. Haga clic en **Realizado**.

El servidor principal estará disponible en la red de producción. Puede gestionar el servidor mediante su consola, el escritorio remoto, SSH o TeamViewer.

7.4.2 Operaciones con un servidor principal

El servidor principal aparece en la sección **Sitio web de recuperación en la cloud** de la consola de copia de seguridad.

Para iniciar o detener el servidor, haga clic en **Iniciar** o **Detener** en el panel derecho.

Para editar la configuración del servidor primario, deténgalo, haga clic en **Información** y, luego, en **Editar**.

Para aplicar un plan de copias de seguridad al servidor principal, haga clic en **Copia de seguridad**. Verá un plan de copias de seguridad predefinido en el que puede cambiar únicamente la planificación y las reglas de retención. Para obtener más información, consulte "Realización de copias de seguridad de servidores en la cloud" (pág. 196).

7.5 Realización de copias de seguridad de servidores en la cloud

Agent para VMware, que se instala en el sitio de recuperación en la cloud, realiza copias de seguridad de los servidores principales y de recuperación. En su versión inicial, las funcionalidades de esta copia de seguridad están relativamente restringidas en comparación con la que realizan los agentes locales. Estas limitaciones son temporales y se eliminarán en futuras versiones.

- La única ubicación de copia de seguridad es el almacenamiento en la cloud.
- No se puede aplicar un plan de copias de seguridad a varios servidores. Cada servidor debe tener su propio plan de copias de seguridad, incluso si todos los planes de copias de seguridad tienen la misma configuración.
- Solo se puede aplicar un plan de copias de seguridad a un servidor.
- No es compatible con la copia de seguridad compatible con la aplicación.
- El cifrado no está disponible.
- Las opciones de copia de seguridad no están disponibles.

Cuando elimina un servidor principal, las copias de seguridad también se eliminan.

Se realiza una copia de seguridad de un servidor de recuperación únicamente en estado de conmutación por error. Sus copias de seguridad siguen la secuencia de copia de seguridad del servidor original. Cuando se lleva a cabo una conmutación por recuperación, el servidor original puede continuar esta secuencia de copia de seguridad. Por lo tanto, las copias de seguridad del servidor de recuperación solo se pueden eliminar manualmente o como resultado de la aplicación de reglas de retención. Cuando se elimina un servidor de recuperación, sus copias de seguridad se conservan siempre.

7.6 Uso de los runbooks

Un runbook es un conjunto de instrucciones en las que se describe la forma de iniciar el entorno de producción en el cloud. Puede crear runbooks en la consola de copias de seguridad. Para acceder a la pestaña **Runbooks**, seleccione **Recuperación ante desastres** > **Runbooks**.

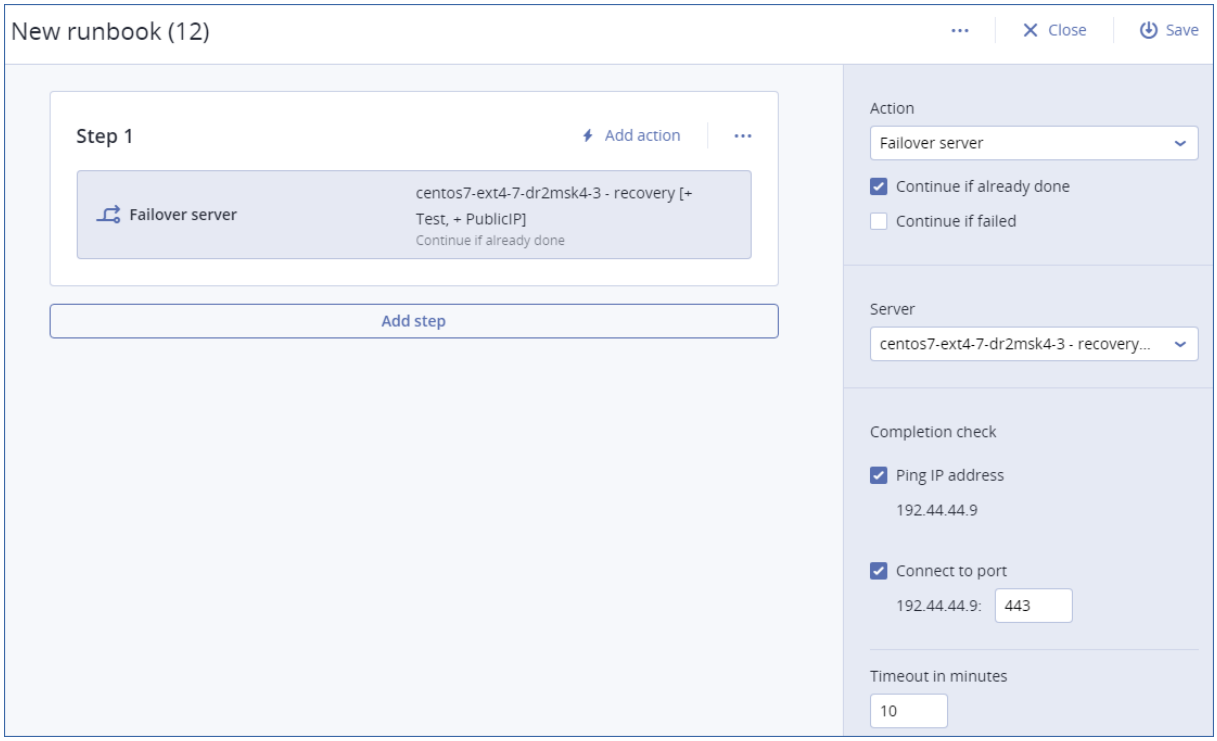
¿Por qué usar runbooks?

Con los runbooks, puede llevar a cabo las siguientes acciones:

- Automatizar una conmutación por error de uno o varios servidores.
- Hacer ping en la IP del servidor y comprobar la conexión al puerto que especifique para poder comprobar automáticamente el resultado de la conmutación por error.
- Establecer la secuencia de operaciones de los servidores mediante la ejecución de aplicaciones distribuidas.
- Incluir operaciones manuales en el flujo de trabajo.
- Verificar la integridad de su solución de recuperación ante desastres mediante la ejecución de runbooks en modo de prueba.

7.6.1 Creación de un runbook

Para empezar a crear un runbook, haga clic en **Crear runbook** > **Añadir paso** > **Añadir acción**. Puede usar la opción de arrastrar y soltar para mover acciones y pasos. No se olvide de poner un nombre distintivo al runbook. Cuando esté creando un runbook grande, haga clic en **Guardar** de vez en cuando. Cuando haya terminado, haga clic en **Cerrar**.



Pasos y acciones

Los runbooks están formados por pasos que se ejecutan consecutivamente. Un paso es un conjunto de acciones que se inician simultáneamente. Una acción puede estar formada por una de estas opciones:

- Una operación que se vaya a llevar a cabo con un servidor en el cloud (**Servidor de conmutación por error**, **Iniciar servidor**, **Detener servidor**, **Servidor de conmutación por recuperación**). Para definir esta operación, tiene que elegir la operación, sus parámetros y el servidor en el cloud.
- Una operación manual que tenga que describir verbalmente. Una vez que se complete la operación, el usuario debe hacer clic en el botón de confirmación para aceptar que el runbook siga con el proceso.
- Ejecución de otro runbook. Para definir esta operación, tiene que elegir el runbook.

  Un runbook puede estar formado únicamente por una ejecución de un runbook determinado. Por ejemplo, si añade la acción "ejecutar Runbook A", puede incluir la acción "ejecutar Runbook B", pero no puede añadir otra acción "ejecutar Runbook A".

***Nota**: En esta versión del producto, el usuario tiene que llevar a cabo una conmutación por recuperación manualmente. Los runbooks muestran un aviso cuando es obligatorio.*

Parámetros de acción

Todas las operaciones que se llevan a cabo con servidores en el cloud tienen los siguientes parámetros:

- **Continuar si ya se ha realizado** (habilitado de forma predeterminada)

Este parámetro define el comportamiento del runbook cuando ya se ha realizado la operación necesaria (por ejemplo, ya se ha llevado a cabo una conmutación por error o ya hay un servidor en ejecución). Cuando está habilitado, el runbook emite una advertencia y continúa. Cuando está deshabilitado, se produce un error en la operación y en el runbook.

- **Continuar si ha generado un error** (deshabilitado de forma predeterminada)

  Este parámetro define el comportamiento del runbook cuando se produce un error en la operación necesaria. Cuando está habilitado, el runbook emite una advertencia y continúa. Cuando está deshabilitado, se produce un error en la operación y en el runbook.

Verificación de finalización

Puede añadir verificaciones de finalización a las acciones **Servidor de recuperación de fallos** e **Iniciar servidor** para asegurarse de que el servidor esté disponible y proporcione los servicios necesarios. Si alguna de las verificaciones falla, la acción se considera fallida.

- **Hacer ping a la dirección IP**

  El software hará ping a la dirección IP de producción del servidor en el cloud hasta que este responda o expire el tiempo de espera, lo que ocurra primero.

- **Conectar a puerto** (443 de forma predeterminada)

  El software usará la dirección IP de producción del servidor en el cloud y el puerto que usted especifique para intentar conectarse a él hasta que se establezca la conexión o expire el tiempo de espera, lo que ocurra primero. De esta forma, puede comprobar si la aplicación que se detecta en el puerto especificado se encuentra en funcionamiento.

El tiempo de espera predeterminado es de 10 minutos. Puede cambiarlo si lo desea.

7.6.2 Operaciones runbooks

Para acceder a la lista de operaciones, mueva el ratón sobre un runbook y haga clic en el icono de puntos suspensivos. Cuando un runbook no funciona, puede llevar a cabo las siguientes operaciones:

- **Ejecutarlo**
- **Editarlo**
- **Clonarlo**
- **Eliminarlo**

Ejecución de un runbook

Cada vez que haya clic en **Ejecutar**, se le pedirá que establezca los parámetros de la ejecución. Estos parámetros se aplicarán a todas las operaciones de conmutación por error y por recuperación incluidas en el runbook. Los runbooks especificados en las operaciones **Ejecutar runbook** heredan estos parámetros del runbook principal.

- **Modo conmutación por error y conmutación por recuperación**

  Elija si quiere ejecutar una conmutación por error de prueba (opción predeterminada) o una real (producción). El modo de conmutación por recuperación se corresponderá con el modo de conmutación por error elegido.

- **Punto de recuperación de conmutación por error**

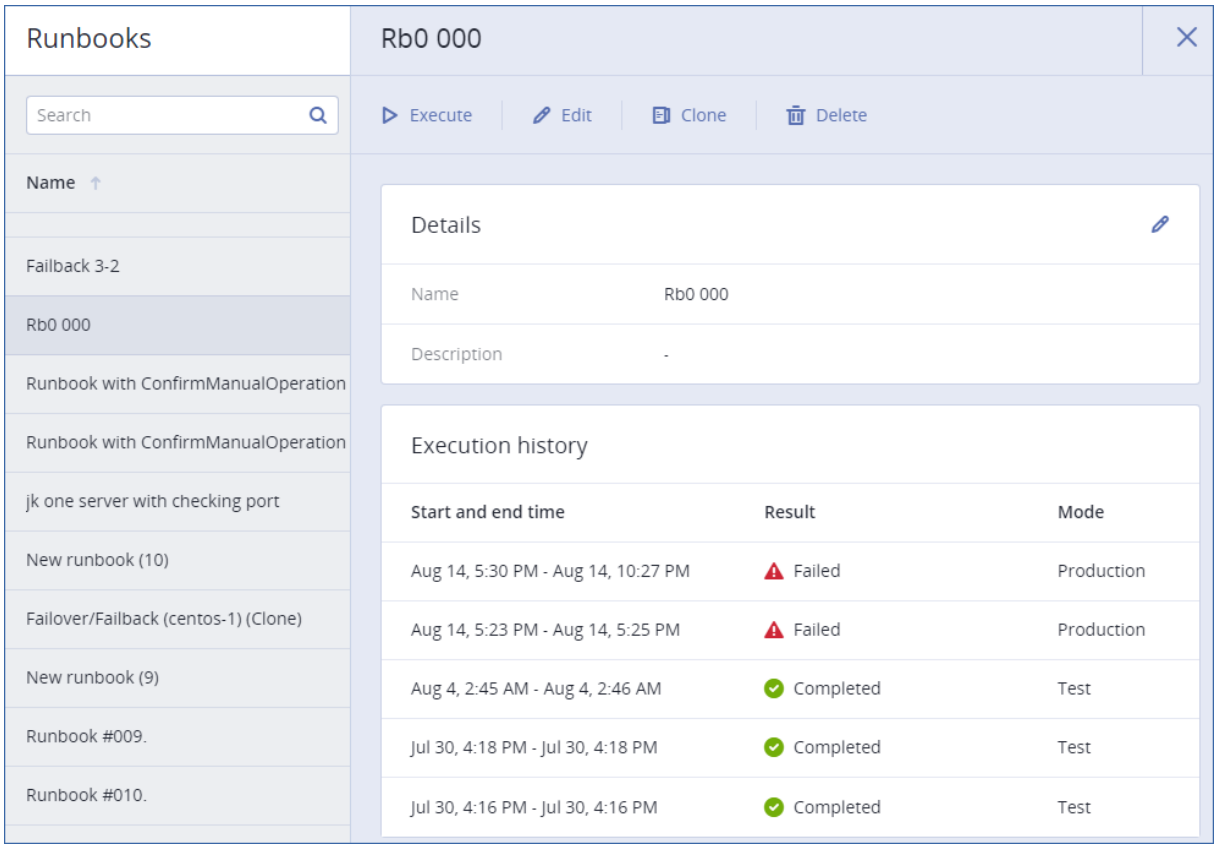
  Elija el punto de recuperación más reciente (opción predeterminada) o seleccione un momento específico del pasado. Si elige la segunda opción, se seleccionarán los puntos de recuperación más cercanos a la fecha y la hora especificadas para cada servidor.

Detención de la ejecución de un runbook

Durante la ejecución de un runbook, puede seleccionar la opción **Detener** en la lista de operaciones. El software completará todas las acciones que ya se hayan iniciado excepto aquellas que requieran interacción del usuario.

Visualización del historial de ejecuciones

Al seleccionar un runbook de la pestaña **Runbooks**, el software muestra información sobre él y el historial de ejecuciones. Haga clic en la línea que corresponda a una ejecución específica para ver el registro de ejecuciones.



8 Operaciones con copias de seguridad

8.1 Pestaña Copias de seguridad

La pestaña **Copias 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 el caso del almacenamiento en la cloud, los usuarios solo tienen acceso a sus propias copias de seguridad. En una implementación de la cloud, 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 **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 copias de seguridad se añaden automáticamente a la pestaña **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.

Para seleccionar un punto de recuperación desde la pestaña Copias de seguridad

1. En la pestaña **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:

   `<nombre del equipo> - <nombre del plan de copias de seguridad>`
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.

8.2 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:

   `<nombre del equipo> - <GUID del plan de copias de seguridad>`
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 incluidos en la copia de seguridad.

   Consejo *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**
   - **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.

8.3 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 (pág. 205).

El nombre del archivo de la copia de seguridad (pág. 127) de una copia de seguridad exportada depende del valor de la opción formato de copia de seguridad (pág. 130):

- Para el formato **Versión 12** con cualquier esquema de copias de seguridad, para crear el nombre del archivo de la copia de seguridad se añade un número de secuencia al nombre del archivo original. 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, 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 otros esquemas de copias de seguridad, aparece una marca de tiempo diferente a la del nombre del archivo de copia de seguridad original. 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 copias de seguridad (pág. 199).
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**.

8.4 Eliminación de copias de seguridad

Para eliminar las copias de seguridad de un equipo que esté conectado y presente en la consola de copia de seguridad

1. En la pestaña **Todos los dispositivos**, seleccione el equipo cuyas copias de seguridad desee eliminar.
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 **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:

   `<nombre del equipo> - <nombre del plan de copias de seguridad>`
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" (pág. 167).
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.

9 Operaciones con los planes de copias de seguridad

Para obtener información sobre cómo crear un plan de copias de seguridad, consulte "Copia de seguridad" (pág. 86).

Para editar un plan de copias de seguridad

1. Si quiere editar el plan de copias de seguridad 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 copias de seguridad.
2. Haga clic en **Copia de seguridad**.
3. Seleccione el plan de copias de seguridad que desee editar.
4. Haga clic en el icono del engranaje que se encuentra al lado del nombre del plan de copias de seguridad y haga clic en **Editar**.
5. Para modificar los parámetros del plan, haga clic en la sección correspondiente en el panel del plan de copias de seguridad.
6. Haga clic en **Guardar cambios**.
7. Para cambiar el plan de copias de seguridad para todos los equipos a los que se aplica, haga clic en **Aplicar los cambios a este plan de copias de seguridad**. De lo contrario, haga clic en **Crear un nuevo plan de copias de seguridad solamente para los recursos seleccionados**.

Para anular un plan de copias de seguridad en equipos

1. Seleccione los equipos en los que desea anular el plan.
2. Haga clic en **Copia de seguridad**.
3. Si se aplican varios planes de copias de seguridad a los equipos, seleccione el plan de copias de seguridad que desea anular.
4. Haga clic en el icono de engranaje que se encuentra junto al nombre del plan de copias de seguridad y, después, en **Anular**.

Para borrar un plan de copias de seguridad

1. Seleccione cualquiera de los equipos a los que se les aplica el plan de copias de seguridad que desea borrar.
2. Haga clic en **Copia de seguridad**.
3. Si se aplican varios planes de copias de seguridad al equipo, seleccione el plan de copias de seguridad que desea borrar.
4. Haga clic en el icono de engranaje que se encuentra junto al nombre del plan y después, haga clic en **Eliminar**.

   Como consecuencia, se anula el plan de copias de seguridad en todos los equipos y se elimina completamente de la interfaz web.

