Servicio de copias de seguridad

Version 7.7

GUÍA DEL USUARIO

Revisión: 02/07/2018

Contenido

1 Acerca del servicio de copias de seguridad

El servicio permite realizar copias de seguridad y recuperar equipos físicos y virtuales, archivos y bases de datos en un almacenamiento local o en la nube.

Este servicio está disponible mediante una interfaz web denominada consola de copia de seguridad.

2 Requerimientos de software

2.1 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
- Microsoft Edge 25 o posterior
- Safari 8 o una versión posterior que se ejecute en los sistemas operativos OS X y iOS

En otros navegadores web (incluido Safari para otros sistemas operativos), la interfaz de usuario podría no mostrarse correctamente o algunas funciones podrían no estar disponibles.

2.2 Sistemas operativos y entornos compatibles

Agente para Windows

Windows XP Professional SP3 (x86, x64)

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

Agente para SQL, Agent for Exchange 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.

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

Agente para Linux

Linux con la versión de kernel 2.6.9 a 4.15 y glibc 2.3.4 o versiones posteriores

Varias distribuciones 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

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

Fedora 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23 y 24

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, 9.0, 9.1, 9.2

CentOS 5.x, 6.x, 7, 7.1, 7.2, 7.3, 7.4

Oracle Linux 5.x, 6.x, 7.0, 7.1, 7.2, 7.3, 7.4, 7.5: 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

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

Agente para VMware

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.

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

Agente para 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

Agente para Virtuozzo

Virtuozzo 6.0.10

2.3 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

2.4 Versiones compatibles de Microsoft Exchange Server

- **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 recuperación de buzones de correo y sus elementos desde la introducción del Service Pack 1 (SP1).
- **Microsoft Exchange Server 2007**: todas las ediciones, todos los Service Pack. No se admite la recuperación de buzones de correo ni de elementos de buzón de correo.

2.5 Versiones de Microsoft SharePoint compatibles

Backup Service 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.

2.6 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		
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		
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	+	+
Microsoft Virtual PC 2004 y 2007 Windows Virtual PC		+
Microsoft Virtual Server 2005		+

Plataforma	Copia de seguridad a nivel de hipervisor (sin agente)	Copia de seguridad desde dentro de un SO huésped
Citrix		
Citrix XenServer 4.1.5, 5.5, 5.6, 6.0, 6.1, 6.2, 6.5, 7.0, 7.1 y 7.2		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		
Parallels Workstation		+
Parallels Server 4 Bare Metal		+
Oracle		
Oracle VM Server 3.0 y 3.3		+
Oracle VM VirtualBox 4.x		+
Virtuozzo		
Virtuozzo 6.0.10 y 6.0.11	+	(Solo Equipos virtuales. No se pueden usar contenedores.)
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.

- **Equipos virtuales cifrados** (presentados en VMware vSphere 6.5)
  - Los equipos virtuales cifrados se incluyen en la copia de seguridad en un estado cifrado. Si el cifrado es crucial en su caso, habilite las copias de seguridad al crear un plan de copias de seguridad (pág. 40).
  - 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.

2.7 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.

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

3 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 (los dispositivos de arranque solo son compatibles con la recuperación). Las limitaciones se aplican tanto a los agentes como a los dispositivos de arranque.

<table>
<tr><th rowspan="2">Sistema de archivos</th><th colspan="3">Compatibilidad con</th><th rowspan="2">Limitaciones</th></tr>
<tr><th>Agentes</th><th>Dispositivos de arranque para Windows y Linux</th><th>Dispositivos de arranque para Mac</th></tr>
<tr><td>FAT16/32</td><td rowspan="3">Todos los agentes</td><td>+</td><td>+</td><td rowspan="4">Sin limitaciones</td></tr>
<tr><td>NTFS</td><td>+</td><td>+</td></tr>
<tr><td>ext2/ext3/ext4</td><td>+</td><td>-</td></tr>
<tr><td>HFS+</td><td rowspan="2">Agente para Mac</td><td>-</td><td>+</td></tr>
<tr><td>APFS</td><td>-</td><td>+</td><td>▪ 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.</td></tr>
<tr><td>JFS</td><td rowspan="3">Agente para Linux</td><td>+</td><td>-</td><td rowspan="2">Los archivos no se pueden excluir de la copia de seguridad del disco.</td></tr>
<tr><td>ReiserFS3</td><td>+</td><td>-</td></tr>
<tr><td>ReiserFS4</td><td>+</td><td>-</td><td rowspan="3">▪ 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</td></tr>
<tr><td>ReFS</td><td rowspan="2">Todos los agentes</td><td>+</td><td>+</td></tr>
<tr><td>XFS</td><td>+</td><td>+</td></tr>
<tr><td>Linux swap</td><td>Agente para Linux</td><td>+</td><td>-</td><td>Sin limitaciones</td></tr>
</table>

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.

4 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.

5 Acceder al servicio de copias de seguridad

Puede iniciar sesión en el servicio de copias de seguridad si activó su cuenta.

Para iniciar sesión en el servicio de copias de seguridad

1. Vaya a la página de inicio del servicio de copias de seguridad. La dirección de la página de inicio de sesión se incluye en el correo electrónico de activación.
2. Escriba el usuario y luego haga clic en **Continuar**.
3. Escriba la contraseña y luego haga clic en **Iniciar sesión**.
4. Si tiene asignada la función de administrador en el servicio de copia de seguridad, haga clic en **Copia de seguridad y recuperación ante desastres**.

   Los usuarios que no tienen asignada la función de administrador inician sesión en la consola de copias de seguridad directamente.

Para cambiar el idioma de la interfaz web, haga clic en el icono de la figura humana que hay en la esquina superior derecha.

El administrador puede cambiar entre la consola de copia de seguridad y el portal de gestión. Para acceder a la consola de copia de seguridad desde el portal de gestión, en la pestaña **Generalidades**, vaya a la sección **Copia de seguridad y recuperación ante desastres** y luego haga clic en **Gestionar servicio**. Para acceder al portal de gestión desde la consola de copia de seguridad, haga clic en **Gestionar cuentas** en la esquina superior izquierda.

6 Instalar el software

6.1 Preparación

Paso 1

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.

Agente para Windows se instala junto con Agent for Exchange, Agente para SQL, Agente para VMware, Agente para Hyper-V y Agente para Active Directory. 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?
Equipos físicos		

¿Qué se va a incluir en las copias de seguridad?	¿Qué agente se debe instalar?	¿Dónde se debe realizar la instalación?
Equipos físicos que ejecutan Windows	Agente para Windows	En el equipo que se incluirá en las copias de seguridad.
Equipos físicos que ejecutan Linux	Agente para Linux	
Equipos físicos que ejecutan macOS	Agente para Mac	
Aplicaciones		
Bases de datos SQL	Agente para SQL	En el equipo que ejecuta Microsoft SQL Server.
Bases de datos de Exchange	Agent for Exchange	En el equipo que realiza el rol de buzón de correo de Microsoft Exchange Server.
Buzones de correo de Microsoft Office 365	Agente para Office 365	En un equipo que ejecute Windows y esté conectado a Internet. En función de la configuración elegida por el proveedor de servicios, es posible que necesite instalar Agente para Office 365. Para obtener más información, consulte "Proteger los buzones de correo de Office 365" (pág. 121).
Equipos que ejecutan Servicios de dominio de Active Directory	Agente para Active Directory	En el controlador de dominio.
Equipos virtuales		
Equipos virtuales VMware ESXi	Agente para VMware	En un equipo Windows con acceso de red a vCenter Server y al almacenamiento del equipo virtual.*
Equipos virtuales Hyper-V	Agente para Hyper-V	En el servidor Hyper-V.
Equipos virtuales y contenedores Virtuozzo	Agente para Virtuozzo	En el servidor Virtuozzo.
Equipos virtuales alojados en Amazon EC2	Los mismo ocurre con los equipos físicos**	En el equipo que se incluirá en las copias de seguridad.
Equipos virtuales alojados en Windows Azure.		
Equipos virtuales de Citrix XenServer		
Red Hat Virtualization (RHV/RHEV)		
Equipos virtuales basados en Kernel (KVM)		
Equipos virtuales de Oracle		
Dispositivos móviles		

¿Qué se va a incluir en las copias de seguridad?	¿Qué agente se debe instalar?	¿Dónde se debe realizar la instalación?
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 más información, consulte "Agente para VMware: copia de seguridad sin LAN" (pág. 138).