10 La pestaña Planes

Importante *Esta función se introdujo en la versión 12.5, que afecta solo a las implementaciones en una instalación. Esta función todavía no está disponible en las implementaciones en la nube. Para obtener más información, consulte "Novedades en Acronis Backup" (pág. 8).*

Puede gestionar los planes de copias de seguridad 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:

- **Copia de seguridad**
- **Réplica de copia de seguridad** (pág. 205)
- **Validación** (pág. 207)
- **Limpieza** (pág. 209)

- **Conversión a VM** (pág. 209)
- **Replicación de equipos virtuales** (pág. 270)
- **Dispositivo de arranque**. Esta sección muestra los planes de copias de seguridad que se han creado para equipos que se inician desde dispositivos de arranque (pág. 228) y solo pueden aplicarse a esos equipos.

Los planes para la réplica de copia de seguridad, validación, limpieza y conversión a equipos virtuales solo están disponibles con la licencia de Advanced. Sin la licencia de Advanced, estas acciones únicamente pueden realizarse como parte de un plan de copias de seguridad.

En cada sección puede crear, editar, deshabilitar, habilitar, eliminar e iniciar un plan, así como inspeccionar su estado.

La clonación y la detención solo están disponibles en planes de copias de seguridad. A diferencia de cuando detiene las copias de seguridad desde la pestaña **Dispositivos**, el plan de copias de seguridad se detendrá en todos los dispositivos en los que se esté ejecutando. Si el inicio de las copias de seguridad no se produce a la vez en todos los dispositivos, la detención del plan de copias de seguridad también impedirá que empiece en los dispositivos en los que aún no ha comenzado a ejecutarse.

También puede exportar un plan a un archivo e importar un plan previamente exportado.

10.1 Procesamiento de datos fuera del host

La mayoría de acciones que son parte de un plan de copias de seguridad 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 replicación, validación, limpieza y conversión de las copias de seguridad 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.

10.1.1 Réplica de copia 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 nube	+	+
Carpeta local	+	+
Carpeta de red	+	+
Carpeta NFS	–	–
Secure Zone	–	–
Servidor SFTP	–	–
Ubicación gestionada	+	+
Dispositivo de cintas	–	+

Creación de un plan de réplica de copia 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 replicar 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" (pág. 113).
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**.

10.1.2 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" (pág. 131).
- **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 copia de seguridad (Agente para VMware o Agente para Hyper-V).

  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 nube	+	+
Carpeta local	+	+
Carpeta de red	+	+
Carpeta NFS	–	–
Secure Zone	–	–
Servidor SFTP	–	–
Ubicación gestionada	+	+
Dispositivo de cintas	+	–

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 validar 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 del disco.

      La configuración predeterminada es **Fina** para VMware ESXi y **Expansión dinámica** para Hyper-V.
   d. No deshabilite la opción **Latido del equipo virtual** si necesita un resultado de validación correcto. Esta opción se ha diseñado para versiones futuras.
   e. [Opcional] Haga clic en **Configuración de VM** para modificar el tamaño de la memoria y las conexiones de red del equipo 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.
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**.

10.1.3 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.

Creación de un plan de limpieza nuevo

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" (pág. 113).
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**.

10.1.4 Conversión a equipo virtual

Puede crear un plan independiente para la conversión a un equipo virtual y ejecutarlo manualmente o de forma planificada.

Para obtener más información sobre los requisitos previos y las limitaciones, consulte "Lo que necesita saber sobre conversión" (pág. 117).

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**
- **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. 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. [Opcional] Para VMware ESXi y Hyper-V, también puede hacer lo siguiente:
   - 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.
10. [Opcional] Haga clic en **Planificación** y, a continuación, cambie la planificación.
11. 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.
12. [Opcional] Para modificar las opciones del plan, haga clic en el icono de engranaje.
13. Haga clic en **Crear**.

11 Dispositivo de arranque

Importante *Algunas de las funciones descritas en esta sección se introdujeron en la versión 12.5, que afecta solo a las implementaciones en una instalación. Estas funciones todavía no están disponibles en las implementaciones en la nube. Para obtener más información, consulte* *"Novedades en Acronis Backup" (pág. 8).*

11.1 Bootable Media Builder

Bootable Media Builder es una herramienta dedicada para la creación de dispositivos de arranque. Solo está disponible para implementaciones en una instalación.

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 de copia de seguridad 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 basado en Linux o en WinPE con la funcionalidad de las copias de seguridad.
- Aparte de crear medios físicos o su ISO, puede cargar el medio en Windows Deployment Services (WDS) y usar el arranque en red.
- Por último, puede escribir el medio directamente en una unidad flash sin utilizar herramientas de terceros.

¿32 o 64 bits?

Bootable Media Builder se puede instalar desde programas de instalación tanto de 32 como de 64 bits. Los bits que tenga el medio se corresponderán con los que tenga el programa de instalación. No obstante, puede crear un medio basado en WinPE de 32 bits usando Media Builder de 64 bits siempre que haya descargado el complemento de 32 bits.

Recuerde que 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).

11.1.1 Dispositivos de arranque basados en Linux

Para crear un dispositivo de arranque basado en Linux

1. Inicie Bootable Media Builder.
2. Especifique la clave de licencia. La licencia no se asignará ni volverá a asignarse. Determina la funcionalidad que se habilitará en el medio creado. Sin las claves de licencia, solo podrá crear medios para recuperación.
3. Seleccione **Tipo de dispositivo de arranque: Predeterminado (dispositivo de arranque basado en Linux)**.

   Seleccione la manera en que los volúmenes y las redes compartidas se manejarán (denominado estilo de los dispositivos).

   - 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.
   - 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 una lista de parámetros, consulte la sección Parámetros del kernel.
5. [Opcional] Seleccione el idioma que se utilizará en el dispositivo de arranque.
6. Seleccione los componentes que se ubicarán en el medio: el agente de arranque y/o Universal Restore.

   Utilizando un medio 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 si hay problemas con la capacidad de arranque del sistema. La herramienta localiza e instala los controladores de dispositivos que son críticos para el inicio del 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.

   Si no se configura, el cargador espera que alguien seleccione si arrancar desde el sistema operativo (de estar presente) o desde el componente.

   Si configura, por ejemplo, **10 s** para el agente de arranque, el agente se iniciará 10 segundos después de que se muestre el menú. Esto habilita el funcionamiento in situ sin interacción al arrancar desde WDS/RIS.
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 (pág. 215) y especifique los parámetros del script.
9. [Opcional] Especifique la configuración de inicio de sesión remota: el nombre de usuario y la contraseña que se deben especificar en una cadena de comando si la utilidad **acrocmd** se instala en un equipo distinto. Si deja estas casillas sin marcar, no es necesario que el comando contenga credenciales.

   Estas credenciales también son necesarias al registrar el dispositivo en el servidor de gestión desde la consola de copia de seguridad (pág. 228).
10. [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" (pág. 221).
11. [Opcional] Especifique la configuración de red (pág. 222): La configuración TCP/IP que será asignada a los adaptadores de red del equipo.
12. [Opcional] Especifique un puerto de red (pág. 223): El puerto TCP que el agente de arranque escucha para las conexiones entrantes.
13. [Opcional] Si hay un servidor proxy habilitado en la red, especifique su nombre de servidor/dirección IP y puerto.
14. Seleccione el tipo de dispositivo que desea crear. Puede:
    - Crear CD, DVD u otro dispositivo de arranque, como una unidad de memoria flash USB, si la BIOS del hardware permite el arranque desde tales dispositivos.
    - Crear una imagen ISO para grabarla posteriormente en un disco vacío o conectarla a un equipo virtual.
    - Cargue los componentes seleccionados en el Acronis PXE Server.
    - Cargar los componentes seleccionados en WDS/RIS.
15. [Opcional] Añada controladores del sistema Windows que usará Universal Restore (pág. 224). Esta ventana aparece si se añade Universal Restore al medio y se selecciona otro medio que no sea WDS/RIS.
16. 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.
17. Compruebe su configuración en la pantalla de resumen y haga clic en **Continuar**.

11.1.1.1 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 inicio.

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=**desactivado**

Desactiva el módulo cuyo nombre aparece en *module_name*. Por ejemplo, para desactivar el uso del módulo SATA, especifique: **sata_sis=desactivado**

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.

11.1.1.2 Scripts en dispositivo de arranque

Nota *Esta funcionalidad solo está disponible con la licencia de Acronis Backup Advanced.*

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

   1. En la consola de copia de seguridad, vaya a **Copias de seguridad** > **Ubicaciones**.
   2. Seleccione la red compartida (haga clic en **Añadir ubicación** si la red compartida no aparece en la lista).
   3. Seleccione la copia de seguridad.
   4. 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/<archivo>**.

- **autostart** - un archivo para iniciar **<script_file>.sh**. El contenido del archivo debe ser el siguiente:

```
#!/bin/sh
. /ConfigurationFiles/bin/variables.sh
. /ConfigurationFiles/bin/<script_file>.sh
. /ConfigurationFiles/bin/post_actions.sh
```

- **autostart.json** - un archivo JSON que contiene lo siguiente:
  - El nombre y la descripción del script que aparecerá en Bootable Media Builder.
  - Los nombres de las variables del script que desea configurar mediante Bootable Media Builder.
  - Los parámetros de los controles que aparecerán en Generador de dispositivos de inicio para cada variable.

Estructura de autostart.json

Objeto de nivel superior

Pareja		Obligatorio	Descripción
Nombre	**Tipo de valor**		
displayName	cadena	Sí	El nombre de script que aparecerá en el Generador de dispositivos de inicio.
description	cadena	No	La descripción del script que aparecerá en el Generador de dispositivos de inicio.
timeout	número	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	cadena	Sí	El nombre de la variable utilizado en **<script_file>.sh**.
type	cadena	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	cadena	Sí	La etiqueta de control que aparece encima del control en el Generador de dispositivos de inicio.
default	cadena si **type** es **string**, **multiString**, **password** o **enum** número si **type** es **number**, **spinner** o **checkbox**	No	El valor predeterminado para el control. Si no se especifica la pareja, el valor predeterminado será una cadena vacía o un cero, dependiendo del tipo de control. El valor predeterminado de una casilla de verificación puede ser **0** (el estado desactivado) o **1** (el estado activado).
order	número (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**)	número	No	El valor mínimo del control de número en un cuadro de número. Si no se especifica la pareja, el valor será **0**.

Pareja		Obligatorio	Descripción
Nombre	**Tipo de valor**		
max (solo para **spinner**)	número	No	El valor máximo del control de número en un cuadro de número. Si no se especifica la pareja, el valor será **100**.
step (solo para **spinner**)	número	No	El valor de paso del control de número de un cuadro de número. Si no se especifica la pareja, el valor será **1**.
items (solo para **enum**)	matriz de cadenas	Sí	Los valores de una lista desplegable.
required (para **string**, **multiString**, **password** y **enum**)	número	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

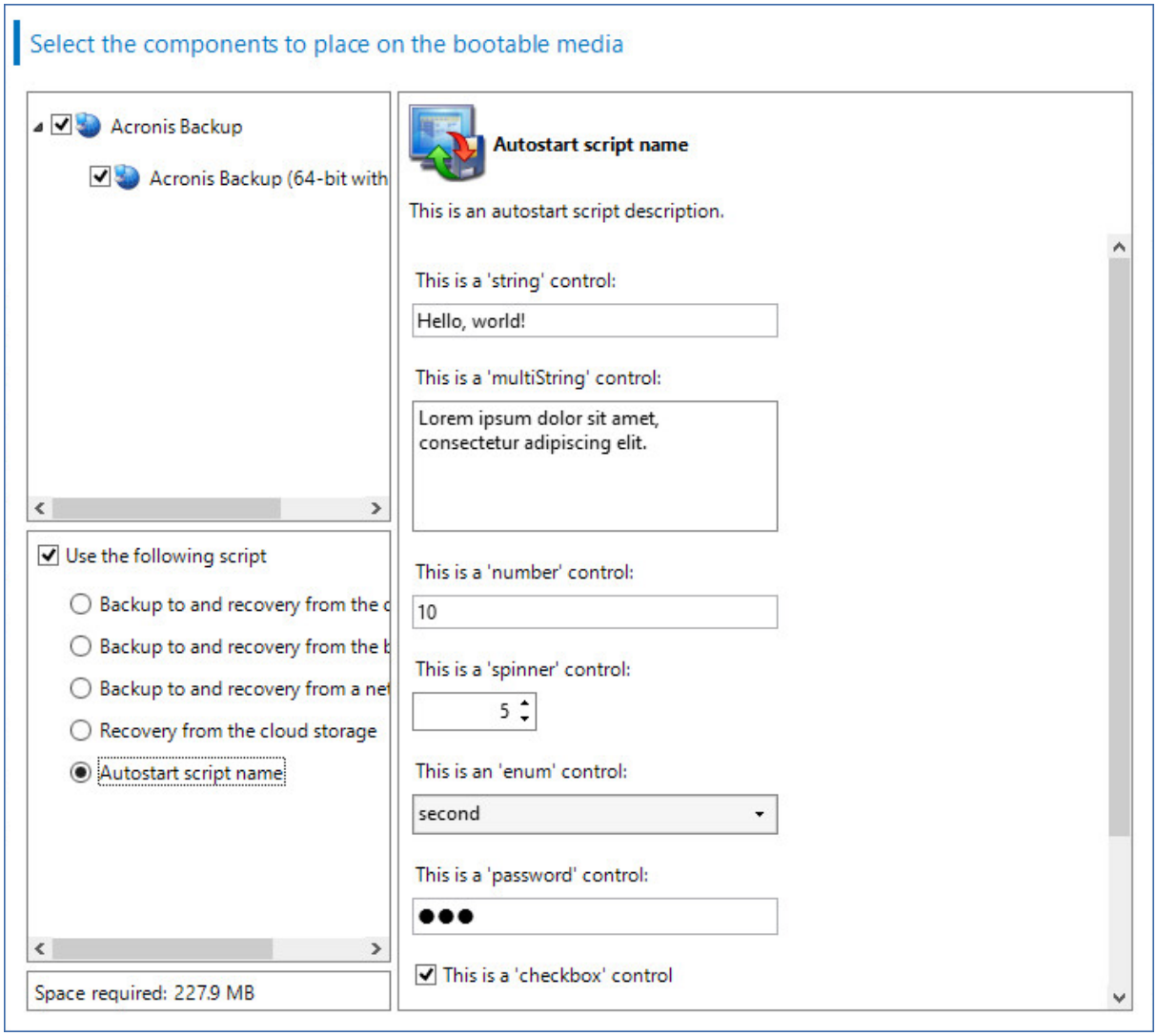
Nombre	Descripción
string	Un cuadro de texto sin límite y en una sola línea que se utiliza para introducir o modificar cadenas cortas.
multiString	Un cuadro de texto sin límite y en varias líneas que se utiliza para introducir o modificar cadenas largas.
password	Un cuadro de texto sin límite y en una 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.



11.1.1.3 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 de copia de seguridad 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 (pág. 228).

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`
- `<dirección IP>` Por ejemplo, `10.250.10.10`
- `<nombre del servidor>` Por ejemplo, `server1` o `server1.example.com`

3. En **Puerto**, especifique el puerto que se deberá usar para acceder al servidor de gestión. El valor predeterminado es 9877.
4. En **Mostrar nombre**, especifique el nombre que deberá mostrarse para este equipo en la consola de copia de seguridad. 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** > **Administradores**). En la consola de copia de seguridad, 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** > **Administradores**). En la consola de copia de seguridad, 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.
   - **No solicitar nombre de usuario y contraseña**

     El equipo se registrará de forma anónima, a menos que el registro anónimo en el servidor de gestión esté deshabilitado (pág. 332).

     La pestaña **Actividades** de la consola de copia de seguridad no muestra quién ha usado el dispositivo.

     En la consola de copia de seguridad, los dispositivos estarán disponibles bajo la organización.

     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**.

11.1.1.4 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 tiene la capacidad de establecer manualmente la configuración de red cuando se ejecuta el agente de arranque en el equipo.

Preconfiguración de múltiples conexiones de red

Puede preestablecer la configuración TCP/IP en 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 la ventana del asistente, se selecciona su configuración para guardarla en el dispositivo. También se guarda la dirección MAC de cada NIC en los dispositivos.

Puede cambiar la configuración, excepto la dirección MAC, o establecer la configuración para una NIC no existente, si fuera necesario.

Una vez que el dispositivo de arranque 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 arranque 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 de la unidad del equipo: NIC1 ocupa la ranura más cercana al procesador, NIC2 es la siguiente ranuras de la unidad y así sucesivamente. Cuando el agente de arranque 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 gestión por medio de la red productiva. 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.

11.1.1.5 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.

11.1.1.6 Controladores para Universal Restore

Cuando crea dispositivos de arranque, tiene la opción de añadir controladores de 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 al 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, por lo que 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 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 Media Builder muestra el contenido del archivo para su información.

Para agregar unidades:

1. Haga clic en **Añadir** 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**.

11.1.2 Dispositivos de arranque basados en WinPE

Bootable Media Builder ofrece tres métodos de integración de Acronis Backup con WinPE:

- Creación del PE ISO con el complemento desde cero.
- Adición del complemento de Acronis a un archivo WIM para cualquier propósito (creación manual de imagen ISO, adición de otras herramientas a la imagen y demás).

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 para Windows 10)

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 la interfaz extensible del firmware unificada (UEFI).

Las imágenes PE basadas en WinPE 4 y versiones posteriores necesitan aproximadamente 1 GB de RAM para funcionar.