**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.

Paso 2

Compruebe los requisitos del sistema para los agentes.

Agente	Espacio de disco ocupado por el/los Agente(s).
Agente para Windows	550 MB
Agente para Linux	500 MB
Agente para Mac	450 MB
Agente para SQL	600 MB (50 MB + 550 MB Agente para Windows)
Agent for Exchange	750 MB (200 MB + 550 MB Agente para Windows)
Agente para Office 365	550 MB
Agente para Active Directory	600 MB (50 MB + 550 MB Agente para Windows)
Agente para VMware	700 MB (150 MB + 550 MB Agente para Windows)
Agente para Hyper-V	600 MB (50 MB + 550 MB Agente para Windows)
Agente para Virtuozzo	500 MB

El consumo de memoria medio es de 300 MB además del sistema operativo y las aplicaciones que se ejecutan. El consumo máximo puede alcanzar los 2 GB, dependiendo de la cantidad y del tipo de datos que procesen los agentes.

Paso 3

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

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

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

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 4

Antes de empezar la instalación, asegúrese de que los cortafuegos y otros componentes del sistema de seguridad de red (como, por ejemplo, un servidor proxy) permiten conexiones tanto de entrada como de salida mediante los siguientes puertos TCP:

- **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. 17) para saber si debe configurar estos valores en cada equipo que ejecute un agente de copia de seguridad.

6.2 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
```

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. Guarde el documento como **proxy.reg**.
5. Ejecute el archivo como administrador.
6. Confirme que desea editar el registro de Windows.

7. 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. 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">"DIRECCIÓN"</value>
    <value name="Port" type="Tdword">"PUERTO"</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. Guarde el archivo.
5. Reinicie el agente ejecutando el comando siguiente en cualquier directorio:

```
sudo service acronis_mms restart
```

En macOS

En macOS, debe especificar la configuración de proxy antes de la instalación tal como se describe a continuación. Para modificar la configuración del servidor proxy después de la instalación, edite el mismo archivo **Global.config** y reinicie el agente.

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>
    </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. Guarde el archivo.
5. 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
```

6.3 Paquetes de Linux

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

- El paquete con los encabezados u orígenes de kernel. La versión del paquete debe coincidir con la versión de kernel.
- El sistema compilador GNU Compiler Collection (GCC). La versión GCC debe ser la versión con la que se compiló el kernel.
- La herramienta Make.
- El interpretador Perl.

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

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

¿Los paquetes requeridos ya están instalados?

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

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

   ```
   cat /proc/version
   ```

   Este comando devuelve líneas similares a las siguientes: **`Linux version 2.6.35.6`** y **`gcc version 4.5.1`**
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 **make**, solo asegúrese de que se ejecute el comando.
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 verificar si el interpretador Perl está instalado:

```
perl --version
```

Si ve información sobre la versión Perl, el interpretador 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	**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`

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.

6.4 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 y el puerto 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. 140) 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 **Registrarse ahora**. 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 ahora**.*

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.
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 **Registrarse ahora**. 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 se le pide, proporcione las credenciales del administrador.
6. Haga clic en **Continuar**.
7. Espere a que se muestre la pantalla de registro.
8. Realice uno de los siguientes procedimientos:
   - Haga clic en **Registrarse ahora**. 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.

6.5 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.

   Puede hacer clic en **Administrar tokens activos** para ver y administrar los tokens ya generados.

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. Haga clic en **Especificar** junto a **Token de registro** y especifique el token generado.
6. Compruebe o modifique la configuración de instalación que se añadirá al archivo .mst y haga clic en **Continuar**.
7. En **Guardar los archivos en**, especifique la ruta para el archivo que haya creado.
8. Haga clic en **Generar**.

Como consecuencia, se generará la transformación .mst y los paquetes de instalación .msi y .cab se extraerán a la carpeta que creó.

Paso 3: Configuración de objetos de directiva de grupo

1. Conéctese al controlador de dominio como un administrador de dominio y, si el dominio tiene más de un controlador de dominio, conéctese a cualquiera de ellos como un administrador de dominio.
2. Si tiene pensado implementar un Agente en una unidad organizacional, asegúrese de que la unidad organizacional existe en el dominio. De lo contrario, omita este paso.
3. En el menú **Inicio**, seleccione **Herramientas administrativas** y haga clic en **Usuarios y equipos de Active Directory** (en Windows Server 2003) o **Administración de directivas de grupo** (en Windows Server 2008 y Windows Server 2012).
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 Windows Server 2012:
   - 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 en Windows Server 2012, en **Objetos de directiva de grupo**, haga clic con el botón derecho del ratón sobre el objeto de directiva de grupo y, a continuación, 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:
   - 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**.

6.6 Actualizar agentes

Gracias a la interfaz web, se pueden actualizar los agentes que se inicien con las siguientes versiones:

- Agente para Windows, agente para VMware, agente para Hyper-V: versiones 11.9.191 y posteriores
- Agente para Linux: versiones 11.9.179 y posteriores
- Otros agentes: se pueden actualizar todas las versiones

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

Para actualizar versiones anteriores del Agente, descargue e instale el Agente más actual manualmente. Para buscar los enlaces de descarga, haga clic en **Todos los dispositivos** > **Añadir**.

Para actualizar un Agente usando la interfaz web

1. 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.
2. Seleccione los equipos en los que desea actualizar los agentes. Los equipos deben estar conectados.
3. Haga clic en **Actualizar Agente**.

   El progreso de la actualización aparece en la pestaña **Actividades**.

6.7 Desinstalación de agentes

En Windows

Si desea quitar componentes de producto individuales (por ejemplo, uno de los agentes o la monitorización de copias de seguridad), ejecute el programa de instalación **Todos los agentes para instalación en Windows**, elija modificar el producto y desmarque la selección de los componentes que desea quitar. El enlace al programa de instalación está presente 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.

1. Inicie sesión como administrador.
2. Vaya a **Panel de control** y luego seleccione **Programas y características** (**Añadir o quitar programas** en Windows XP) > **Agente de copia de seguridad Acronis** > **Desinstalar**.
3. [Opcional] Seleccione la casilla de verificación **Eliminar los registros y las opciones de configuración**.

   Si tiene previsto volver a instalar el agente, deje esta casilla de verificación sin marcar. Si selecciona la casilla de verificación, 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)**.

   Si tiene previsto volver a instalar el agente, deje esta casilla de verificación sin marcar. 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**.

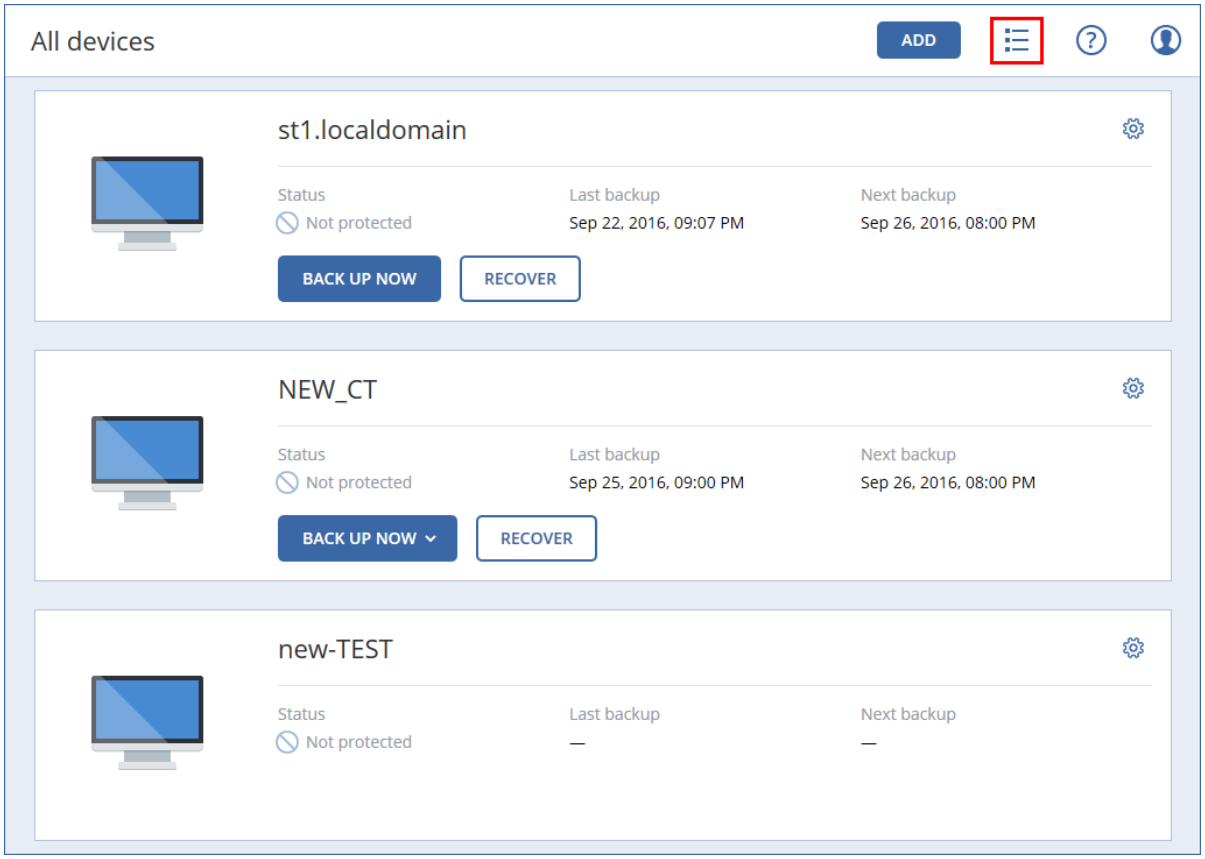
En OS X

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**.

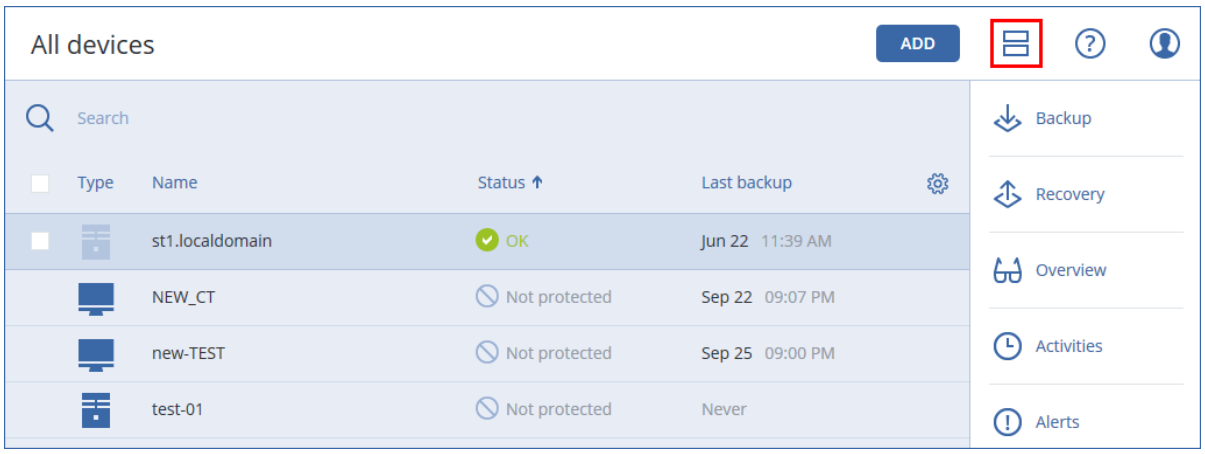
7 Vistas de la consola de copias de seguridad

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.

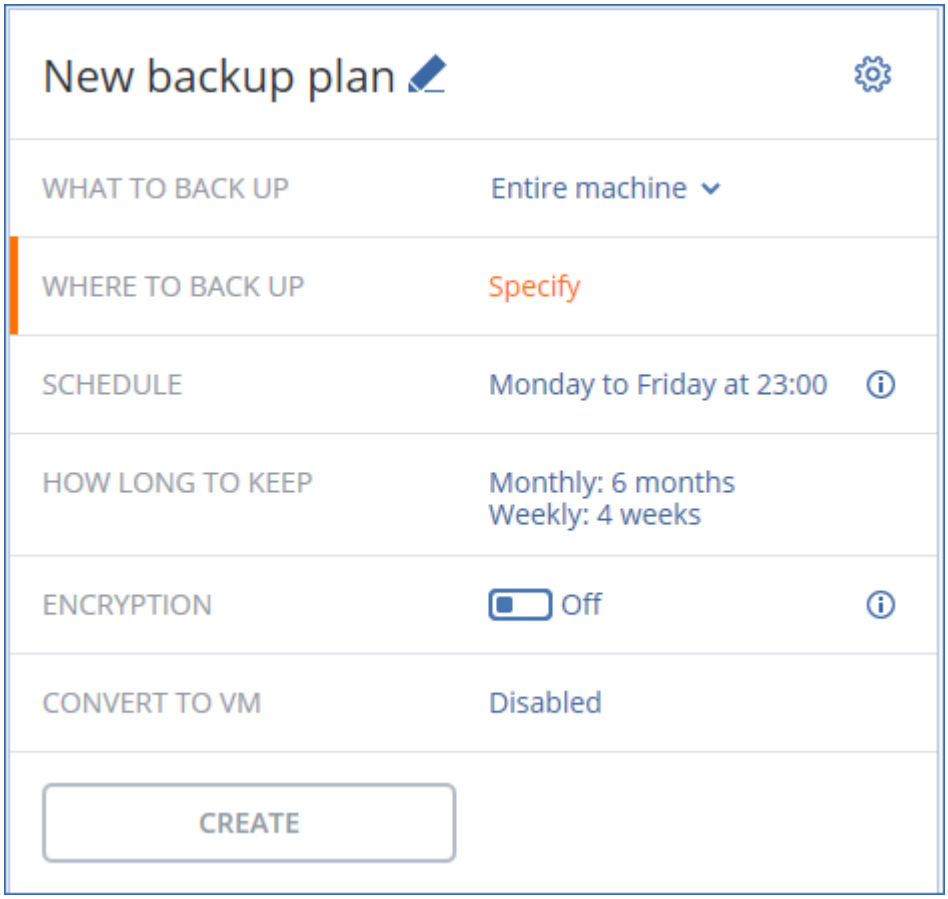
8 Crear copia de seguridad

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.

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.

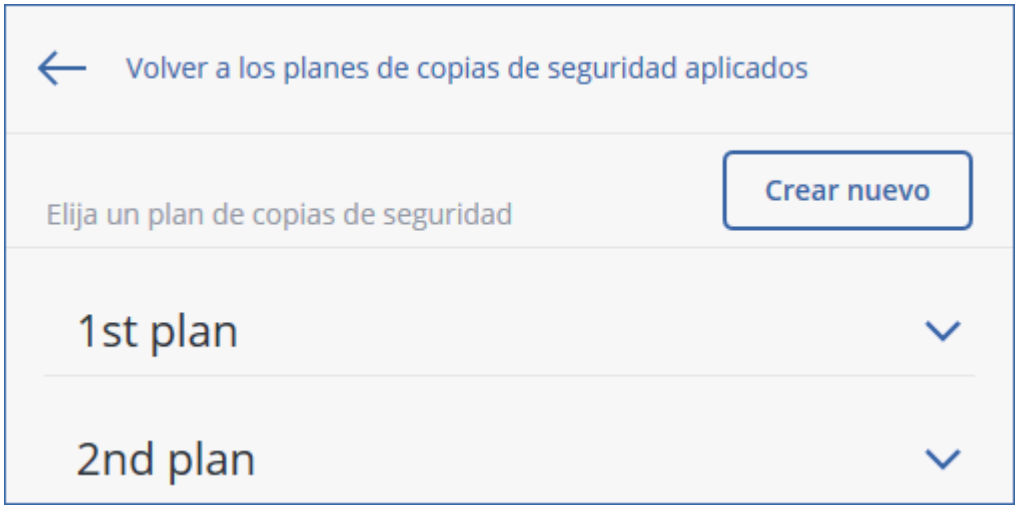


3. [Opcional] Para modificar el nombre del plan de copias de seguridad, haga clic en el nombre predeterminado.
4. [Opcional] Para modificar los parámetros del plan, haga clic en la sección correspondiente del panel del plan de copias de seguridad.
5. [Opcional] Para modificar las opciones de copia de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