11.1.2.1 Preparación: WinPE 2.x y 3.x

Para poder crear o modificar las imágenes PE 2.x o 3.x, instale Bootable Media Builder en un equipo en el que esté instalado Windows Automated Installation Kit (AIK). Si no tiene un equipo con AIK, prepárelo de la siguiente manera:

Para preparar un equipo con AIK

1. Descargue e instale Windows Automated Installation Kit.

   Automated Installation Kit (AIK) para Windows Vista (PE 2.0):

   http://www.microsoft.com/Downloads/details.aspx?familyid=C7D4BC6D-15F3-4284-9123-679830D629F2&displaylang=es

   Automated Installation Kit (AIK) para Windows Vista SP1 y Windows Server 2008 (PE 2.1):

   http://www.microsoft.com/downloads/details.aspx?FamilyID=94bb6e34-d890-4932-81a5-5b50c657de08&DisplayLang=es

   Automated Installation Kit (AIK) para Windows 7 (PE 3.0):

   http://www.microsoft.com/DOWNLOADS/details.aspx?familyid=696DD665-9F76-4177-A811-39C26D3B3B34&displaylang=es

   Complemento de Automated Installation Kit (AIK) para Windows 7 SP1 (PE 3.1):

   http://www.microsoft.com/es-es/download/details.aspx?id=5188

   Puede encontrar los requisitos del sistema para la instalación en los siguientes enlaces.
2. [Opcional] Grabe el WAIK en un DVD o cópielo en una unidad de memoria flash.
3. Instale Microsoft .NET Framework desde este kit (NETFXx86 o NETFXx64, según su hardware).
4. Instale el analizador de Microsoft Core XML (MSXML) 5.0 o 6.0 de este kit.
5. Instale Windows AIK de este kit.
6. Instale Bootable Media Builder en el mismo equipo.

Es recomendable que se familiarice con la documentación de ayuda suministrada con Windows AIK. Para tener acceso a la documentación, seleccione **Microsoft Windows AIK -> Documentación** desde el menú de inicio.

11.1.2.2 Preparación: WinPE 4.0 y posterior

Para poder crear o modificar las imágenes de PE 4 o posterior, instale Bootable Media Builder en un equipo que tenga instalado Windows Assessment and Deployment Kit (ADK). Si no tiene un equipo con ADK, prepárelo de la siguiente manera:

Para preparar un equipo con ADK

1. Descargue el programa de instalación de Assessment and Deployment Kit.

   Assessment and Deployment Kit (ADK) para Windows 8 (PE 4.0):
   http://www.microsoft.com/es-es/download/details.aspx?id=30652.

   Assessment and Deployment Kit (ADK) para Windows 8.1 (PE 5.0):
   http://www.microsoft.com/es-ES/download/details.aspx?id=39982.

Assessment and Deployment Kit (ADK) para Windows 10 (PE para Windows 10): https://msdn.microsoft.com/es-es/windows/hardware/dn913721%28v=vs.8.5%29.aspx.

Puede encontrar los requisitos del sistema para la instalación en los enlaces anteriores.

2. Instale Assessment and Deployment Kit en el equipo.
3. Instale Bootable Media Builder en el mismo equipo.

11.1.2.3 Incorporación del complemento de Acronis a WinPE

Para incorporar el complemento de Acronis a WinPE:

1. Inicie Bootable Media Builder.
2. Especifique las claves de licencia. Las claves de licencia no se asignarán ni volverán a asignarse. Determinan la funcionalidad que se habilitará para el dispositivo creado. Sin las claves de licencia, solo podrá crear medios para 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 la interfaz extensible del firmware unificada (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 en 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 una línea de comando si la utilidad **acrocmd** se ejecuta en un equipo distinto. Si deja estas casillas vacías, la conexión remota a través de la interfaz de la línea de comando se deshabilitará.

   Estas credenciales también son necesarias al registrar el dispositivo en el servidor de gestión desde la consola de copia de seguridad (pág. 228).
7. Especifique las configuraciones de red (pág. 222) de los adaptadores de red del equipo o elija la configuración automática DHCP.
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" (pág. 221).
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. Para utilizar 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 cópielo en una unidad flash.