8.1 Apuntes del plan de copias de seguridad

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. 30) Normas de directiva (pág. 30) Filtros de archivo (pág. 50)	Nube (pág. 35) Carpeta local (pág. 35) Carpeta de red (pág. 35) NFS (pág. 35)* Secure Zone (pág. 35)**	Siempre incremental (archivo único) (pág. 38) Siempre completas (pág. 38) Completas semanalmente, incrementales diariamente (pág. 38) Personalizadas (F-D-I) (pág. 38)	Por antigüedad de las copias de seguridad (norma única/por conjunto de copias de seguridad) (pág. 39) Por número de copias de seguridad (pág. 39) Guardar indefinidamente (pág. 39)
Discos/volúmenes (equipos virtuales)	Normas de directiva (pág. 30) Filtros de archivo (pág. 50)	Nube (pág. 35) Carpeta local (pág. 35) Carpeta de red (pág. 35) NFS (pág. 35)*		
Archivos (sólo equipos físicos)	Selección directa (pág. 33) Normas de directiva (pág. 33) Filtros de archivo (pág. 50)	Nube (pág. 35) Carpeta local (pág. 35) Carpeta de red (pág. 35) NFS (pág. 35)* Secure Zone (pág. 35)**	Siempre completas (pág. 38) Completas semanalmente, incrementales diariamente (pág. 38) Personalizadas (F-D-I) (pág. 38)	

Configuración de ESXi	Selección directa (pág. 35)	Carpeta local (pág. 35) Carpeta de red (pág. 35) NFS (pág. 35)*		
Sitios web (archivos y bases de datos MySQL)	Selección directa (pág. 126)	Nube (pág. 35)	—	
Estado del sistema	Selección directa (pág. 34)	Nube (pág. 35) Carpeta local (pág. 35) Carpeta de red (pág. 35)	Siempre completas (pág. 38) Completas semanalmente, incrementales diariamente (pág. 38) Personalizadas (F-I) (pág. 38)	
Bases de datos SQL	Selección directa (pág. 110)			
Bases de datos de Exchange	Selección directa (pág. 111)			
Buzones de correo de Office 365	Selección directa (pág. 122)		Siempre incremental (archivo único) (pág. 38)	

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

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

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

8.2.1 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. 50).

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.

8.2.1.1 ¿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)**, 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.

8.2.2 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. 50).

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**.

8.2.3 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

8.2.4 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. Vaya a **VMware** > **Servidores y clústeres**.
2. Busque los servidores ESXi de los que desea realizar la copia de seguridad.
3. Seleccione los servidores ESXi y haga clic en **Copia de seguridad**.
4. En **De qué realizar copias de seguridad**, seleccione **Configuración de ESXi**.
5. 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.

8.3 Seleccionar un destino

Haga clic en **Dónde hacer copias de seguridad** y seleccione una de las siguientes opciones:

- **Almacenamiento en la cloud**

  Las copias de seguridad se almacenarán en el centro de datos de la cloud.

- **Carpetas locales**

  Si se selecciona un único equipo, busque una carpeta en el equipo seleccionado o escriba la ruta de la carpeta.

  Si se seleccionan varios equipos, escriba la ruta de la carpeta. Las copias de seguridad se almacenarán en esta carpeta en cada uno de los equipos seleccionados o en el equipo en el que está instalado el Agente para equipos virtuales. Si la carpeta no existe, se creará.

- **Carpeta de red**

  Esta carpeta se comparte a través de SMB/CIFS/DFS.

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

- Para recursos compartidos de SMB o CIFS: `\\<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.

- **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. 36).

8.3.1 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. 148). 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 crear Secure Zone

1. Decida en qué disco quiere crear Secure Zone.
2. Inicie la interfaz de la línea de comandos y escriba **`acrocmd list disks`** para ver el número del disco.
3. Use el comando **`create asz`** de la utilidad **`acrocmd`**. El comando utiliza primero el espacio sin asignar en el disco y, si es insuficiente, toma espacio libre de los volúmenes especificados. Para obtener más información, consulte "Cómo la creación de Secure Zone transforma el disco" más abajo.

   Ejemplos:

   - Creación de una Secure Zone en el disco 1 de un equipo local. Secure Zone se creará con un tamaño predeterminado, que es el promedio entre los valores máximo (todo el espacio sin asignar) y mínimo (unos 50 MB).

     ```
     acrocmd create asz --disk=1
     ```

   - Creación de una Secure Zone protegida con contraseña con un tamaño de 100 GB en el disco 2 del equipo local. Si el espacio sin asignar no es suficiente, el espacio se tomará del segundo volumen de ese disco.

     ```
     acrocmd create asz --disk=2 --volume=2-2 --asz_size=100gb --password=abc12345
     ```

   - Creación de una Secure Zone de 20 GB en el disco 1 de un equipo remoto.

     ```
     acrocmd create asz --host=192.168.1.2 --credentials=john,pass1 --disk=1
     --asz_size=20gb
     ```

   Para ver la descripción detallada del comando **`create asz`**, consulte la referencia de la línea de comando.

Cómo la creación de Secure Zone transforma el disco

- Secure Zone siempre se crea al final del disco duro. Cuando calcule la distribución final de los volúmenes, el programa utilizará primero el espacio sin asignar al final.
- Si no hay espacio o no suficiente espacio sin asignar al final del disco, pero sí hay espacio sin asignar entre volúmenes, los mismos se moverán para agregar más espacio sin asignar al final.
- Cuando se recopile todo el espacio sin asignar y el mismo siga siendo insuficiente, el programa sacará espacio libre de los volúmenes que seleccione, de forma proporcional, reduciendo el tamaño de los volúmenes. Cambiar el tamaño de volúmenes bloqueados requiere reiniciar el sistema.
- 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.

8.4 Planificar

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.

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. 148).

  Este esquema no está disponible al hacer copias de seguridad en 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**).

- **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.

Opciones de planificación adicionales

Con cualquier destino, puede realizar 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. 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, con un valor máximo de demora establecido en 30 minutos.*

8.5 Reglas de retención

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 conservación se especifican para cada conjunto de copias de seguridad (pág. 148) 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.
   - **Guardar las copias de seguridad indefinidamente.**

***Nota** No se puede eliminar una copia de seguridad almacenada en una carpeta local o de red si tiene copias de seguridad dependientes que no pueden ser suprimidas. Estas cadenas de copias de seguridad se eliminan únicamente cuando expira la vida útil de todas sus copias de seguridad. El almacenamiento de copias de seguridad cuya eliminación ha sido pospuesta, requiere espacio adicional. Además, la antigüedad y la cantidad de copias de seguridad pueden superar los valores que especifique.*

8.6 Replicación

Si habilita la réplica de copia de seguridad, cada una de las copias de seguridad se copiará en una segunda ubicación inmediatamente tras su creación. Si las copias de seguridad anteriores no se replicaron (por ejemplo, se perdió la conexión a la red), el software también replica todas las copias de seguridad que aparecieron desde la última replicación realizada correctamente.

Las copias de seguridad replicadas no dependen de las copias de seguridad que permanecen en la ubicación original y viceversa. Puede recuperar los datos desde cualquier copia de seguridad, sin acceso a otras ubicaciones.

Ejemplos de uso

- **Recuperación ante desastres fiable**

Almacene sus copias de seguridad tanto en el lugar (para la recuperación inmediata) como fuera del lugar (para asegurar las copias de seguridad de un fallo de almacenamiento o un desastre natural).

- **Uso del almacenamiento en la cloud para proteger los datos de un desastre natural**

  Replique las copias de seguridad en el almacenamiento en la cloud transfiriendo solo los cambios realizados en los datos.

- **Mantenimiento de solo los últimos puntos de recuperación**

  Elimine las copias de seguridad anteriores para un almacenamiento rápido según las reglas de retención para no utilizar demasiado el espacio de almacenamiento caro.

Ubicaciones compatibles

Puede replicar una copia de seguridad *desde* cualquiera de las siguientes ubicaciones:

- Una carpeta local
- Una carpeta de red
- Secure Zone

Puede replicar una copia de seguridad *en* cualquiera de las siguientes ubicaciones:

- Una carpeta local
- Una carpeta de red
- El almacenamiento en la cloud

Para habilitar la réplica de copia de seguridad

1. En el panel del plan de copias de seguridad, habilite el conmutador **Replicar copias de seguridad**.

   Este conmutador solo se muestra si la replicación es compatible con la ubicación seleccionada en **Dónde realizar copias de seguridad**.
2. En **A dónde replicar**, especifique el destino de la replicación, tal como se describe en "Seleccionar un destino" (pág. 35).
3. En **Cuánto tiempo guardarlas**, especifique las reglas de retención, tal como se describe en "Reglas de retención" (pág. 39).

8.7 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.

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.

Después de guardar la configuración, ya no será posible modificarla, pero sí podrá restablecerla de la forma que se describe a continuación.

Esta opción está disponible para equipos que ejecutan Windows o Linux. No es compatible con OS X.

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.

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 es **%ProgramFiles%\BackupClient**.
   - En Linux: **/usr/sbin/acropsh -m manage_creds --set-password** `<encryption_password>`

Las copias de seguridad se cifrarán por medio del algoritmo EEA con una clave de 256 bits.

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 es **%ProgramFiles%\BackupClient**.
   - En Linux: **/usr/sbin/acropsh -m manage_creds --reset**

Importante: *Si restablece la configuración de cifrado en un equipo, las copias de seguridad de dicho equipo fallarán. Para seguir con la copia de seguridad del equipo, cree un nuevo plan de copias de seguridad.*

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.

8.8 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. Haga clic en **Ejecutar ahora** en el panel del plan de copias de seguridad.

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

8.9 Opciones de copia de seguridad

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	Virtuozzo	Windows
Alertas (pág. 46)	+	+	+	+	+	+	+	+	+	+

	Copia de seguridad a nivel de discos			Copia de seguridad a nivel de archivos			Equipos virtuales			SQL y Exchange
	Windows	Linux	macOS	Windows	Linux	macOS	ESXi	Hyper-V	Virtuozzo	Windows
Consolidación de la copia de seguridad (pág. 46)	+	+	+	+	+	+	+	+	+	-
Formato de la copia de seguridad (pág. 47)	+	+	+	+	+	+	+	+	+	+
Validación de la copia de seguridad (pág. 48)	+	+	+	+	+	+	+	+	+	+
Seguimiento de bloques modificados (CBT) (pág. 48)	+	-	-	-	-	-	+	+	-	-
Tasa de compresión (pág. 49)	+	+	+	+	+	+	+	+	+	+
Manejo de errores (pág. 49)										
Reintentar si se produce un error.	+	+	+	+	+	+	+	+	+	+
No mostrar mensajes ni diálogos durante el procesamiento (modo silencioso)	+	+	+	+	+	+	+	+	+	+
Ignorar los sectores defectuosos	+	+	+	+	+	+	+	+	+	-

	Copia de seguridad a nivel de discos			Copia de seguridad a nivel de archivos			Equipos virtuales			SQL y Exchange
	Windows	Linux	macOS	Windows	Linux	macOS	ESXi	Hyper-V	Virtuozzo	Windows
Reintentar si se produce un error durante la creación de instantáneas de VM	-	-	-	-	-	-	+	+	+	-
Copias de seguridad incrementales/diferenciales rápidas (pág. 50)	+	+	+	-	-	-	-	-	-	-
Instantánea de la copia de seguridad a nivel de archivo (pág. 52)	-	-	-	+	+	+	-	-	-	-
Filtros de archivo (pág. 50)	+	+	+	+	+	+	+	+	+	-
Truncamiento de registros (pág. 52)	-	-	-	-	-	-	+	+	-	Solo SQL
Toma de instantáneas de LVM (pág. 53)	-	+	-	-	-	-	-	-	-	-
Puntos de montaje (pág. 53)	-	-	-	+	-	-	-	-	-	-
Instantánea multivolumen (pág. 54)	+	-	-	+	-	-	-	-	-	-
Rendimiento (pág. 54)	+	+	+	+	+	+	+	+	+	+
Envío de datos físicos (pág. 55)	+	+	+	+	+	+	-	-	-	-
Comandos previos/posteriores (pág. 56)	+	+	+	+	+	+	+	+	+	+

	Copia de seguridad a nivel de discos			Copia de seguridad a nivel de archivos			Equipos virtuales			SQL y Exchange
	Windows	Linux	macOS	Windows	Linux	macOS	ESXi	Hyper-V	Virtuozzo	Windows
Comandos previos o posteriores a la captura de datos (pág. 58)	+	+	+	+	+	+	-	-	-	+
Planificación (pág. 60)										
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. 60)	+	+	-	-	-	-	+	+	+	-
División (pág. 61)	+	+	+	+	+	+	+	+	+	+
Manejo de fallos de la tarea (pág. 61)	+	+	+	+	+	+	+	+	+	+
Volume Shadow Copy Service (VSS)	+	-	-	+	-	-	-	+	-	+
Volume Shadow Copy Service (VSS) para equipos virtuales (pág. 62)	-	-	-	-	-	-	+	+	-	-
Copia de seguridad semanal (pág. 63)	+	+	+	+	+	+	+	+	+	+

	Copia de seguridad a nivel de discos			Copia de seguridad a nivel de archivos			Equipos virtuales			SQL y Exchange
	Windows	Linux	macOS	Windows	Linux	macOS	ESXi	Hyper-V	Virtuozzo	Windows
Registro de eventos de Windows (pág. 63)	+	-	-	+	-	-	+	+	-	+

8.9.1 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.

8.9.2 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 preajuste 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 el almacenamiento en la cloud.
- El esquema de copias de seguridad está configurado como **Siempre incremental (archivo único)**.
- El formato de copia de seguridad (pág. 47) se configura en la **versión 12**.

Las copias de seguridad almacenadas en el almacenamiento en la cloud, con el formato tanto de la versión 11 como de la 12, y las copias de seguridad de archivo único, siempre se consolidan ya que la estructura interna permite realizar una consolidación rápida y sencilla.

Sin embargo, si se usa el formato de la versión 12 y hay varias cadenas de copias de seguridad (cada cadena almacenada en un archivo .tibx independiente), la consolidación solo funciona en la última cadena. El resto de cadenas se eliminan como un todo, excepto la primera, que se reducen 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.

8.9.3 Formato de 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 preajuste 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.
- **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.

Formato y archivos de copia de seguridad

En el caso de las ubicaciones de copia de seguridad que se puedan buscar con un administrador de archivos (como carpetas locales o de red), el formato de copia de seguridad determinará el número de archivos y su extensión. La tabla que aparece a continuación incluye los archivos que se pueden crear por equipo o buzón de correo.

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

8.9.4 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. 128) en el entorno de ESXi o Hyper-V.

8.9.5 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.

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 contenido del disco se rastrean continuamente en el nivel del bloque. Cuando se inicia una copia de seguridad, los cambios se pueden guardar inmediatamente en esta.

8.9.6 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.

8.9.7 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.

8.9.8 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.

8.9.9 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. 47) 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.*

8.9.10 Instantánea de la copia de seguridad a nivel de archivo

Esta opción solo sirve para la copia de seguridad a nivel de archivo.

Esta opción define si se hace una copia de seguridad archivo por archivo o si se toma una instantánea de los datos.

Nota *A los archivos que no estén almacenados en redes compartidas se les realizará la copia de seguridad uno a uno.*

El valor predeterminado es: **Crear instantánea si es posible**.

Puede seleccionar una de las siguientes opciones:

- **Crear instantáneas 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.

8.9.11 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.

8.9.12 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.

8.9.13 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. 82)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. 82)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. 82)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**.

8.9.14 Instantánea multivolumen

Esta opción es eficaz solo en los sistemas operativos de Windows.

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. 52) 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 preajuste es: **Habilitado**.

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.