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
```

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.

11.2 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" (pág. 228).

11.3 Registro de dispositivos en el servidor de gestión

El registro de dispositivos de arranque le permite gestionar los dispositivos a través de la consola de copia de seguridad 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 Backup al servidor de gestión.

Puede registrar los dispositivos desde la consola de la copia de seguridad o desde la IU de los dispositivos.

Se pueden configurar con antelación los parámetros de registro en la opción servidor de gestión (pág. 221) de Bootable Media Builder. Si se configuran con anterioridad todos los parámetros de registro, los dispositivos aparecerán en la consola de copia de seguridad 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 consola de copia de seguridad

Los dispositivos deben crearse con Bootable Media Builder (pág. 210). Se debe especificar un nombre de usuario y contraseña para una conexión remota en la opción **Configuraciones de inicio de sesión remoto** de Bootable Media Builder.

Para registrar dispositivos desde la consola de copia de seguridad

1. Inicie el equipo desde el disco o la unidad USB. Anote la dirección IP que se muestra en la ventana de inicio.
2. En la consola de copias de seguridad, haga clic en **Añadir**.
3. Vaya hacia abajo a **Dispositivos de arranque** y, a continuación, haga clic en **Registrar un equipo iniciado desde un dispositivo de arranque**.
4. Introduzca la dirección IP del equipo iniciado desde los dispositivos de arranque.

5. Introduzca el nombre de usuario y la contraseña que se especificaron al crear el dispositivo, en la opción **Configuraciones de inicio de sesión remoto** de Bootable Media Builder.
6. Seleccione el nombre o la dirección IP que el medio 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 en el registro de medios.
7. Haga clic en **Agregar**.

Registro de los dispositivos desde la IU del dispositivo

Se puede crear o descargar el dispositivo con Bootable Media Builder (pág. 210).

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** > **Administradores**). En la consola de copia de seguridad, 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 de copia de seguridad. 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 el nombre de dominio completamente cualificado (FQDN) o la dirección IP del equipo.
6. Haga clic en **Aceptar**.

11.4 Configuración de los dispositivos iSCSI y NDAS

Esta sección describe cómo configurar los dispositivos de la Internet Small Computer System Interface (iSCSI) y los de Network Direct Attached Storage (NDAS) 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.

Para añadir un dispositivo NDAS (solo en un dispositivo de arranque basado en Linux):

1. Haga clic en **Herramientas** > **Configurar dispositivos iSCSI/NDAS**.
2. Haga clic en **Dispositivos NDAS** y, a continuación, en **Agregar dispositivo**.
3. Especifique el ID de 20 caracteres del dispositivo.
4. Para desea permitir datos de escritura en el dispositivo, especifique la clave de escritura de cinco caracteres. Sin esta clave, el dispositivo solo estará disponible en el modo de solo lectura.
5. Haga clic en **Aceptar**.
6. Haga clic en **Cerrar** para cerrar la ventana.

11.5 Startup Recovery Manager

Startup Recovery Manager es un componente de arranque que reside en el disco del sistema en Windows o en la partición /boot en Linux y está configurado para iniciarse en el tiempo de arranque al pulsar F11. Elimina la necesidad disponer de un dispositivo o conexión de red para ejecutar la utilidad de rescate de inicio.

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 Acronis Startup Recovery Manager…" y, a continuación, pulse F11. El programa se iniciará y puede realizar la recuperación.

También puede realizar copias de seguridad con Startup Recovery Manager mientras esté en movimiento.

En equipos con el cargador de arranque GRUB instalado, seleccione Startup Recovery Manager en el menú de arranque en lugar de pulsar F11.

Los equipos arrancados con Startup Recovery Manager se pueden registrar en el servidor de gestión de forma similar a los equipo que se han iniciado desde el dispositivo de arranque. Para hacerlo, haga clic en **Herramientas** > **Registrar dispositivo en el servidor de gestión** y, a continuación, siga el procedimiento paso a paso descrito en la sección "Registro de dispositivos en el servidor de gestión" (pág. 228).

Activación de Startup Recovery Manager

En un equipo que ejecute Agente para Windows o Agente para Linux, se puede activar Startup Recovery Manager mediante la consola de copia de seguridad.

Para activar Startup Recovery Manager en la consola de copia de seguridad:

1. Seleccione el equipo en el que desea activar Startup Recovery Manager.
2. Haga clic en **Detalles**.
3. Habilite el conmutador **Startup Recovery Manager**.
4. Espere mientras el software activa Startup Recovery Manager.

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.

Qué sucede al activar Startup Recovery Manager

La activación habilita el mensaje de tiempo de arranque "Pulse F11 para Startup Recovery Manager…" (si no tiene el cargador de arranque GRUB) o añade el elemento "Startup Recovery Manager" al menú de GRUB (si tiene GRUB).

El disco del sistema (o la partición /boot en Linux) debe tener por lo menos 100 MB de espacio libre para activar Startup Recovery Manager.

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 MRB con su propio código de arranque. Por lo tanto, necesitará activar nuevamente cargadores de inicio de terceros, si están instalados.

En Linux, si utiliza un cargador de arranque que no sea GRUB (como LILO), considere instalarlo en un registro de arranque de partición de raíz (o arranque) de Linux en lugar del MBR antes de activar Startup Recovery Manager. De lo contrario, vuelva a configurar este cargador de inicio manualmente después de la activación.

Desactivación de Startup Recovery Manager

La desactivación se realiza de forma similar a la activación.

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, deberá 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).

11.6 Acronis PXE Server

Acronis PXE Server 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 mediante 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" (pág. 211).

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.

11.6.1 Instalación de Acronis PXE Server

Para instalar Acronis PXE Server

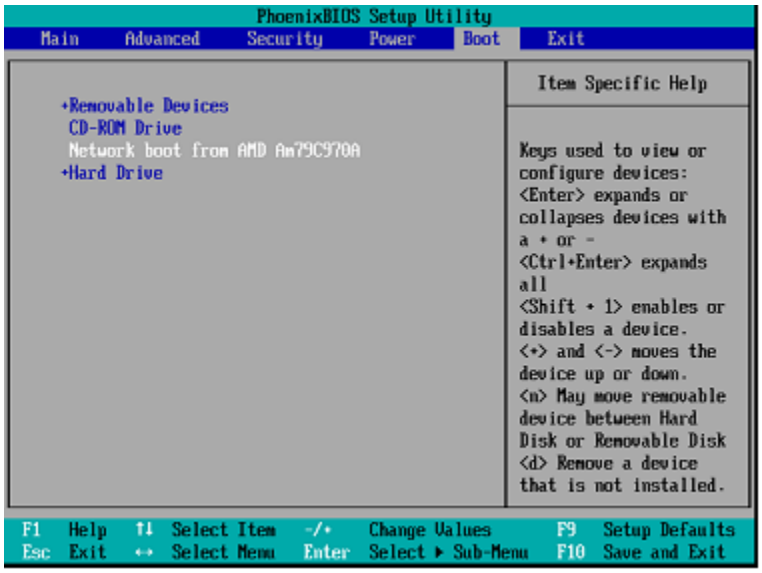
1. Inicie sesión como administrador e inicie el programa de instalación de Acronis Backup.
2. [Opcional] Para cambiar el idioma del programa de instalación, haga clic en **Idioma de instalación**.
3. Acepte los términos del acuerdo de licencia y seleccione si el equipo participará en el Programa de experiencia del cliente (PEC) de Acronis.
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 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.

11.6.2 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.

11.6.3 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://support.microsoft.com/en-us/help/257579/pxe-clients-do-not-receive-an-ip-address-from-a-dhcp-server.

12 Protección de dispositivos móviles

Para realizar una copia de seguridad y recuperar los datos de sus dispositivos móviles, utilice la aplicación de copia de seguridad.

Dispositivos móviles compatibles

- Smartphones y tablets con el sistema operativo Android 4.1 o posterior.
- iPhones, iPads y iPods con el sistema operativo iOS 8 o posterior.

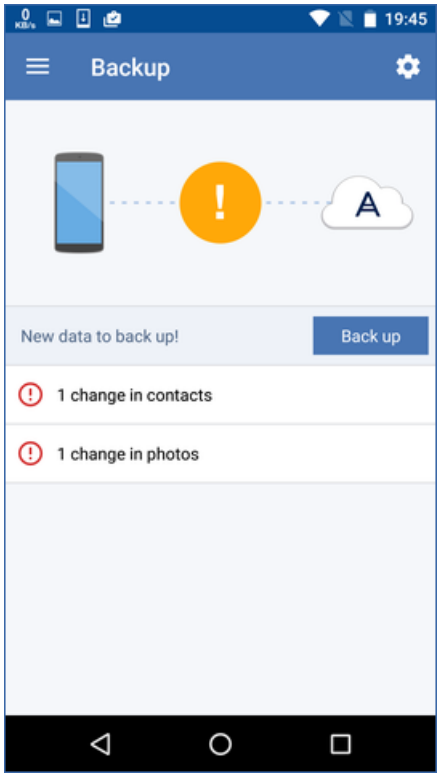
De qué puede realizar una copia de seguridad

- Contactos

- Fotografías
- Vídeos
- Calendarios
- Mensajes de texto (solo en dispositivos Android)
- Recordatorios (solo en dispositivos iOS)

Qué necesita saber

- Puede realizar una copia de seguridad de los datos solo en el almacenamiento en la cloud.
- En cualquier momento que abra la aplicación, verá el resumen de cambios en los datos y podrá iniciar manualmente una copia de seguridad.



- La funcionalidad **Copia de seguridad continua** se encuentra habilitada de forma predeterminada. En este modo, la aplicación de copia de seguridad comprobará si hay cambios en los datos cada seis horas y realizará una copia de seguridad automáticamente si cambian algunos datos. Puede desactivar la copia de seguridad continua o cambiar al modo **Solo cuando esté cargando** en la configuración de la aplicación para dispositivos móviles.
- 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 fotografía, vídeo o contacto en un equipo utilizando la consola de copias de seguridad.
- 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 para dispositivos móviles, puede recuperar los datos solo desde la última copia de seguridad. Si necesita recuperar datos de copias de seguridad más antiguas, utilice la consola de copias de seguridad en un tablet o en un equipo.
- No se aplican las reglas de retención a las copias de seguridad de dispositivos móviles.

- Si hay una tarjeta SD presente durante la copia de seguridad, también se podrá realizar una copia de seguridad de los datos almacenados en esta tarjeta. Los datos se recuperarán en una tarjeta SD si está presente durante dicho proceso. En caso contrario, se guardarán en el almacenamiento interno.
- Los datos se recuperarán al almacenamiento interno, independientemente de si los datos originales estaban ubicados en el almacenamiento interno del dispositivo o en la tarjeta SIM.

Instrucciones paso a paso

Para 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 la cuenta Acronis.
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.

Para iniciar una copia de seguridad de un dispositivo iOS

1. Abra la aplicación de copias de seguridad.
2. Inicie sesión con la cuenta Acronis.
3. Seleccione las categorías de datos de las que desea realizar la copia de seguridad. De manera predeterminada, se seleccionan todas las categorías.
4. Pulse **Crear copia de seguridad ahora**.
5. 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.

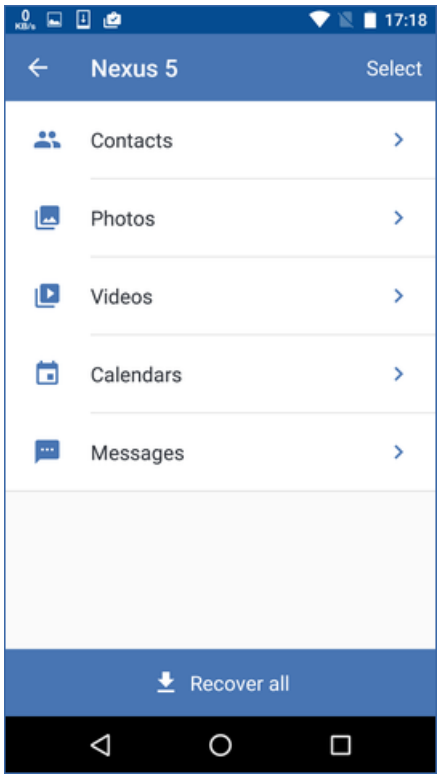
Para iniciar una copia de seguridad de un dispositivo Android

1. Abra la aplicación de copias de seguridad.
2. Inicie sesión con la cuenta Acronis.
3. [Solo en dispositivos Android 6.0 y posterior] 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.
4. [Opcional] Seleccione las categorías de datos que no desea incluir en la copia de seguridad. Para ello, pulse el icono de engranaje, después el control deslizante de las categorías de datos que desea excluir de la copia de seguridad y, finalmente, la flecha atrás.
5. Pulse **Crear copia de seguridad**.

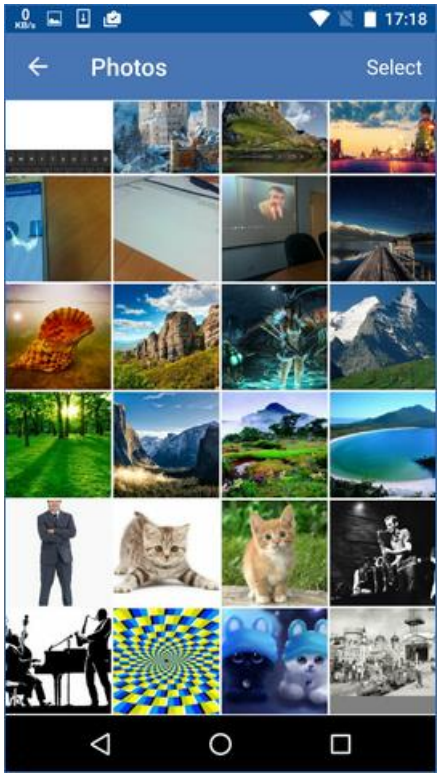
Para recuperar los datos a un dispositivo móvil

1. Abra la aplicación de copias de seguridad.
2. Deslice el dedo hacia la derecha y, después, pulse **Acceso y recuperación**.
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.



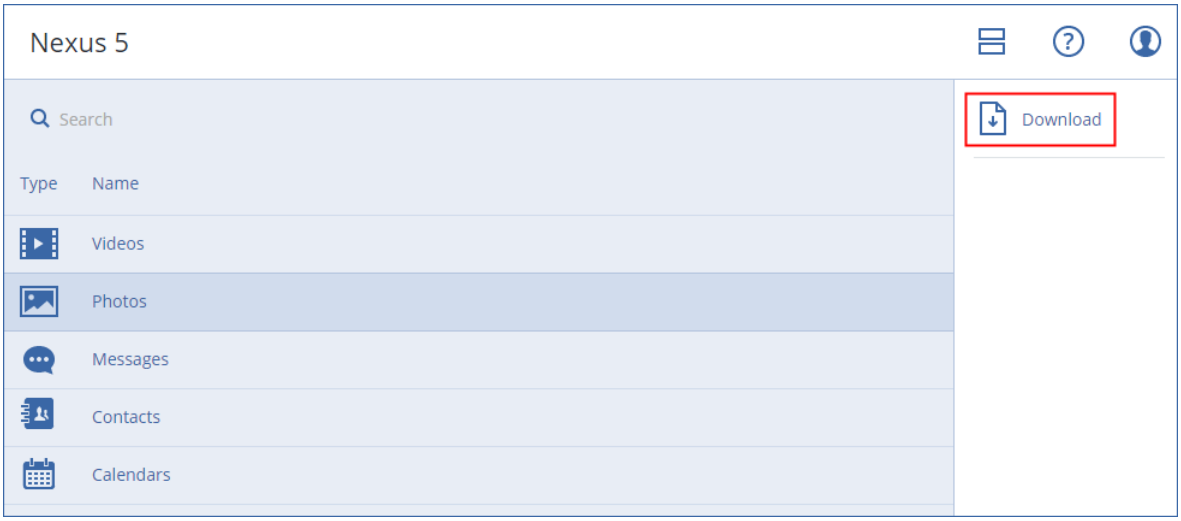
5. Realice uno de los siguientes procedimientos:
   - Para recuperar un único elemento, púlselo.
   - Para recuperar varios elementos, pulse **Seleccionar** y después seleccione las casillas de verificación de los elementos elegidos.



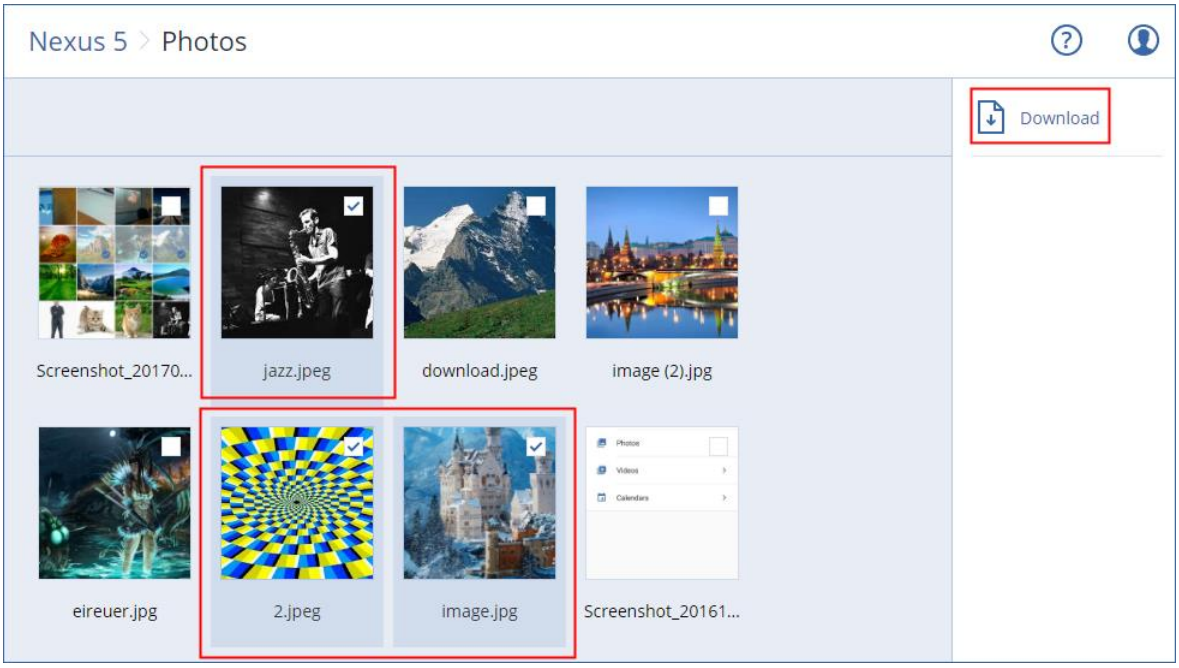
6. Pulse **Recuperar**.

Para acceder a los datos a través de la consola de copias de seguridad

1. En un equipo, abra un explorador y vaya a https://backup.acronis.com/.
2. Inicie sesión con la cuenta Acronis.
3. En **Todos los dispositivos**, seleccione el nombre de su dispositivo móvil y, a continuación, haga clic en **Recuperación**.
4. Seleccione el punto de recuperación.
5. Realice una de las siguientes operaciones:
   - Para descargar todas las fotografías, todos los vídeos o contactos, seleccione las categorías de datos correspondientes. Haga clic en **Descargar**.



   - Para descargar fotografías, vídeos o contactos uno a uno, seleccione el nombre de la categoría de datos correspondiente y, después, seleccione las casillas de verificación de los elementos elegidos. Haga clic en **Descargar**.



   - Para ver una vista preliminar de un mensaje de texto, una fotografía o un contacto, seleccione el nombre de la categoría de datos correspondiente y haga clic en el elemento elegido.

Para obtener más información, consulte http://www.acronis.com/redirector/products/atimobile/docs/?lang=es. Esta ayuda también está disponible es la aplicación de copia de seguridad (pulse **Configuración** > **Ayuda** en el menú de la aplicación para dispositivos móviles).

13 Protección de aplicaciones de Microsoft

Importante *Algunas de las funciones descritas en esta sección se introdujeron en la versión 12.5, que afecta solo a las implementaciones en una instalación. Estas funciones todavía no están disponibles en las implementaciones en la nube. Para obtener más información, consulte "Novedades en Acronis Backup" (pág. 8).*

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 copias de seguridad 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 Office 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 (pág. 248) Bases de datos como archivos (pág. 248)	Todo el equipo (pág. 157) Bases de datos a una instancia activa de SQL Server (pág. 248) Bases de datos como archivos (pág. 248)	Todo el equipo (pág. 157)
Microsoft Exchange Server	Bases de datos a un servidor activo de Exchange (pág. 252) Bases de datos como archivos (pág. 252) Recuperación granular a un servidor activo de Exchange Server u Office 365 (pág. 254)*	Todo el equipo (pág. 157) Bases de datos a un servidor activo de Exchange (pág. 252) Bases de datos como archivos (pág. 252) Recuperación granular a un servidor activo de Exchange Server u Office 365 (pág. 254)*	Todo el equipo (pág. 157)
Servidores de bases de datos de Microsoft SharePoint	Bases de datos a una instancia activa de SQL Server (pág. 248) Bases de datos como archivos (pág. 248) Recuperación granular mediante SharePoint Explorer	Todo el equipo (pág. 157) Bases de datos a una instancia activa de SQL Server (pág. 248) Bases de datos como archivos (pág. 248) Recuperación granular mediante SharePoint Explorer	Todo el equipo (pág. 157)
Servidor web front-end de Microsoft SharePoint	-	-	Todo el equipo (pág. 157)
Servicios de dominio de Active Directory	-	Todo el equipo (pág. 157)	-

* La recuperación granular también está disponible a partir de la copia de seguridad de un buzón de correo.

13.1 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.

En un controlador de dominio, asegúrese de que:

- El escritor de Active Directory para VSS esté activado.

Al crear un plan de copias de seguridad, asegúrese de que:

- En los equipos físicos, la opción de copia de seguridad Volume Shadow Copy Service (VSS) (pág. 154) esté habilitada.
- En los equipos virtuales, la opción de copia de seguridad Volume Shadow Copy Service (VSS) para equipos virtuales (pág. 155) esté habilitada.

Otros requisitos para copias de seguridad compatibles con la aplicación

Al crear un plan de copias de seguridad, compruebe que **Todo el equipo** esté seleccionado para la copia de seguridad.

Si las aplicaciones se ejecutan en equipos virtuales de los que Agente para VMware hace una copia de seguridad, asegúrese de que:

- Los equipos virtuales de los que se va a realizar una copia de seguridad cumplen los requisitos de inactividad coherente con la aplicación y aparecen en el siguiente artículo de la base de conocimientos de VMware: https://pubs.vmware.com/vsphere-6-5/index.jsp?topic=%2Fcom.vmware.vddk.pg.doc%2FvddkBkupVadp.9.6.html
- Las herramientas de VMware están instaladas y actualizadas en los equipos.
- El control de cuentas de usuario (UAC) está deshabilitado en los equipos. 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.

13.2 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" (pág. 239).

Seleccione las bases de datos tal como se describe a continuación y luego especifique otros ajustes del plan de copias de seguridad según corresponda (pág. 87).

13.2.1 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 copias de seguridad (pág. 138).

Para seleccionar bases de datos de SQL

1. Haga clic en **Dispositivos** > **Microsoft SQL**.

   El software muestra el árbol de los grupos de disponibilidad AlwaysOn (AAG) de SQL Server, equipos que ejecutan Microsoft SQL Server, instancias de SQL Server y bases de datos.
2. Busque los datos de los que desea realizar la copia de seguridad.

   Expanda los nodos del árbol o haga doble clic en los elementos de la lista de la parte derecha del árbol.
3. Seleccione los datos de los que desea realizar la copia de seguridad. Puede seleccionar los AAG, equipos que ejecuten SQL Server, instancias de SQL Server o bases de datos individuales.
   - Si selecciona un AAG, se realizará una copia de seguridad de todas las bases de datos que se incluyan en el AAG seleccionado. Para obtener más información acerca de la copia de seguridad de los AAG, consulte "Protección de los grupos de disponibilidad AlwaysOn (AAG)" (pág. 242).
   - Si selecciona un equipo que ejecute 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 **Copia de seguridad**. Si se le pide, proporcione las credenciales para acceder a los datos de SQL Server. 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.

13.2.2 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 del registro de transacciones se truncan después de cada copia de seguridad correcta.

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" (pág. 247), 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)" (pág. 244).
   - 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" (pág. 247), puede seleccionar los buzones de correo para la copia de seguridad (pág. 248).
4. Si se le pide, proporcione las credenciales para acceder a los datos.
5. Haga clic en **Copia de seguridad**.

13.2.3 Protección de los grupos de disponibilidad AlwaysOn (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

Acronis Backup es compatible *solo* grupo de disponibilidad AlwaysOn (AAG) para SQL Server 2012 o posterior. Otras configuraciones de clúster, tales como instancia del clúster de conmutación por error, creación de reflejo de la base de datos y trasvase de registros *no* son compatibles.

¿Cuántos agentes se necesitan para la copia de seguridad y recuperación de los datos del clúster?

Para una copia de seguridad y recuperación de datos correcta de un clúster, Agent for SQL debe estar instalado en cada nodo del clúster de WSFC.

Copias de seguridad de bases de datos incluidas en AAG

1. Instale Agent por SQL en cada nodo del clúster WSFC.

   Consejo *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 para realizar una copia de seguridad según se describe en «Seleccionar bases de datos SQL" (pág. 241).

   Importante *Debe seleccionar el propio AAG, en lugar de los nodos o las bases de datos individuales contenidos dentro de este. Si selecciona los elementos individuales dentro del AAG, la copia de seguridad no será compatible con el clúster y solo las copias seleccionadas y solo se realizarán copias de seguridad de los elementos.*

3. Configure la opción de copia de seguridad «Modo de copia de seguridad de clústeres» (pág. 132)

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 Copias de seguridad (pág. 199). Los nombres de copias de seguridad del AAG están basados en la plantilla siguiente `<nombre del AAG> - <nombre del plan de copias de seguridad>` y tienen un icono especial.

2. Para configurar la recuperación, siga los pasos descritos en «Recuperación de base de datos SQL» (pág. 248), a partir del paso 5.

El software define automáticamente un nodo de clúster en donde se recuperarán los datos. El nombre del nodo se visualizará en el campo **Recuperar a**. Puede cambiar manualmente el nodo de destino.

Importante *Microsoft SQL Server no permite que se sobrescriba una base de datos incluida en un grupo de disponibilidad AlwaysOn durante una recuperación. Debe excluir la base de datos de destino del AAG antes de la recuperación. O bien, puede recuperar la base de datos como una nueva que no pertenezca al AAG. Una vez que se haya completado la recuperación, puede restablecer la configuración original del AAG.*

13.2.4 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.

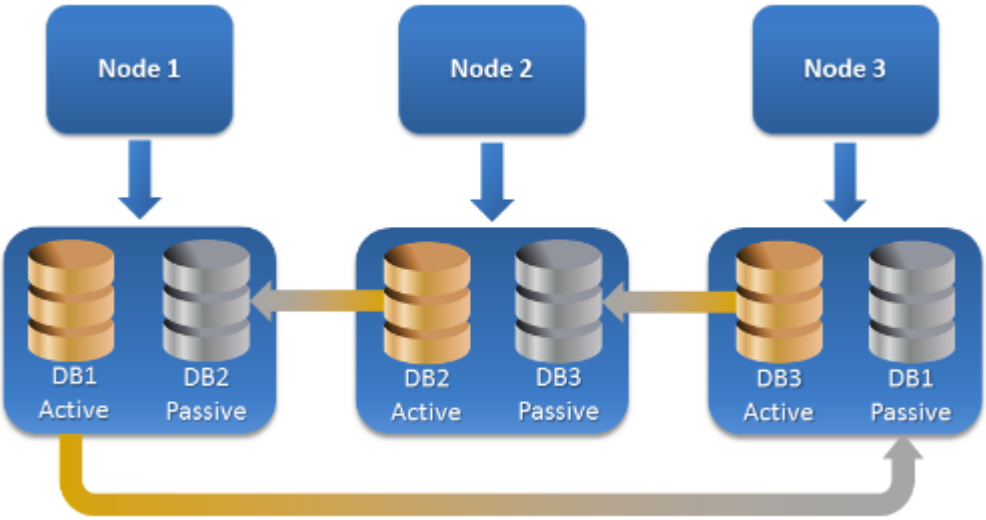
Copia de seguridad compatible con el clúster

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.

Consejo *Después de instalar el agente en uno de los nodos, la consola de copias de seguridad 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 copias de seguridad, seleccione el DAG según se describe en "Seleccionar datos de Exchange Server" (pág. 241).
2. Configure la opción de copia de seguridad «Modo de copia de seguridad de clústeres» (pág. 132)
3. Especifique las demás opciones de configuración del plan de copias de seguridad según corresponda (pág. 87).

Importante *Para la copia de seguridad compatible con el clúster, asegúrese de seleccionar el propio DAG. Si selecciona nodos individuales o bases de datos dentro del DAG, solo se realizará la copia de seguridad de los elementos seleccionados y se omitirá la opción* ***Modo de copia de seguridad de clústeres****.*

Recuperación de los datos del clúster de Exchange

1. Seleccione el punto de recuperación de la base datos que desea recuperar. No se puede seleccionar todo un clúster para la recuperación.

   Al seleccionar una copia de una base de datos en clúster en **Dispositivos** > **Microsoft Exchange** > **Bases de datos** > `<nombre de clúster>` > `<nombre de nodo>` y hacer clic en **Recuperar**, el software muestra solo los puntos de recuperación que se correspondan con las horas a las que se realizó la copia de seguridad de la copia.

   La manera más fácil para ver todos los puntos de recuperación de una base de datos en clúster es seleccionar su copia de seguridad en la pestaña Copias de seguridad (pág. 199).
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.

13.3 Copia de seguridad compatible con la aplicación

La copia de seguridad a nivel de disco compatible con la aplicación está disponible para equipos físicos y para equipos virtuales ESXi.

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 copias de seguridad (pág. 138). Los registros de transacción de Exchange solo se truncan en los equipos virtuales. Puede habilitar la opción de copia de seguridad completa de VSS (pág. 154) 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 Agente para VMware (Windows) hace una copia de seguridad del equipo.

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 **Copias de seguridad** y, a continuación, seleccione este equipo en **Equipo desde el cual examinar**.

En las secciones "Requisitos previos" (pág. 239) y "Derechos de usuario necesarios" (pág. 247) se recogen otros requisitos.

13.3.1 Derechos de usuario necesarios

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 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.
- Para Exchange Server:

  Exchange 2007: La cuenta debe pertenecer al grupo de roles **Administradores de la organización de Exchange**.