8.9.15 Rendimiento

Prioridad de proceso

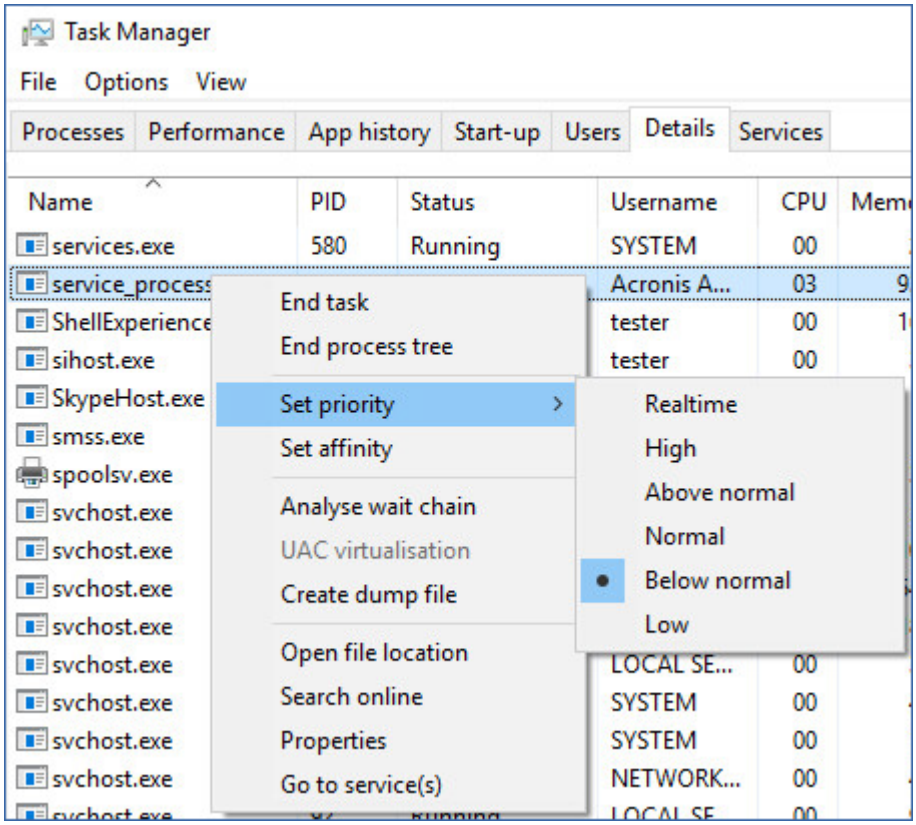
Esta opción define la prioridad del proceso de copia de seguridad en el sistema operativo.

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

El valor predeterminado es: **Baja** (en Windows corresponde a **Por debajo de lo 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 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

Esta opción 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 la nube).

El valor predeterminado es: **Deshabilitado**.

Cuando esta opción está habilitada, puede especificar la velocidad de salida máxima permitida en KB/segundos.

8.9.16 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. 47) 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, el agente para Linux y el agente para Mac.

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 preajuste es: **Deshabilitado**

Acerca del servicio de envío de datos físicos

La interfaz web del servicio de envío de datos físicos solo está disponible para los administradores.

Para obtener instrucciones detalladas acerca del uso del servicio de envío de datos físicos y la herramienta de creación de pedidos, consulte la Guía del administrador para el envío de datos físicos. Para acceder a este documento en la interfaz web del servicio de envío de datos físicos, haga clic en el icono de signo de interrogación.

Información general acerca del proceso de envío de datos físicos

1. 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.

   Para acceder a la interfaz web, inicie sesión en el portal de gestión, haga clic en **Información general** > **Uso** y, a continuación, en **Gestionar servicio**, que encontrará en **Envío de datos físicos**.

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.

8.9.17 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”).

8.9.17.1 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.

8.9.17.2 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**.

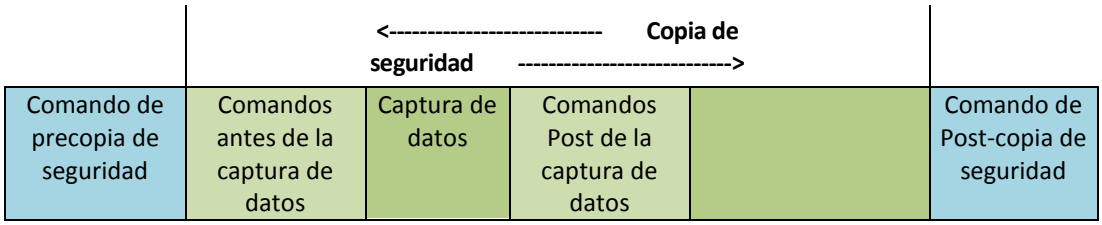
Cuando no se marca la casilla de verificación, los resultados de la ejecución del comando no afectarán al éxito o fallo de la copia de seguridad. Puede realizar un seguimiento de la ejecución de comandos desde la pestaña **Actividades**.

6. Haga clic en **Realizado**.

8.9.18 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 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.

8.9.18.1 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	Seleccionado	Seleccionado	Borrado	Borrado

datos hasta que finalice la ejecución de comandos				
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.

8.9.18.2 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.

8.9.19 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: **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. 143) 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.

8.9.20 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. 49) 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.

8.9.21 División

Esta opción sirve para los esquemas de copias de seguridad **Siempre completas**, **Completas semanalmente, incrementales diariamente** y **Personalizado**.

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.

8.9.22 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**.

8.9.23 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**.

La selección entre el proveedor de instantáneas de hardware, los proveedores de instantáneas de software y el Proveedor de instantáneas de software de Microsoft la lleva a cabo automáticamente el Servicio de instantáneas de volumen.

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. 58) 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. 52).

8.9.24 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. 49) 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.

8.9.25 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**.

8.9.26 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**.

9 Recuperación

9.1 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. 65) Uso de dispositivos de arranque (pág. 69)
Equipo físico (Mac)	Uso de dispositivos de arranque (pág. 69)
Equipo virtual (VMware o Hyper-V)	Uso de la interfaz web (pág. 67) Uso de dispositivos de arranque (pág. 69)
Equipo virtual o contenedor (Virtuozzo)	Uso de la interfaz web (pág. 67)
Configuración de ESXi	Uso de dispositivos de arranque (pág. 77)
Archivos/Carpetas	Uso de la interfaz web (pág. 73) Descargar archivos del almacenamiento en la cloud (pág. 74) Uso de dispositivos de arranque (pág. 76) Extraer archivos de copias de seguridad locales (pág. 77)
Estado del sistema	Uso de la interfaz web (pág. 77)
Bases de datos SQL	Uso de la interfaz web (pág. 113)
Bases de datos de Exchange	Uso de la interfaz web (pág. 115)
Buzones de correo de Exchange	Uso de la interfaz web (pág. 117)
Buzones de correo de Office 365	Uso de la interfaz web (pág. 123)
Sitios web	Uso de la interfaz web (pág. 127)

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.

9.2 Crear dispositivos de inicio

El dispositivo de inicio es un CD, DVD, unidad flash USB u otro dispositivo extraíble que le permite ejecutar el Agente sin la ayuda de un sistema operativo. El objetivo principal del dispositivo de inicio es recuperar un sistema operativo que no se pueda iniciar.

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

Puede recuperar tanto Windows como Linux con el mismo dispositivo. Para recuperar OS X, cree un dispositivo diferente en un equipo que ejecute OS X.

Para crear dispositivos de inicio en Windows o Linux

1. Descargue el archivo ISO de dispositivo de arranque. Para descargar el archivo, seleccione un equipo y haga clic en **Recuperar** > **Otros métodos de recuperación...** > **Descargar la imagen ISO**.
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 y para un equipo BIOS, use `Win32DiskImager`. En Linux, debe usar la utilidad `dd`.
   - Conecte el archivo ISO como una unidad de CD/DVD al equipo virtual que desea recuperar.

Para crear dispositivos de inicio en OS X

1. En un equipo donde esté instalado Agente para Mac, haga clic en **Aplicaciones** > **Rescue Media Builder**.
2. El software muestra los dispositivos extraíbles conectados. Seleccione el que desee convertir en un dispositivo de inicio.

   Advertencia *Toda la información del disco se borrará.*
3. Haga clic en **Crear**.
4. Espere mientras el software crea el dispositivo de inicio.

9.3 Recuperar un equipo

9.3.1 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:

- OS X
- Cualquier sistema operativo desde cero o en un equipo sin conexión

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. 100).
   - Recupere el equipo como se describe en "Recuperar discos usando dispositivos de inicio" (pág. 69).
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.

- Si la asignación de discos falla, recupere el equipo como se detalla en "Recuperar discos usando dispositivos de inicio" (pág. 69). El dispositivo le permite elegir los discos que desea recuperar y asignarlos manualmente.

5. Haga clic en **Iniciar recuperación**.
6. 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**.

9.3.2 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. 137).

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. 100).
   - Recupere el equipo como se describe en "Recuperar discos usando dispositivos de inicio" (pág. 69).
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 **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**.

9.3.3 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.

Es posible modificar este comportamiento mediante la opción de recuperación de gestión de energía del equipo virtual (haga clic en **Opciones de recuperación** > **Gestión de energía del equipo virtual**).

Para recuperar un equipo virtual

1. Realice uno de los siguientes procedimientos:
   - Seleccione un equipo incluido en la copia de seguridad, haga clic en **Recuperación** y, a continuación, seleccione un punto de recuperación.
   - Seleccione un punto de recuperación en la pestaña de copias de seguridad (pág. 100).
2. Haga clic en **Recuperar** > **Todo el equipo**.
3. Si desea recuperar 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 en "Equipo físico" (pág. 65). En caso contrario, se recomienda realizar la migración V2P mediante el uso de dispositivos de inicio (pág. 69).
4. El software selecciona automáticamente el equipo original como equipo de destino.

   Para recuperar en otro equipo virtual, haga clic en **Equipo de destino** y, a continuación, haga lo siguiente:

   a. Seleccione el hipervisor (**VMware ESXi**, **Hyper-V** o **Virtuozzo**).

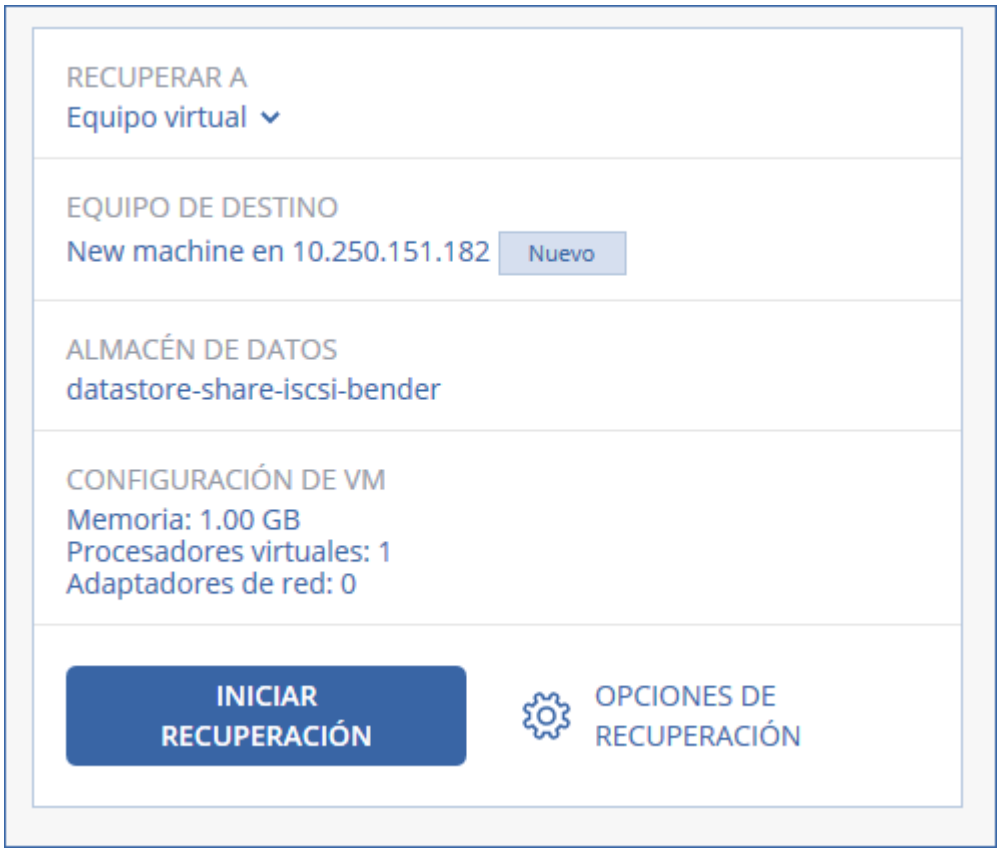
      Solo los equipos virtuales Virtuozzo pueden recuperarse en Virtuozzo. Para más información sobre la migración V2V, consulte "Migración de equipos" (pág. 137).

   b. Seleccione si desea realizar la recuperación en un equipo nuevo o 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 de acceso** para Hyper-V y Virtuozzo. A continuación, seleccione el almacén de datos (almacenamiento) 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. 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**.

9.3.4 Recuperar discos usando dispositivos de arranque

Para obtener información sobre cómo crear dispositivos de inicio, consulte "Crear dispositivos de arranque" (pág. 64).

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.

9.3.5 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. 71).
5. Haga clic en **Aceptar**.

9.3.5.1 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.

9.3.5.2 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.

9.4 Recuperación de archivos

9.4.1 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 una de las siguientes operaciones:

   - [Recomendado] Si la copia de seguridad se encuentra en el almacenamiento compartido o en la cloud (es decir, otros agentes pueden acceder a ella), haga clic en **Seleccionar equipo**, seleccione un equipo de destino que tenga conexión a Internet y, a continuación, seleccione un punto de recuperación.
   - Seleccione un punto de recuperación en la pestaña de copias de seguridad (pág. 100).
   - Descargue los archivos desde el almacenamiento en la cloud (pág. 74).
   - Use dispositivos de arranque (pág. 76).
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. 50).

   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.
8. Haga clic en **Recuperar**.

   En **Recuperar en**, verá una de las opciones siguientes:

   - El equipo que contenía originalmente los archivos que quiere recuperar (si hay un agente instalado en este equipo).
   - El equipo donde está instalado Agente para VMware, Agente para Hyper-V o Agente para Virtuozzo (si los archivos proceden de un equipo virtual ESXi, Hyper-V o Virtuozzo).

   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**.

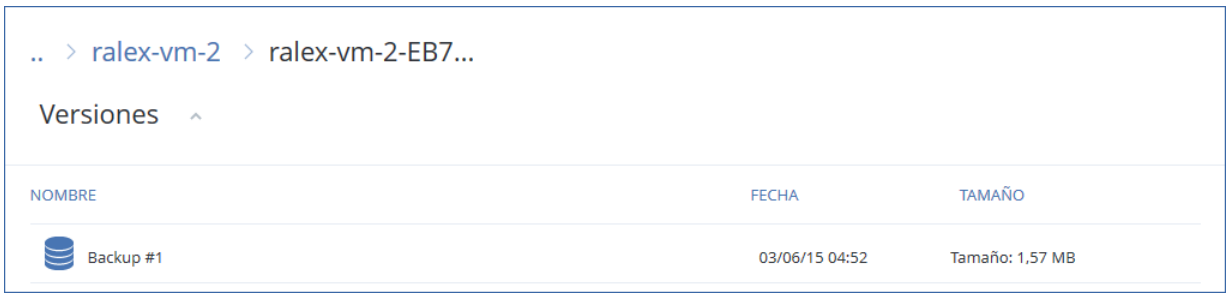
9.4.2 Descargar archivos del almacenamiento en la nube

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

Limitación: 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.