  Exchange 2010 y posterior: La cuenta debe pertenecer al grupo de roles **Gestión de la organización**.
- Para Active Directory:

  La cuenta debe ser un administrador de dominios.

13.4 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.

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.
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 (pág. 248).
10. Haga clic en **Agregar**.

Como resultado, los buzones de correo aparecen bajo **Dispositivos** > **Microsoft Exchange** > **Buzones de correo**.

13.4.1 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 copias de seguridad según corresponda (pág. 87).

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**.

13.4.2 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 al grupo de funciones **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.

13.5 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. 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.

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" (pág. 251).

Si solo usa Agente para VMware, el único método de recuperación disponible será la recuperación de bases de datos como archivos.

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" (pág. 251).

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 copias de seguridad (pág. 199).

   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] 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 copias de seguridad (pág. 199).

   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**.

13.5.1 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.

13.5.2 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**.

13.6 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 (pág. 254).

Si solo usa Agente para VMware, el único método de recuperación disponible será la recuperación de bases de datos como archivos.

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 copias de seguridad (pág. 199).

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 copias de seguridad (pág. 199).

   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**.

13.6.1 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). Al recuperar una base de datos en una ubicación alternativa (como una base de datos nueva o la base de datos de recuperación), la base de datos no se podrá montar hasta que su estado sea Cierre correcto utilizando el comando **`Eseutil /r <Enn>`**. **`<Enn>`** especifica el prefijo del archivo de registro para la base de datos (o grupo de almacenamiento que contiene la base de datos) en la que usted necesita aplicar los archivos del 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

13.7 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 Office 365.

Se pueden recuperar los siguientes elementos:

- Buzones de correo (salvo los buzones de correo de archivo)
- Carpetas públicas
- 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 para las cuentas de usuario

Un buzón de correo que se recupera desde una copia de seguridad debe tener una cuenta de usuario asociada en Active Directory.

Los buzones de correo del usuario y su contenido solo pueden recuperarse si las cuentas de usuario asociadas están *habilitadas*. Los buzones de correo compartidos, de sala y equipo pueden recuperarse solo si sus cuentas de usuario asociadas están *deshabilitadas*.

Un buzón de correo que no cumpla con las condiciones anteriores se omitirá durante la recuperación.

Si se omiten algunos buzones de correo, la recuperación finalizará correctamente con advertencias. Si se omiten todos los buzones de correo, la recuperación fallará.

Recuperación a Office 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 Office 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 Office 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 Office 365, consulte "Proteger los buzones de correo de Office 365" (pág. 261).

13.7.1 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 Office 365] Si el Agente para Office 365 no está instalado en el equipo que ejecuta Exchange Server y del que se ha realizado la copia de seguridad, realice 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" (pág. 260).
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 copias de seguridad (pág. 199).

   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 realizar la recuperación a Office 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.

   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 la sección Derechos de usuario necesarios (pág. 248).
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 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 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 Copias de seguridad (pág. 199) 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.

13.7.2 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 Office 365] Si el Agente para Office 365 no está instalado en el equipo que ejecuta Exchange Server y del que se ha realizado la copia de seguridad, realice 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" (pág. 260).
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 copias de seguridad (pág. 199).

   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.

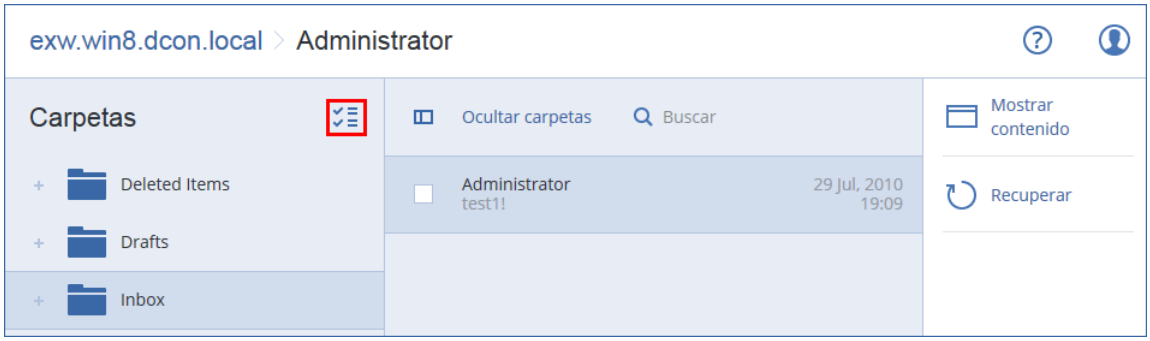
   Tiene a su disposición las siguientes opciones de búsqueda. No se pueden usar caracteres comodín.

   - 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.

   Consejo: *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 Office 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.

    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 la sección Derechos de usuario necesarios (pág. 248).
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**.
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 Copias de seguridad (pág. 199) 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.

    Consejo: *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.

13.7.3 Copia de bibliotecas de Microsoft Exchange Server

Al recuperar los buzones de correo de Exchange o los elementos de buzón de correo en Office 365 (pág. 254), puede que necesite copiar las bibliotecas siguientes 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.

Copie los archivos siguientes, en función de la versión de Microsoft Exchange Server de la que se ha realizado la copia de seguridad.

Versión de Microsoft Exchange Server	Bibliotecas	Ubicación predeterminada
Microsoft Exchange Server 2010	ese.dll esebcli2.dll store.exe	%ProgramFiles%\Microsoft\Exchange Server\V14\bin
Microsoft Exchange Server 2013	ese.dll	%ProgramFiles%\Microsoft\Exchange Server\V15\bin
	msvcr110.dll	%WINDIR%\system32
Microsoft Exchange Server 2016 y 2019	ese.dll	%ProgramFiles%\Microsoft\Exchange Server\V15\bin
	msvcr110.dll msvcp110.dll	%WINDIR%\system32

Las bibliotecas deben ubicarse en la carpeta **%ProgramData%\Acronis\ese**. Si esta carpeta no existe, créela manualmente.

13.8 Cambio de las credenciales de acceso de SQL Server o Exchange Server

Puede cambiar las credenciales de acceso de SQL Server o Exchange Server sin tener que volver a instalar el agente.

Para cambiar las credenciales de acceso de SQL Server o Exchange Server

1. Haga clic en **Dispositivos** y, a continuación, en **Microsoft SQL** o **Microsoft Exchange**.
2. Seleccione el Grupo de disponibilidad de AlwaysOn, el Grupo de disponibilidad de base de datos, la instancia de SQL Server o el equipo que ejecuta Microsoft 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** y, a continuación, en **Microsoft Exchange** > **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**.

14 Protección de los buzones de correo de Office 365

Motivos para hacer una copia de seguridad de los buzones de correo de Microsoft Office 365.

Si bien Microsoft Office 365 es un servicio en la cloud, las copias de seguridad regulares 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 Office 365 haya caducado. Asimismo, puede conservar una copia local de los buzones de correo de Office 365 si así lo requiere un cumplimiento normativo.

¿Qué necesito para realizar una copia de seguridad de los buzones de correo?

Para realizar copias de seguridad y recuperar buzones de correo de Office 365, debe tener el rol de administrador global en Microsoft Office 365.

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. En el caso de las implementaciones en la cloud, el agente debe estar registrado en la cuenta de administrador del nivel más alto (administrador de cliente).

- En el caso de las implementaciones en la cloud, indique las credenciales del administrador de cliente durante la instalación del agente y al iniciar sesión en la interfaz web.
- Indique las credenciales del administrador global de Office 365 en la página **Microsoft Office 365** de la interfaz web.

  El agente iniciará sesión en Office 365 usando esta cuenta. Para permitir que el agente acceda al contenido de los buzones de correo, se asignará el rol de gestión **ApplicationImpersonation** a esta cuenta.

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 Office 365 o a un servidor activo de Exchange Server.

Cuando se recupera un buzón de correo a un buzón de Office 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 copias de seguridad a más de 500 buzones de correo puede provocar una degradación del rendimiento de copia de seguridad. Para proteger un gran número de buzones de correo, crear varios planes de copias de seguridad y programarlos para ejecutarlos en momentos diferentes.
- No se puede realizar una copia de seguridad de los buzones de correo de archivo (**Archivo local**).
- No se admite la recuperación a un buzón de correo nuevo de Office 365. Primero debe crear un usuario de Office 365 nuevo manualmente y, después, recuperar los elementos en el buzón de correo del usuario.
- No se admite la recuperación a otra organización de Microsoft Office 365.
- Algunos tipos o propiedades de elementos admitidos en Office 365 podrían no ser compatibles con Exchange Server. Se omitirán en una recuperación a Exchange Server.

14.1 Selección de buzones de correo

Seleccione los buzones de correo tal como se describe a continuación y luego especifique otros ajustes del plan de copias de seguridad según corresponda (pág. 87).

Pasos para seleccionar buzones de correo

1. Haga clic en **Microsoft Office 365**.
2. Si así se le solicita, inicie sesión como administrador global en Microsoft Office 365.
3. Seleccione los buzones de correo de los que desea realizar una copia de seguridad.
4. Haga clic en **Copia de seguridad**.

14.2 Recuperación de buzones de correo y elementos de los buzones

14.2.1 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. Se describen otros requisitos para este usuario en "Recuperación de elementos de buzón de correo y de buzones de correo de Exchange" (pág. 254) bajo el epígrafe "Requisitos para las cuentas de usuario".
2. Haga clic en **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 Copias de seguridad (pág. 199) 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" (pág. 256), a partir del paso 9. No se requieren más pasos para este procedimiento.

   Para recuperar a Office 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**.

14.2.2 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 cuyos elementos de buzón de correo se están recuperando. De lo contrario, cree el usuario. Se describen otros requisitos para este usuario en "Recuperación de elementos de buzón de correo y de buzones de correo de Exchange" (pág. 254) bajo el epígrafe "Requisitos para las cuentas de usuario".
2. Haga clic en **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 Copias de seguridad (pág. 199) 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.

   Consejo: *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 Office 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 la sección Derechos de usuario necesarios (pág. 248).
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**.

14.3 Cambio de las credenciales de acceso de Office 365

Puede cambiar las credenciales de acceso de Office 365 sin tener que volver a instalar el agente.

Para cambiar la credenciales de acceso de Office 365

1. Haga clic en **Dispositivos** > **Microsoft Office 365**.
2. Seleccione la organización de Office 365.
3. Haga clic en **Especificar credenciales**.
4. Introduzca las credenciales del administrador global de Office 365 y haga clic en **Aceptar**.

   El agente iniciará sesión en Office 365 usando esta cuenta. Para permitir que el agente acceda al contenido de los buzones de correo, se asignará el rol de gestión **ApplicationImpersonation** a esta cuenta.

15 Protección de Oracle Database

La protección de Oracle Database se describe en un documento independiente disponible en http://dl2.acronis.com/u/pdf/AcronisBackup_12.5_OracleBackup_whitepaper.pdf

16 Active Protection

Importante *Algunas de las funciones descritas en esta sección se introdujeron en la versión 12.5, que afecta solo a las implementaciones en una instalación. Estas funciones todavía no están disponibles en las implementaciones en la nube. Para obtener más información, consulte "Novedades en Acronis Backup" (pág. 8).*

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.

Active Protection está disponible para los equipos que ejecutan Windows 7 y versiones posteriores, o Windows Server 2008 R2 y versiones posteriores. 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 que realiza un proceso con las cadenas de eventos registrados en la base de datos de los patrones de comportamiento malicioso. Este enfoque permite a Active Protection detectar malware nuevo identificando su comportamiento típico.

Configuración de Active Protection

Para minimizar los recursos consumidos por el análisis heurístico y para eliminar los llamados falsos positivos, cuando un programa de confianza se considera ransomware, puede definir la configuración siguiente:

- Procesos de confianza que nunca se consideran ransomware. Los procesos firmados por Microsoft siempre son de confianza.
- Procesos peligrosos que siempre se consideran ransomware. Estos procesos no podrán iniciarse mientras Active Protection esté habilitado en el equipo.
- Carpetas en las que no se controlarán los cambios de archivos.

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%.

Plan de Active Protection

Todas las opciones de configuración de Active Protection se incluyen en el plan de Active Protection. Este plan puede aplicarse a varios equipos.

En una organización solo puede haber un plan de Active Protection. Si la organización tiene unidades, los administradores de la unidad no tienen permiso para aplicar, editar o revocar el plan.

Aplicación del plan de Active Protection

1. Seleccione los equipos en los que desea habilitar Active Protection.
2. Haga clic en **Active Protection**.
3. [Opcional] Haga clic en **Editar** para modificar las opciones de configuración siguientes:
   - 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** (predeterminado)

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.

- En **Procesos peligrosos**, especifique los procesos peligrosos que siempre se considerarán ransomware y, a continuación, haga clic en **Realizado**.
- En **Procesos de confianza**, especifique los procesos de confianza que nunca se considerarán ransomware y, a continuación, haga clic en **Realizado**. Los procesos firmados por Microsoft siempre son de confianza.
- En **Exclusiones de carpetas**, especifique una lista de carpetas en la que no se controlarán los cambios de los archivos y, a continuación, haga clic en **Realizado**.
- Deshabilite el conmutador **Autoprotección**.

  Autoprotección evita los cambios no autorizados en los procesos propios del software, los archivos de registro, los archivos ejecutables y de configuración y las copias de seguridad que se encuentran en las carpetas locales. No recomendamos deshabilitar esta función.
- Cambiar las opciones de protección.

4. Si ha modificado la configuración, haga clic en **Guardar cambios**. Los cambios se aplicarán a todos los equipos en los que Active Protection esté habilitado.
5. Haga clic en **Aplicar**.

16.1 Opciones de protección

Copias de seguridad

Esta opción es válida cuando está activada la opción **Autoprotección** en el plan Active Protection.

Esta opción 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 resulta útil, por ejemplo, si elimina archivos de copia de seguridad o los mueve a una ubicación diferente con una secuencia de comandos.

El valor predeterminado es: **Habilitado**.

Si esta opción está habilitada, 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 deshabilitada, 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.

Protección frente a criptominería

Esta opción define si Active Protection detecta posibles casos de malware de criptominado.

El valor predeterminado es: **Habilitado**.

Si se detecta alguna actividad relacionada con la criptominería, se lleva a cabo la **acción sobre la detección** seleccionada (excepto revertir archivos de la caché, porque no hay nada que revertir).

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 criptominado a la lista de **procesos peligrosos** para evitar que se ejecute.

Dispositivos asignados

Esta opción define si Active Protection protege las carpetas de la red que están asignadas como dispositivos locales.

Esta opción se aplica a carpetas compartidas por SMB o NFS.

El valor predeterminado es: **Habilitado**.

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, asegúrese de especificar una carpeta local. No se admiten carpetas de red, ni siquiera las de dispositivos asignados.

17 Operaciones especiales con equipos virtuales

17.1 Ejecución de un equipo virtual desde una copia de seguridad (Instant Restore)

Nota *Esta funcionalidad solo está disponible con la licencia de Acronis Backup Advanced.*

Puede ejecutar un equipo virtual desde una copia de seguridad a nivel de disco que contenga un sistema operativo. Esta operación, también conocida como "recuperación 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 copia de seguridad.
- 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.

17.1.1 Ejecución del equipo

1. Realice uno de los siguientes procedimientos:
   - Seleccione un equipo incluido en la copia de seguridad, haga clic en **Recuperación** y, a continuación, seleccione un punto de recuperación.
   - Seleccione un punto de recuperación en la pestaña de copias de seguridad (pág. 199).
2. Haga clic en **Ejecutar como VM**.

   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.
5. [Opcional] Haga clic en **Configuración de VM** para modificar el tamaño de la memoria y las conexiones de red del equipo virtual.
6. [Opcional] Seleccione el estado de energía de un equipo virtual (**Activado**/**Apagado**).
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.

17.1.2 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.

17.1.3 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 copias de seguridad.

En un equipo ESXi, 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.

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. La configuración predeterminada es **Thin** (Fina).
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.

17.2 Trabajar en VMware vSphere

Esta sección describe operaciones que son específicas para entornos de VMware vSphere.

17.2.1 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 (pág. 274) 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** (pág. 272)

  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** (pág. 273)

  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.

17.2.1.1 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 icono del engranaje para modificar las opciones de replicación (pág. 274).
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: 

17.2.1.2 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.

17.2.1.3 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** (pág. 273)

  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** (pág. 273)

  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** (pág. 274)

  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 (pág. 275).
7. Haga clic en **Iniciar recuperación**.
8. Confirme su decisión.

17.2.1.4 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)" (pág. 132).

Aprovisionamiento del disco

Esta opción define los ajustes de aprovisionamiento del disco para la réplica.

El preajuste es: **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" (pág. 135).

Comandos previos/posteriores

Esta opción se parece a la opción de copia de seguridad "Comandos previos/posteriores" (pág. 144).

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" (pág. 155).

17.2.1.5 Opciones de conmutación por recuperación

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" (pág. 177).

Comandos pre/post

Esta opción se parece a la opción de recuperación "Comandos pre/post" (pág. 178).

Gestión de energía de VM

Esta opción se parece a la opción de recuperación "Gestión de energía de VM" (pág. 179).

17.2.1.6 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 (pág. 271).

   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 duro 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.

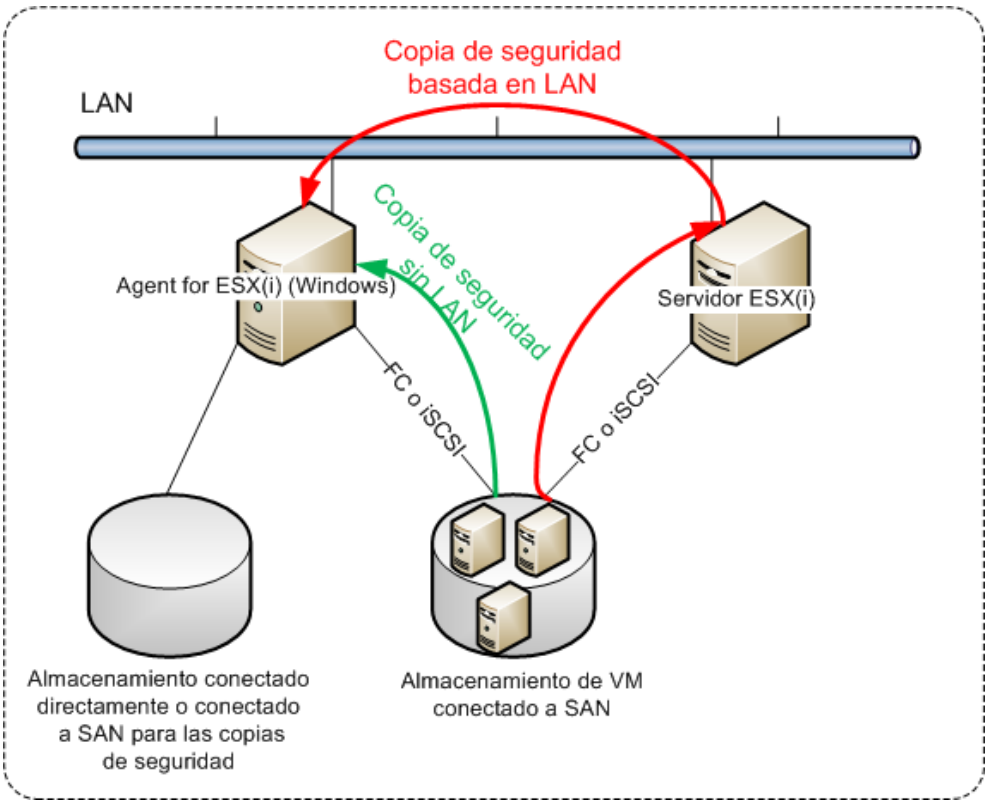
Como resultado, el software continuará actualizando la réplica. Todas las replicaciones serán incrementales.

17.2.2 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 símbolo del sistema, escriba **`diskpart`** y, a continuación, presione **Intro**.
2. Escriba **`san`** y, a continuación, presione **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

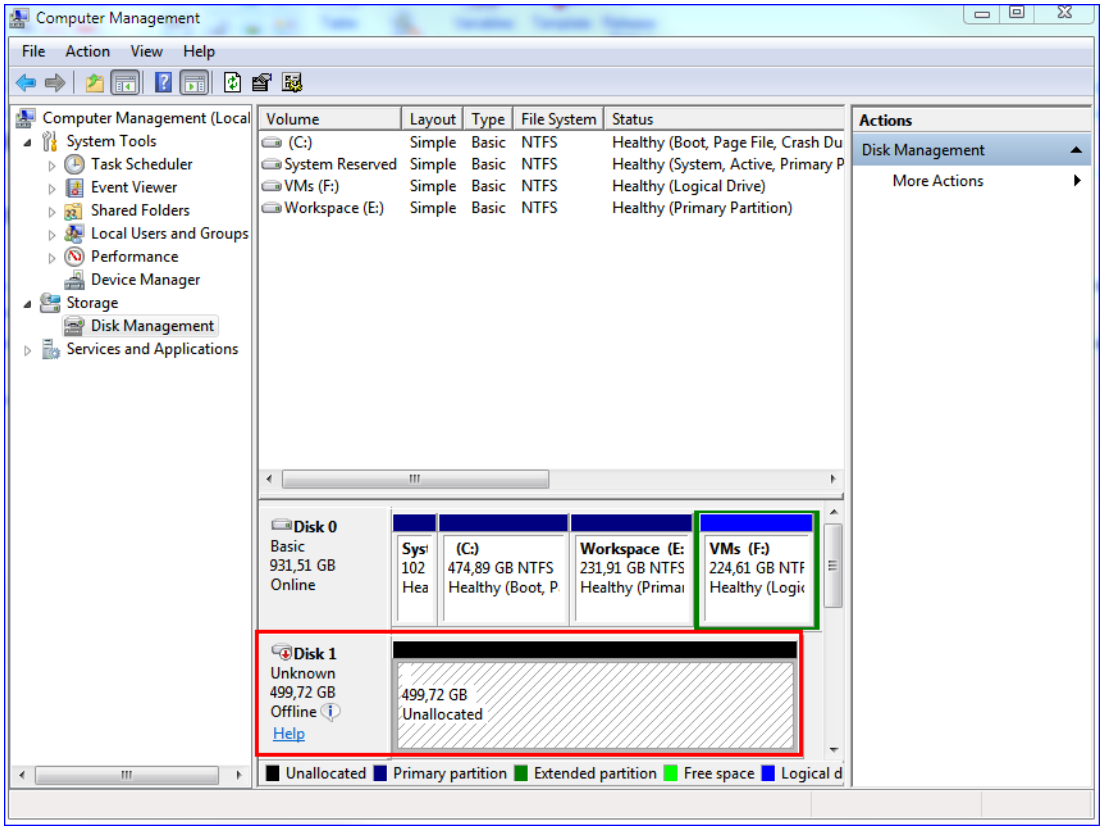
1. Vaya al **Panel de control** > **Herramientas administrativas** > **Iniciador de iSCSI**.

   Consejo: *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.



17.2.3 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?

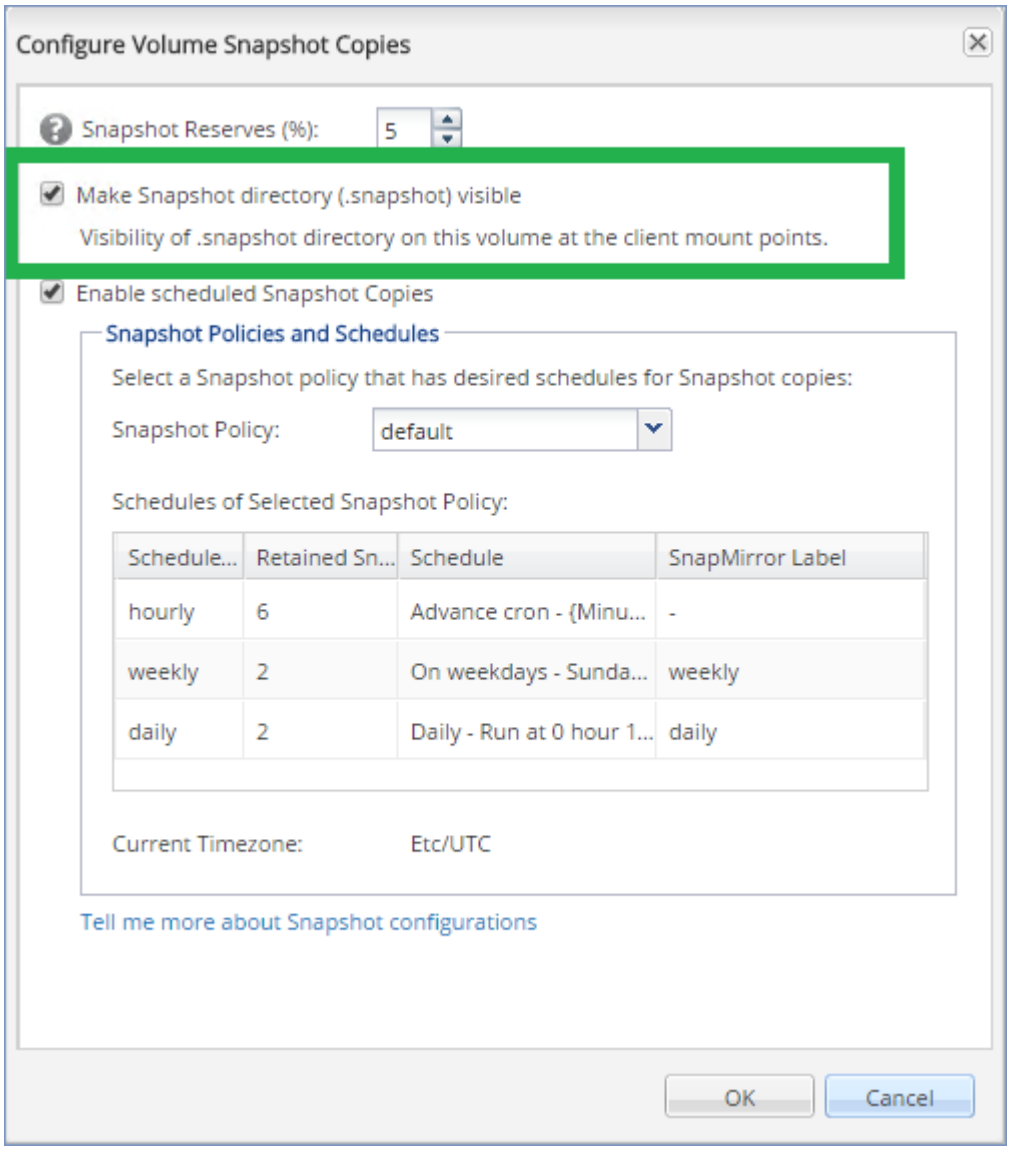
Si desea utilizar las instantáneas de hardware SAN al realizar copias de seguridad de equipos virtuales, asegúrese de que se cumplan todas las condiciones siguientes:

- El almacenamiento SAN de NetApp cumple los requisitos descritos en "Requisitos de almacenamiento NetApp SAN" (pág. 279).
- El equipo que ejecuta Agente para VMware (Windows) está configurado como se describe en "Configurar el equipo que ejecuta Agente para VMware" (pág. 281).
- El almacenamiento SAN está registrado en el servidor de gestión (pág. 282).
- [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" (pág. 283).
- La opción de copia de seguridad "Instantáneas de hardware SAN" (pág. 148) está habilitada en las opciones de plan de copias de seguridad.

17.2.3.1 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.

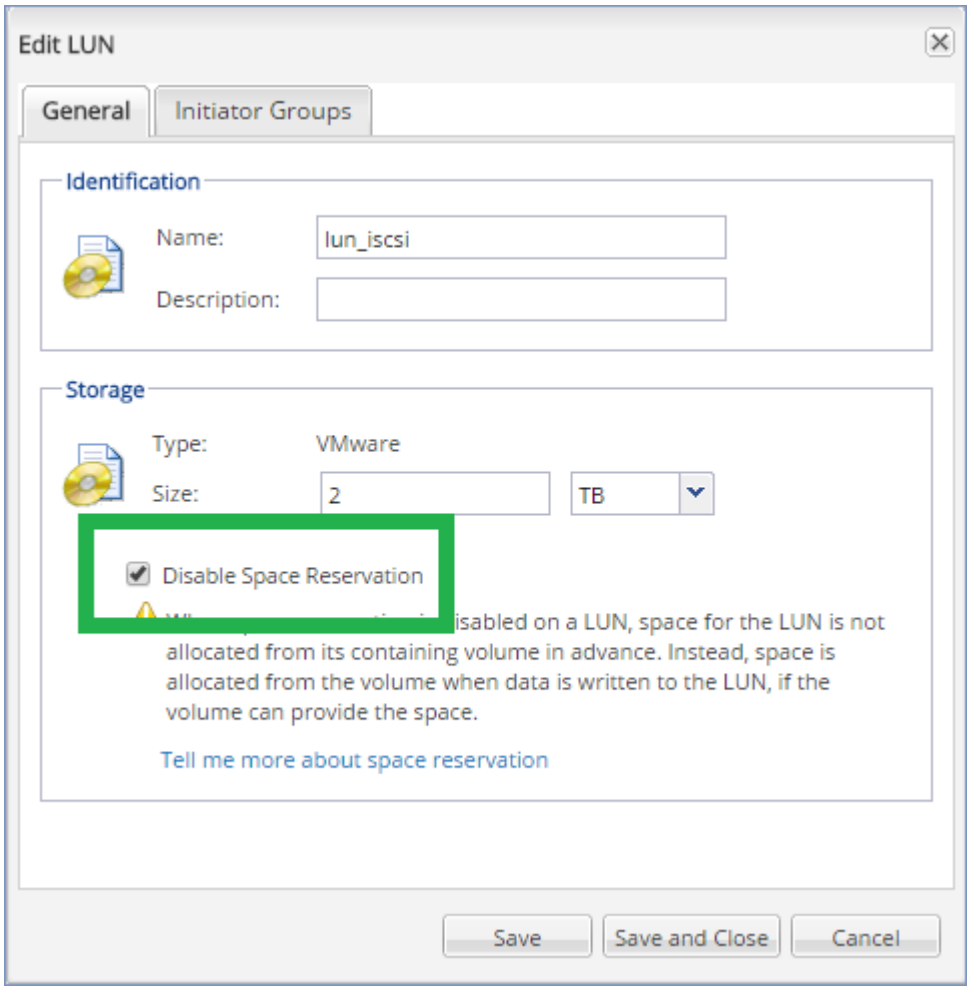


- [Para almacenes de datos NFS] El acceso a recursos compartidos NFS desde los clientes Windows NFSv3 debe estar habilitado en el Equipo Virtual de Almacenamiento (SVM) que se haya especificado al crear el almacén de datos. El acceso puede habilitarse mediante el siguiente comando:

```
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.



17.2.3.2 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" (pág. 276).

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).

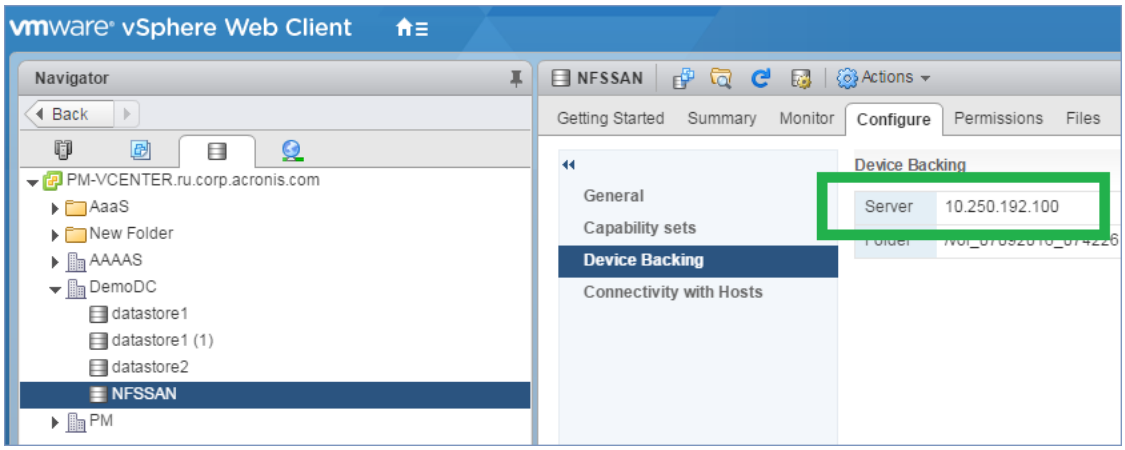
- El cliente NFS se ha configurado para acceso anónimo. Esto se puede realizar de la siguiente manera:
  a. Abra el Editor del registro.
  b. Busque la siguiente clave del registro: **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ClientForNFS\CurrentVersion\Default**
  c. En esta clave, cree un nuevo valor **DWORD** 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.

17.2.3.3 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**.

17.2.4 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 (pág. 283) 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 copias de seguridad (pág. 86), en **Dónde realizar copias de seguridad**, seleccione **Carpetas locales** y, a continuación, escriba la letra correspondiente al almacenamiento conectado localmente, por ejemplo, **D:**.

17.2.5 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 equipos**
- 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 (pág. 278). 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. (pág. 283)
- 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.

17.2.6 Cambio de las credenciales de acceso de vSphere

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**.

17.2.7 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. Agente para VMware (dispositivo virtual) solo está disponible para su implementación en una instalación.

Para realizar las operaciones en todos los servidores host y clústeres gestionados por un servidor vCenter Server, el Agente para VMware necesita los privilegios en el servidor vCenter Server. Si desea que el agente trabaje solo en un servidor host ESX específico, asigne al agente los mismos privilegios en el host.

Indique la cuenta con los privilegios necesarios durante la instalación o configuración de Agente para VMware. Si necesita cambiar la cuenta más tarde, consulte la sección "Cambio de las credenciales de acceso de vSphere" (pág. 285).

		Operación				
Objeto	**Privilegio**	**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 criptográficas (primeros pasos con vSphere 6.5)	**Agregar disco**	+*				
	Acceso directo	+*				
Almacén de datos	**Asignar espacio**		+	+	+	+
	Examinar almacén de datos				+	+
	Configurar los almacenes de datos	+	+	+	+	+
	Operaciones con archivos de bajo nivel				+	+
Global	**Licencias**	+	+	+	+	
	Deshabilitar métodos	+	+	+		

		Operación				
Objeto	**Privilegio**	**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**
	Habilitar métodos	+	+	+		
Servidor > Configuración	**Configuración de autoarranque de VM**					+
	Configuración de partición de almacenamiento				+	
Servidor > Inventario	**Modificar clúster**					+
Servidor > Operaciones locales	**Crear VM**				+	+
	Eliminar VM				+	+
	Reconfigurar VM				+	+
Red	**Asignar red**		+	+	+	+
Recurso	**Asignar equipo virtual a pool de recursos**		+	+	+	+
vApp	**Agregar equipo virtual**				+	
	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		+	+	+	

		Operación				
Objeto	**Privilegio**	**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**
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	+	+	+	+	

		Operación				
Objeto	**Privilegio**	**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**
Equipo virtual > **Estado**	**Crear instantánea**	+		+	+	+
	Eliminar instantánea	+		+	+	+

* 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.

17.3 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 físico	+	+	+
Equipo virtual VMware ESXi	+	+	+
Equipo virtual Hyper-V	+	+	+

Para obtener instrucciones sobre cómo realizar la migración, consulte las siguientes secciones:

- Physical-to-virtual (P2V) - "Equipo físico a virtual" (pág. 159)
- Virtual-to-virtual (V2V) - "Equipo virtual" (pág. 161)
- Virtual-to-physical (V2P) - "Equipo virtual" (pág. 161) o "Recuperación de discos usando dispositivos de arranque" (pág. 162)

Aunque es posible realizar la migración V2P en la interfaz web, se recomienda usar dispositivos de arranque 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.

17.4 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 copias de seguridad en el equipo. La copia de seguridad y la recuperación son iguales que en un equipo físico. No obstante, el equipo se cuenta como virtual al definir las cuotas del número de equipos en una implementación en la nube.

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" (pág. 157). 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 en una instalación

- 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 cloud, 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.

17.5 Limitar el número total de equipos virtuales que se incluyen en la copia de seguridad al mismo tiempo

La opción de copia de seguridad **Programación** (pág. 149) define cuántos equipos virtuales puede incluir el agente en la copia de seguridad simultáneamente al ejecutar un plan de copias de seguridad específico.

Si varios planes de copias de seguridad se superponen en el tiempo, se sumarán los números especificados en la copia de seguridad a las opciones. Aunque el número total resultante esté programáticamente limitado a 10, los planes que se superpongan pueden afectar al rendimiento de copia de seguridad y sobrecargar el host y el almacenamiento del equipo virtual.

Puede reducir el número total de equipos virtuales que un agente para VMware o un agente para Hyper-V puede incluir en la copia de seguridad al mismo tiempo.

Para limitar el número total de equipos virtuales que un agente para VMware (Windows) o un agente para Hyper-V puede incluir en la copia de seguridad:

1. En el equipo que en el que se ejecute el agente, cree un documento de texto y ábralo con un editor de texto, como el Bloc de notas.
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. Haga lo siguiente para reiniciar el agente:
   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
```

Para limitar el número total de equipos virtuales que un agente para VMware (dispositivo virtual) o un agente para VMware (Linux) puede incluir en la copia de seguridad:

1. En el equipo que ejecuta el agente, inicie el shell de comandos:
   - **Agente para VMware (dispositivo virtual):** presione Ctrl+Máyus+F2 en la interfaz de usuario del dispositivo virtual.
   - **Agente para VMware (Linux):** inicie sesión como usuario raíz en el equipo que ejecuta el dispositivo Acronis Backup. La contraseña es la misma que la de la consola de copia de seguridad.
2. Abra el archivo **/etc/Acronis/MMS.config** en un editor de texto, como **vi**.
3. Busque la siguiente sección:

```
<key name="SimultaneousBackupsLimits">
    <value name="MaxNumberOfSimultaneousBackups" type="Tdword">"10"</value>
</key>
```

4. Reemplace `10` por el valor decimal del límite que desee establecer.
5. Guarde el archivo.
6. Reinicie el agente:
   - **Agente para VMware (dispositivo virtual):** ejecute el comando **`reboot`**.
   - **Agente para VMware (Linux):** ejecute el comando siguiente:

```
sudo service acronis_mms restart
```

18 Supervisión e informes

Importante *Esta función se introdujo en la versión 12.5, que afecta solo a las implementaciones en una instalación. Esta función todavía no está disponible en las implementaciones en la nube. Para obtener más información, consulte "Novedades en Acronis Backup" (pág. 8).*

La sección del **Panel de control** le permite supervisar el estado actual de su infraestructura de copia de seguridad. La sección de **Informes** le permite generar informes a demanda y planificados sobre la infraestructura de la copia de seguridad. La sección **Informes** está disponible solo con una licencia Avanzada.

Las secciones **Panel de control** y **Informes** aparecen bajo la pestaña **Resumen** solo si el componente **Servicio de monitorización** ha sido instalado con el servidor de gestión (se instala de manera predeterminada).

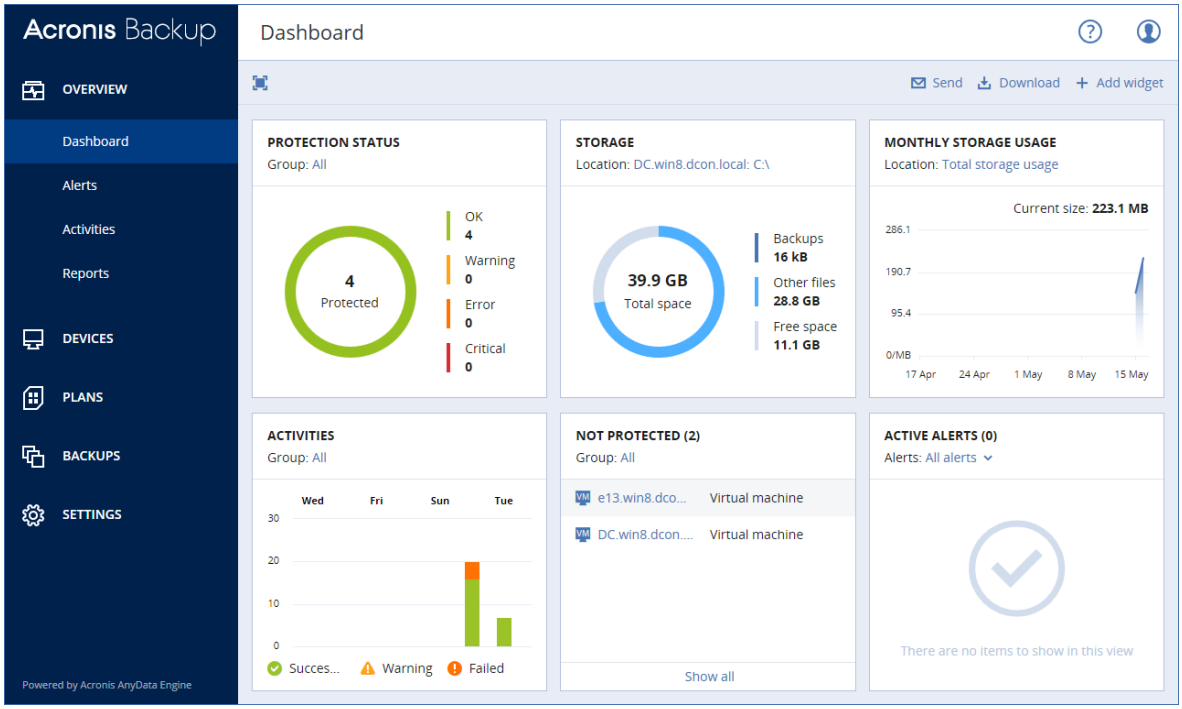
18.1 Tablero

El **Panel de control** proporciona una serie de widgets personalizables que dan una imagen general de su infraestructura de copia de seguridad. Los widgets se actualizan en tiempo real. Puede elegir entre más de 20 widgets, presentados como gráficos circulares, tablas, gráficos, diagramas de barras y listas.

De forma predeterminada aparecen los widgets siguientes:

- **Estado de la protección**. Muestra los estados de protección del grupo de dispositivos seleccionado.
- **Almacenamiento**. Muestra el espacio total, libre y ocupado de la ubicación de copia de seguridad seleccionada.
- **Uso mensual del almacenamiento**. Muestra la tendencia de uso mensual del espacio de la ubicación de copia de seguridad seleccionada.
- **Actividades**. Muestra los resultados de actividades de los últimos siete días.
- **Sin protección**. Muestra los dispositivos sin planes de copias de seguridad.

- **Alertas activas**. Muestra las cinco alertas activas más recientes.



Los widgets tienen elementos interactivos que le permiten investigar y solucionar problemas.

Puede descargar el estado actual del panel de control en formato .pdf o .xlsx, o bien enviarlo por correo electrónico. Para enviar el panel de control por correo electrónico, asegúrese de haber configurado el **Servidor de correo electrónico** (pág. 330).

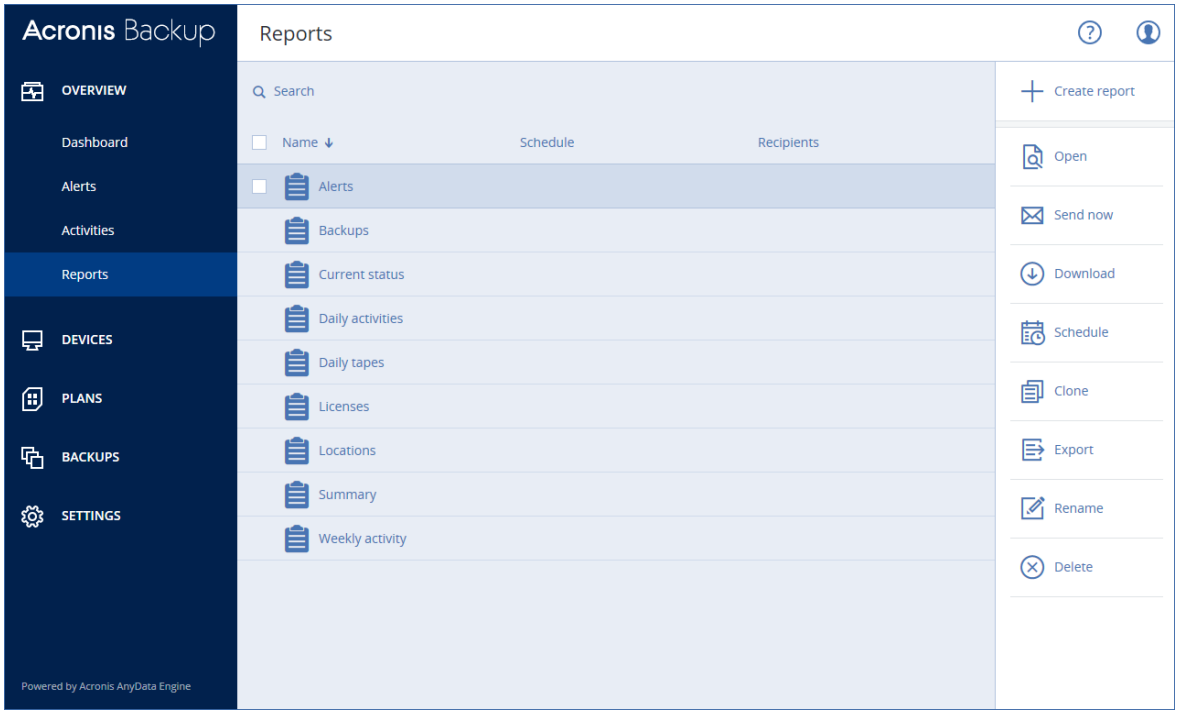
18.2 Informes

Nota *Esta funcionalidad solo está disponible con la licencia de Acronis Backup Advanced.*

Un informe puede incluir cualquier conjunto de los widgets del panel de control. Puede utilizar informes predefinidos o crear un informe personalizado.

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** (pág. 330).

Si desea procesar un informe con un software de terceros, programe guardar el informe en el formato .xlsx en una carpeta específica.



Operaciones básicas con informes

Haga clic en **Generalidades** > **Informes**, seleccione un informe y, a continuación, realice uno de los siguientes procedimientos:

- Para ver un informe, haga clic en **Abrir**.
- Para enviar el informe a través de correo electrónico, haga clic en **Enviar ahora**, especifique las direcciones de correo electrónico, seleccione el formato del informe y, a continuación, haga clic en **Enviar**.
- Para descargar el informe, haga clic en **Descargar**.

Programación de 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 elipsis vertical en 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**.

18.3 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 (pág. 329), 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: `<ruta_de_instalación>`**\AlertManager\alert_manager.yaml**

  En este caso, `<installation_path>` es la ruta de instalación del servidor de gestión. De forma 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 se ha habilitado 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
```

19 Grupos de los dispositivos

Importante *Algunas de las funciones descritas en esta sección se introdujeron en la versión 12.5, que afecta solo a las implementaciones en una instalación. Estas funciones todavía no están disponibles en las implementaciones en la nube. Para obtener más información, consulte "Novedades en Acronis Backup" (pág. 8).*

Los grupos de dispositivos se han diseñado para gestionar cómodamente un gran número de dispositivos registrados.

Puede aplicar un plan de copias de seguridad 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 equipos**.

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 copias de seguridad 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 copias de seguridad 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 copias de seguridad 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 copias de seguridad 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 copias de seguridad 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.

19.1 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.

19.2 Incorporación de dispositivos en grupos estáticos

1. Haga clic en **Dispositivos** y, a continuación, seleccione un dispositivo 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**.

19.3 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 criterios de búsqueda y los operadores descritos a continuación.
3. Haga clic en **Guardar como** junto al campo de búsqueda.
4. Escriba el nombre del grupo y, a continuación, haga clic en **Aceptar**.

Criterios de búsqueda

La tabla siguiente incluye los criterios de búsqueda disponibles.

Criterio	Significado	Ejemplos de consultas de búsqueda
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 = 'ru-00'**
comment	Comentario dirigido a un dispositivo. Valor predeterminado: ▪ Descripción del equipo tomada de las propiedades del ordenador en Windows para equipos físicos que ejecutan Windows. ▪ Vacío para otros dispositivos. Para ver el comentario, en **Dispositivos**, seleccione el dispositivo, haga clic en **Detalles** y busque la sección **Comentario**. Para añadir un comentario o modificarlo, haga clic en **Agregar** o **Editar**.	**comment = 'important machine'** **comment = ''** (todos los equipos sin ningún comentario)
ip	Dirección IP (solo para equipos físicos)	**ip RANGE ('10.250.176.1','10.250.176.50')**
memorySize	Tamaño de la RAM en megabytes (MiB)	**memorySize < 1024**
insideVm	Equipo virtual con un agente dentro. Valores posibles: ▪ **true** ▪ **false**	**insideVm = true**
osName	Nombre del sistema operativo.	**osName LIKE '%Windows XP%'**
osType	Tipo de sistema operativo. Valores posibles: ▪ **'windows'** ▪ **'linux'** ▪ **'macosx'**	**osType IN ('linux', 'macosx')**
osProductType	Tipo de producto de sistema operativo. Valores posibles: ▪ **'dc'** Significa controlador de dominio. ▪ **'server'** ▪ **'workstation'**	**osProductType = 'server'**

Criterio	Significado	Ejemplos de consultas de búsqueda
isOnline	Disponibilidad del equipo. Valores posibles: ▪ **true** ▪ **false**	**isOnline = true**
tenant	El nombre de la unidad a la que pertenece el dispositivo.	**tenant = 'Unit 1'**
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'**
state	Estado del dispositivo. Valores posibles: ▪ **'idle'** ▪ **'interactionRequired'** ▪ **'canceling'** ▪ **'backup'** ▪ **'recover'** ▪ **'install'** ▪ **'reboot'** ▪ **'failback'** ▪ **'testReplica'** ▪ **'run_from_image'** ▪ **'finalize'** ▪ **'failover'** ▪ **'replication'** ▪ **'createAsz'** ▪ **'deleteAsz'** ▪ **'resizeAsz'**	**state = 'backup'**
status	Estado de dispositivo. Valores posibles: ▪ **'notProtected'** ▪ **'ok'** ▪ **'warning'** ▪ **'error'** ▪ **'critical'**	**status = 'ok'**

Criterio	Significado	Ejemplos de consultas de búsqueda
protectedByPlan	Dispositivos que están protegidos por un plan de copias de seguridad 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'**
okByPlan	Dispositivos que están protegidos por un plan de copias de seguridad con un ID determinado y tienen el estado **Bueno**.	**okByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'**
errorByPlan	Dispositivos que están protegidos por un plan de copias de seguridad con un ID determinado y tienen el estado **Error**.	**errorByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'**
warningByPlan	Dispositivos que están protegidos por un plan de copias de seguridad con un ID determinado y tienen el estado **Advertencia**.	**warningByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'**
runningByPlan	Dispositivos que están protegidos por un plan de copias de seguridad con un ID determinado y tienen el estado **Ejecutando**.	**runningByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'**
interactionByPlan	Dispositivos que están protegidos por un plan de copias de seguridad con un ID determinado y tienen el estado **Interacción necesaria**.	**interactionByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'**
ou	Equipos que pertenecen a la unidad organizativa de Active Directory.	**ou IN ('RnD', 'Computers')**
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'**
lastBackupTime	La fecha y la hora de la última copia de seguridad realizada correctamente. El formato es `'AAAA-MM-DD HH:MM'`.	**lastBackupTime > '2016-03-11'** **lastBackupTime <= '2016-03-11 00:15'** **lastBackupTime is null**
lastBackupTryTime	La hora del último intento de realización de la copia de seguridad. El formato es `'AAAA-MM-DD HH:MM'`.	**lastBackupTryTime >= '2016-03-11'**
nextBackupTime	La hora de la siguiente copia de seguridad. El formato es `'AAAA-MM-DD HH:MM'`.	**nextBackupTime >= '2016-03-11'**
agentVersion	Versión del agente de copia de seguridad instalado.	**agentVersion LIKE '12.0.*'**

Criterio	Significado	Ejemplos de consultas de búsqueda
hostId	ID interno del agente de copia de seguridad. Para obtener el ID del agente de copia de seguridad, debajo de **Dispositivos**, seleccione el equipo, haga clic en **Detalles** > **Todas las propiedades**. El ID aparece en el campo **hostId**.	**hostId = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'**

Operadores

La tabla siguiente resume los operadores disponibles.

Operador	Significado	Ejemplos
AND	Operador de conjunción lógica.	**name like 'ru-00' AND status = ok**
OR	Operador de disyunción lógica.	**state=backup OR status = ok**
NOT	Operador de negación lógica.	**NOT(osProductType = 'workstation')**
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 uno o a varios ▪ _ El guion bajo representa un solo carácter	**name LIKE 'ru-00'** **name LIKE '*ru-00'** **name LIKE '*ru-00*'** **name LIKE 'ru-00_'**
ILIKE 'modelo de comodines'	Igual que el operador LIKE, pero distingue mayúsculas y minúsculas.	**name ILIKE 'Ru-00'**
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')**
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')**

19.4 Aplicación de una copia de seguridad a un grupo

1. Haga clic en **Dispositivos** y, a continuación, seleccione el grupo integrado que contiene a su vez el grupo al que desea aplicar un plan de copias de seguridad.

   El software muestra la lista de grupos secundarios.
2. Seleccione el grupo al que desea aplicar un plan de copias de seguridad.
3. Haga clic en **Copia de seguridad**.
4. Continúe con la creación del plan de copias de seguridad como se indica en "Copia de seguridad" (pág. 86).

20 Opciones de almacenamiento avanzadas

Nota *Esta funcionalidad solo está disponible con la licencia de Acronis Backup Advanced.*

20.1 Dispositivos de cintas

Las siguientes secciones describen en detalle cómo utilizar dispositivos de cintas para almacenar copias de seguridad.

20.1.1 ¿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 caso especial 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.

20.1.2 Información general sobre la compatibilidad de cintas

Los agentes de copia de seguridad 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.

20.1.2.1 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 copia de seguridad y los nodos de almacenamiento no utilizan RSM. Al detectar el dispositivo de cintas (pág. 313), 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.

20.1.2.2 Hardware compatible

Acronis Backup 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 Backup es compatible con dispositivos de cintas conectados por USB.

En Windows, Acronis Backup 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 comprobar si su dispositivo específico es compatible, utilice la Herramienta de compatibilidad del hardware como se describe en el siguiente artículo de Acronis Knowledge Base: https://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-backup-advanced-tape-hcl.

20.1.2.3 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 Vista 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. Busque la línea `<value name="ArsmDmlDbProtocol" type="TString">`.
5. Cambie la ruta en esta línea.
6. Guarde el archivo.

7. Inicie el servicio **acronis_rsm**.

20.1.2.4 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">
        "valor"
    </value>
    <value name=DefaultBlockSize" type="Dword">
        "valor"
    </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

Line in /etc/Acronis/BackupAndRecovery.config (en un equipo que ejecuta Linux):

```
    <value name=DefaultBlockSize" type="Dword">
        "valor"
    </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

Line in /etc/Acronis/BackupAndRecovery.config (en un equipo que ejecuta Linux):

```
    <value name="WriteCacheSize" type="Dword">
        "valor"
    </value>
```

Si especifica un valor distinto de cero no admitido por el sistema operativo, la copia de seguridad fallará.

20.1.2.5 Opciones de copia de seguridad relacionadas con la cinta

Puede configurar las opciones de copia de seguridad de **Gestión de cintas** (pág. 150) 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 copias de seguridad.
- 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).

20.1.2.6 Operaciones paralelas

Acronis Backup 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 (pág. 317) o borrado (pág. 319)), puede iniciar la operación que utiliza un intercambiador (mover (pág. 315) una cinta a otra ranura o expulsar (pág. 319) 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 (pág. 313) puede realizarse simultáneamente con cualquier otra operación. Durante el inventario (pág. 316), 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.

20.1.2.7 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 Office 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 cintas no es posible.
7. El software no puede sobrescribir automáticamente una cinta que contenga al menos una copia de seguridad no eliminada o si hay copias de seguridad dependientes en otras cintas.
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 (pág. 207) 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).

20.1.2.8 Legibilidad de cintas escritas por productos de Acronis anteriores

La siguiente tabla resume la legibilidad de cintas escritas por Acronis True Image Echo, True Image Acronis 9.1 y las familias de productos Acronis Backup & Recovery 10 y Acronis Backup & Recovery 11 en Acronis Backup. La tabla también ilustra la compatibilidad de las cintas escritas de varios componentes de Backup Acronis.

Pueden añadirse copias de seguridad incrementales y diferenciales a copias de seguridad examinadas de nuevo y creadas por Acronis Backup 11.5 y Acronis Backup 11.7.

			...es legible en un dispositivo de cinta conectado en un equipo con...			
			Dispositivo de arranque Backup de Acronis	Agente para Windows Backup de Acronis	Agente para Linux Backup de Acronis	Nodo de almacenamiento Backup de Acronis
Cinta escrita en un dispositivo de cinta	Dispositivo de arranque	9.1	+	+	+	+
		Echo	+	+	+	+
		ABR10	+	+	+	+

conectado a nivel local (unidad de cinta o biblioteca de cintas) por...		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	+	+	+	+

20.1.3 Comenzar con el uso del dispositivo de cintas

20.1.3.1 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 copias de seguridad se ha 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 de copia de seguridad.
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" (pág. 316).

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 (pág. 315) dichas cintas al grupo **Cintas libres** manualmente.

*Las cintas enviadas al pool **Cintas importadas** contienen copias de seguridad escritas por el software 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 copias de seguridad como se indica en la sección "Copia de seguridad" (pág. 86). 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 **Copias de seguridad** > **Grupos de cintas 'Acronis'**.
- Las cintas con copias de seguridad se trasladarán al grupo **Acronis**.

20.1.3.2 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 de copia de seguridad.
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" (pág. 316).

      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 (pág. 315) dichas cintas al grupo **Cintas libres** manualmente.

      *Las cintas enviadas al pool **Cintas importadas** contienen copias de seguridad escritas por el software 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 (pág. 314).

   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 copias de seguridad 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 copias de seguridad como se indica en la sección "Copia de seguridad" (pág. 86). 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" (pág. 316) 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.

20.1.3.3 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 de copia de seguridad.
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 (pág. 157) 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 (pág. 316) 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 (pág. 316) rápido.

   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 (pág. 317) 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.

20.1.3.4 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" (pág. 229).
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 (pág. 316) 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.

20.1.3.5 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>**//**, donde <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 (pág. 316) 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.

20.1.4 Gestión de cintas

20.1.4.1 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.

20.1.4.2 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 (pág. 315) 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 pool contiene cintas escritas por Acronis Backup 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 disponibles

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.

20.1.4.3 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" (pág. 314).
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 pool, no se olvide de modificar los planes de copias de seguridad que tengan al pool como ubicación de la copia de seguridad. De lo contrario, estos planes de copias de seguridad 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.

20.1.4.4 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.

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 libres**, 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.

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" (pág. 314).
6. Seleccione el grupo al que desea mover las cintas.
7. Haga clic en **Mover** para guardar los cambios.

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 (pág. 315) 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 (pág. 317). 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 o el nodo de almacenamiento al que se conectará el dispositivo de cintas. Después, seleccione el dispositivo de cintas del que quiera realizar el inventario.
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.

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 (pág. 320) 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 (pág. 319), retire (pág. 320) la información sobre la misma de la base de datos y después inserte la cinta nuevamente en el dispositivo de cintas.

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 (pág. 316) 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.

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.

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.

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 (pág. 150), 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 (pág. 319)).

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 (pág. 319), 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 (pág. 316) 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 (pág. 317) 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 (pág. 150), 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 la Cinta 1, **Tuesday** para la 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.

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.

20.2 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 almacenamientos dedicados de las copias de seguridad de la empresa (ubicaciones gestionadas).

20.2.1 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 (pág. 35).

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" (pág. 328).

Para instalar un nodo de almacenamiento o un servicio de catalogación

1. Inicie sesión como administrador e inicie el programa de instalación de Acronis Backup.
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 seleccione si el equipo participará en el Programa de experiencia del cliente (PEC) de Acronis.
4. Haga clic en **Instalar un agente de copias de seguridad**.
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 Backup 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. Puede usar las credenciales de sesión de Windows actuales o especificar explícitamente el nombre de usuario y la contraseña.

      Aunque no sea administrador del servidor de gestión, puede registrar el equipo si selecciona la opción **Conectar sin autenticación**. Esto funciona siempre que el servidor de gestión admita registrarse de forma anónima, opción que puede estar deshabilitada (pág. 332).
   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" (pág. 333).
10. [Opcional] Cambie otros ajustes de la instalación según se describe en "Personalización de los ajustes de instalación" (pág. 42).
11. Haga clic en **Instalar** para proceder con la instalación.
12. Cuando haya terminado la instalación, haga clic en **Cerrar**.

20.2.2 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 (pág. 313). 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 **Copias de seguridad** > **Agregar ubicación** y haga clic en **Nodo de almacenamiento**.
- Cuando cree un plan de copias de seguridad, 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 **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" (pág. 324).
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" (pág. 324).
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" (pág. 326).
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" (pág. 329).
11. Haga clic en **Realizado** para crear la ubicación.

Para crear una ubicación gestionada en un dispositivo de cintas:

1. Haga clic en **Copias de seguridad** > **Agregar ubicación** o, al crear un plan de copias de seguridad, 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" (pág. 314), 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* ***Copias de seguridad*** *> la ubicación >* ***Editar*** *y cambie el valor del campo* ***Dirección****.*

20.2.3 Deduplicación

20.2.3.1 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.

Consejo*: 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 de 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.

20.2.3.2 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:

  $$S = 5000 * 90 / 65536 + 10 = 17 \text{ GB}$$

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, puesto que 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.

40-160 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 esto, cree varios planes de copias de seguridad con varias programaciones.

20.2.4 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 copias de seguridad 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 AES 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.

20.2.5 Catalogación

20.2.5.1 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 **Copias 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" (pág. 321).

La sección **Catálogo** aparece solo para los administradores de la organización (pág. 333).

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 Backup 12.5

Selección de los datos incluidos en la copia de seguridad para su recuperación

1. Haga clic en **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.

***Consejo** Para ver qué servicio cataloga una ubicación, seleccione la ubicación en **Copias de seguridad** > **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'' (pág. 156).
   - [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**.

20.2.5.2 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

20.2.5.3 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 **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**.

21 Configuración del sistema

Esta configuración solo está disponible para implementaciones en una instalación.

Para acceder a esta configuración, haga clic en **Configuración** > **Configuración del sistema**.

La sección **Configuración del sistema** aparece solo para administradores de la organización (pág. 333).

21.1 Notificaciones por correo electrónico

Puede ajustar la configuración general que sea habitual para las notificaciones por correo electrónico enviadas desde el servidor de gestión.

En las opciones de copia de seguridad predeterminadas (pág. 332), 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 copias de seguridad (pág. 134), 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 copias de seguridad que usan esta configuración.*

Antes de ajustar estas opciones de configuración, asegúrese de que se hayan configurado las opciones del **servidor de correo electrónico** (pág. 330).

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 la 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 a la 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**.

21.2 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**

Debe activar la opción de configuración **Aplicaciones menos seguras** en la cuenta de Gmail. Para obtener más información, consulte https://support.google.com/accounts/answer/6010255.

- **Yahoo Mail**
- **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.

21.3 Seguridad

Utilice estas opciones para mejorar la seguridad de la implementación en la instalación de Acronis Backup.

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: **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: **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 Backup 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: **Deshabilitado**.

21.4 Actualizaciones

Esta opción define si Acronis Backup busca una nueva versión cada vez que un administrador de la organización inicie sesión en la consola de copias de seguridad.

El valor predeterminado es: **Habilitado**.

Si esta opción está deshabilitada, el administrador puede buscar actualizaciones manualmente, como se describe en "Buscar actualizaciones de software" (pág. 63).

21.5 Opciones de copia de seguridad predeterminadas

Los valores predeterminados de opciones de copia de seguridad (pág. 123) son los mismos para todos los planes de copia de seguridad del servidor de gestión. Al crear un plan de copias de seguridad, puede anular un valor predeterminado con un valor personalizado que será específico del plan en cuestión únicamente.

Para algunas de las opciones de copia de seguridad, puede cambiar el valor de una opción predeterminada contra el predefinido. El nuevo valor se utilizará de forma predeterminada en todos los planes de copia de seguridad creados cuando se aplica el cambio.

Para cambiar el valor de la opción predeterminada

1. Haga clic en **Configuración** > **Configuración del sistema**.
2. Amplíe la sección **Opciones de copia de seguridad predeterminadas**.
3. Seleccione la opción y, a continuación, realice los cambios necesarios.
4. Haga clic en **Guardar**.

21.6 Configuración del registro anónimo

Al llevar a cabo la instalación local de un agente (pág. 51), el programa de instalación sugiere la opción de registrar el equipo en el servidor de gestión de forma anónima, es decir, conectarse sin autenticación. El registro anónimo también se emplea si se especifican las credenciales incorrectas del servidor de gestión en la interfaz gráfica de usuario de Agente parar VMware (dispositivo virtual). Gracias al registro anónimo, el administrador del servidor de gestión puede delegar la instalación del agente a los usuarios.

El registro anónimo en el servidor de gestión se puede deshabilitar para que haya que introducir siempre el nombre de usuario y la contraseña correctas del administrador del servidor de gestión al registrar un dispositivo. Si el usuario decide registrarse de forma anónima, se producirá un error en el registro. También se rechazará el registro del dispositivo de arranque configurado previamente en la opción **No solicitar nombre de usuario y contraseña**. Durante la realización de una instalación sin supervisión, tendrá que proporcionar un token de registro en el archivo de transformación (.mst) o como parámetro de comando `msiexec`.

Pasos para deshabilitar la opción de registro anónimo en el servidor de gestión

1. Inicie sesión en el equipo donde está instalado el servidor de gestión.
2. Abra el siguiente archivo de configuración en un editor de texto:
   - En Windows: **%ProgramData%\Acronis\ApiGateway\api_gateway.json**
   - En Linux: **/var/lib/Acronis/ApiGateway/api_gateway.json**
3. Busque la siguiente sección:

```
"auth" : {
     "anonymous_role" : {
        "enabled" : true,
        // ...
  },
```

4. Cambie **`true`** por **`false`**.
5. Guarde el archivo **api_gateway.json**.

   Importante *Tenga cuidado de no eliminar accidentalmente comas, paréntesis o comillas en el archivo de configuración.*

6. Reinicie Acronis Service Manager Service como se describe en "Cambio de la configuración del certificado SSL" (pág. 84).

22 Administración de cuentas de usuario y unidades de organización

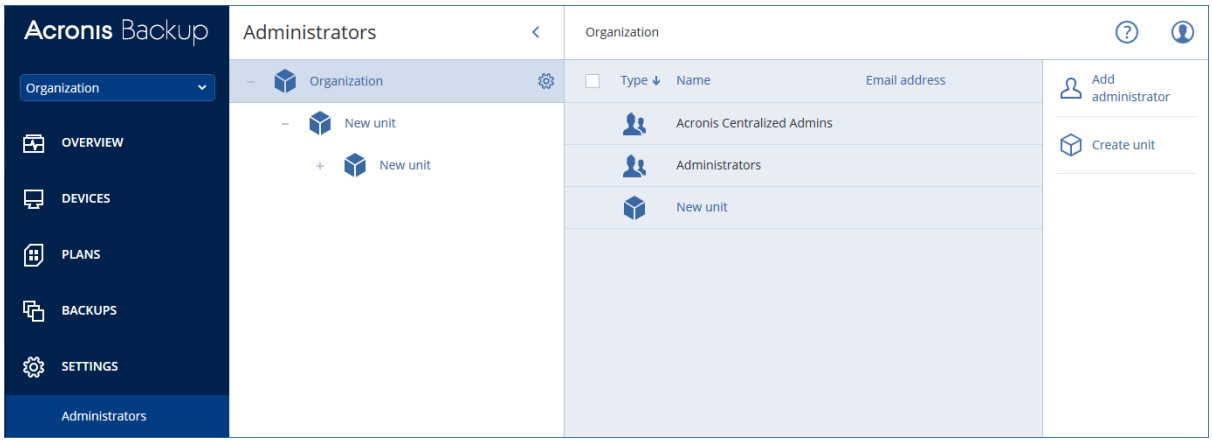
22.1 Implementación en una instalación

La funcionalidad descrita en esta sección solo está disponible para administradores de la organización (pág. 333).

Para acceder a esta configuración, haga clic en **Configuración** > **Administradores**.

22.1.1 Administradores y unidades

El panel **Administradores** muestra el grupo **Organización** con las unidades del árbol (si las hubiera) y la lista de administradores de la unidad que está seleccionada en el árbol.



¿Quiénes son los administradores del servidor de gestión?

Cualquier cuenta con la que se pueda iniciar sesión en la consola de copia de seguridad es un administrador del servidor de gestión.

Los administradores de la organización son los administradores de más alto nivel. *Los administradores de la unidad* son los administradores de los grupos secundarios (unidades).

En la consola de copia de seguridad, cada administrador tiene una vista centrada en su área de control. Un administrador puede ver y gestionar cualquier elemento que esté en su nivel o en cualquier nivel inferior.

¿Quiénes son los 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 de copia de seguridad 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.

¿Quién puede ser administrador?

Si el servidor de gestión está instalado en un equipo de Windows incluido en un dominio de Active Directory, cualquier usuario o grupo de usuarios locales o del dominio puede añadirse a los administradores del servidor de gestión. De lo contrario, solo pueden añadirse usuarios y grupos locales.

Para obtener información sobre cómo añadir un administrador al servidor de gestión, consulte la sección "Incorporación de administradores" (pág. 335).

Unidades y administradores de unidades

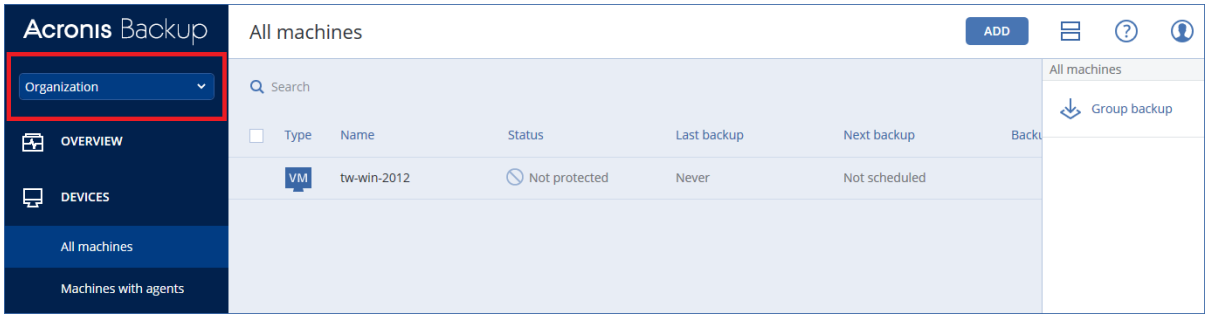
El grupo **Organización** se crea automáticamente al instalar el servidor de gestión. Con la licencia Acronis Backup Advanced puede crear grupos secundarios llamados unidades, que normalmente corresponden a unidades o departamentos de la organización, y añadir administradores a estas unidades.

De esta forma, puede delegar la gestión de las copias de seguridad a otras personas cuyos permisos de acceso estarán estrictamente limitados a las unidades correspondientes.

Para obtener información sobre cómo crear una unidad, consulte la sección "Creación de dispositivos de arranque" (pág. 336).

¿Qué sucede si se añade una cuenta a varias unidades?

Se puede añadir una cuenta como **administrador de la unidad** a cualquier cantidad de unidades. En una cuenta de este tipo, así como para administradores de organización, el selector de unidades se muestra en la consola de copias de seguridad. Mediante este selector, el administrador puede ver y gestionar cada unidad por separado.



Aunque una cuenta que tenga permiso para todas las unidades, no tiene permiso para la organización. Los administradores 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 (pág. 45), 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 (pág. 51), 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.

22.1.2 Incorporación de administradores

Para añadir administradores

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

   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 **Añadir administrador**.
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. Repita los pasos del 4 al 6 para todos los usuarios o grupos que desee añadir.
8. Al finalizar, haga clic en **Listo**.
9. [Solo en Linux] Añada los nombres de usuario al módulo de autenticación conectable Acronis Linux PAM, como se describe más adelante.

Para añadir usuarios a Acronis Linux PAM

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.

22.1.3 Creación de unidades

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

22.2 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 gestión** cuando inicie sesión en el servicio de copia de seguridad, o bien haga clic  en el icono de puntos suspensivos vertical de la esquina superior derecha y, a continuación, en **Portal de gestión**. 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 copia de seguridad.

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 copia de seguridad.

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 copia de seguridad.

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 Office 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 copias de seguridad. 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 uso por encima del límite en varios dispositivos, el usuario no puede aplicar un plan de copias de seguridad 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 cloud** desaparece de la consola de copia de seguridad.
- **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 de copia de seguridad, 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 copia de seguridad 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 copia de seguridad incluye los datos siguientes sobre la organización o la 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.

23 Referencia de la línea de comandos

La referencia de la línea de comandos es un documento independiente disponible en Argentina/support/documentation/AcronisBackup_12.5_Command_Line_Reference

24 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.

Declaración de copyright

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.

25 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 cualquier copia de seguridad completa.

Copia de seguridad diferencial

La copia de seguridad diferencial almacena los cambios de los datos a partir de la última copia de seguridad completa (pág. 341). Necesita 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.

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 copias de seguridad) 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).