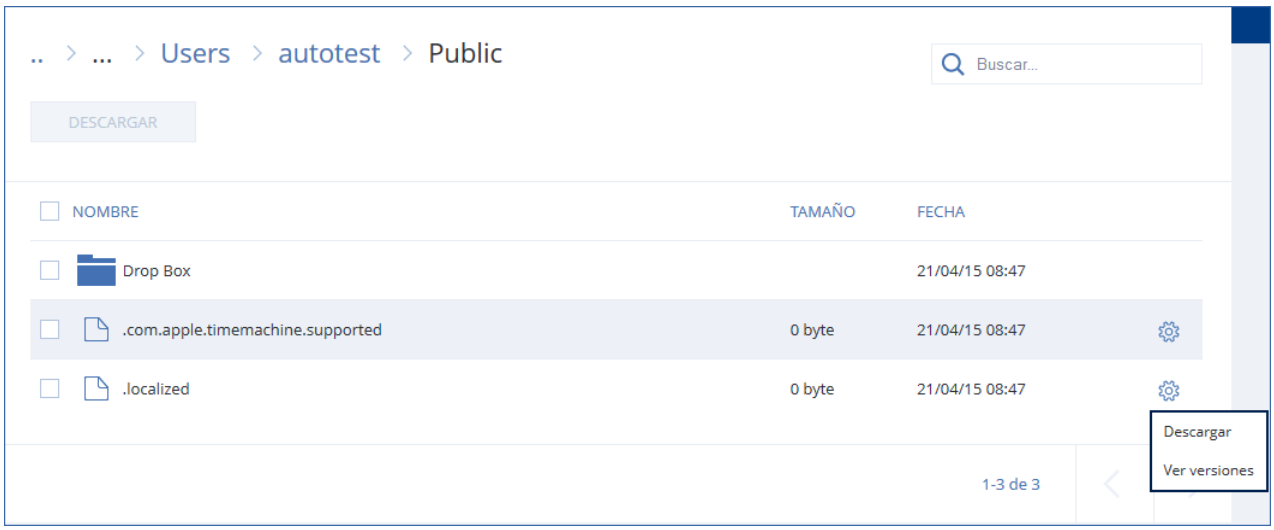
Para descargar archivos del almacenamiento en la nube

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] Bajo **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 y carpetas 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**.

9.4.3 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. 73).
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.

9.4.4 Recuperación de archivos usando dispositivos de arranque

Para obtener información sobre cómo crear dispositivos de arranque, consulte "Crear dispositivos de arranque" (pág. 64).

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.

9.4.5 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.

9.5 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**.

9.6 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. 64).

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. Si la copia de seguridad se encuentra en el almacenamiento en la cloud al que se accede a través de un servidor proxy, haga clic en **Herramientas** > **Servidor proxy** y después indique el nombre de servidor/dirección IP y el puerto. 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:
   - Vaya a la carpeta ubicada en **Carpetas locales** o **Carpetas de red**.

   Haga clic en **Aceptar** para confirmar su selección.
7. En **Mostrar**, seleccione **Configuración de ESXi**.
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. Haga clic en **Aceptar**.
10. 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.
11. 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**.
12. [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.
13. [Opcional] Haga clic en **Opciones de recuperación** para especificar configuraciones adicionales.
14. Haga clic en **Aceptar** para comenzar la recuperación.

9.7 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, Hyper-V y Virtuozzo	Windows
Validación de la copia de seguridad (pág. 80)	+	+	+	+	+	+	+	+	+
Fecha y hora de los archivos (pág. 81)	-	-	-	+	+	+	+	-	-
Manejo de errores (pág. 80)	+	+	+	+	+	+	+	+	+
Exclusiones de archivos (pág. 81)	-	-	-	+	+	+	+	-	-
Seguridad a nivel de archivo (pág. 81)	-	-	-	+	-	-	-	-	-
Flashback (pág. 81)	+	+	+	-	-	-	-	+	-
Recuperación de ruta completa (pág. 81)	-	-	-	+	+	+	+	-	-
Puntos de montaje (pág. 82)	-	-	-	+	-	-	-	-	-
Rendimiento (pág. 82)	+	+	-	+	+	+	-	+	+
Comandos previos/posteriores (pág. 82)	+	+	-	+	+	+	-	+	+
Cambios en el identificador de seguridad (SID) (pág. 84)	+	-	-	-	-	-	-	-	-
Gestión de energía de VM (pág. 84)	-	-	-	-	-	-	-	+	-

	Discos			Archivos				Equipos virtuales	SQL y Exchange
	Windows	Linux	Dispositivo de arranque	Windows	Linux	macOS	Dispositivo de arranque	ESXi, Hyper-V y Virtuozzo	Windows
Registro de eventos de Windows (pág. 84)	+	-	-	+	-	-	-	Solo Hyper-V	+

9.7.1 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.

9.7.2 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: **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: **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.

9.7.3 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**.

9.7.4 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.*

9.7.5 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.

9.7.6 Flashback

Esta opción es efectiva cuando se recuperan discos y volúmenes en equipos físicos y virtuales, excepto para Mac.

Esta opción solo funciona si el diseño del volumen del disco que se está recuperando coincide exactamente con el del disco de destino.

Si esta opción está habilitada, solo se recuperan las diferencias entre los datos en la copia de seguridad y los datos en el disco de destino. Esto acelera la recuperación de los equipos físicos y virtuales. Los datos se comparan a nivel de bloque.

Cuando se recupera un equipo físico, el valor predeterminado es: **Deshabilitado**.

Cuando se recupera un equipo virtual, el valor predeterminado es: **Habilitado**.

9.7.7 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**.

9.7.8 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. 53) 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.*

9.7.9 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.

9.7.10 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.

9.7.10.1 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.

9.7.10.2 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.*

9.7.11 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.

9.7.12 Gestión de energía de VM

Estas opciones son efectivas cuando Agente para VMware, Agente para Hyper-V o Agente para Virtuozzo realizan la recuperación en un equipo virtual.

Apagar máquinas virtuales de destino al iniciar la recuperación

El valor predeterminado: **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 de otro equipo, es posible que la réplica del equipo existente aparecerá en la red. Para tener seguridad, encienda la máquina virtual manualmente, después de tomar las precauciones necesarias.

9.7.13 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**.

10 Recuperación ante desastres

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
- 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.

10.1 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
- Debian 9
- Ubuntu 16.04
- Windows Server 2008/2008 R2
- Windows Server 2012/2012 R2
- Windows Server 2016: todas las opciones de instalación, excepto Nano Server

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

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.

10.2 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:

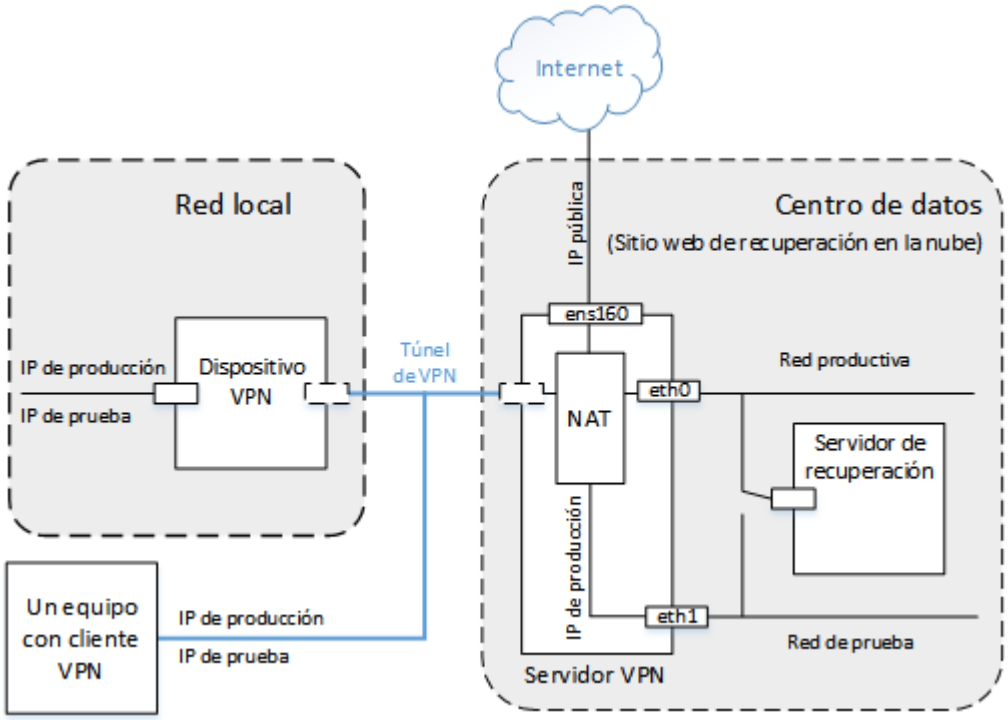
- Un dispositivo VPN, situado en sus instalaciones.
- Un servidor VPN, ubicado en el sitio web de recuperación en la cloud.

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.



10.2.1 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.

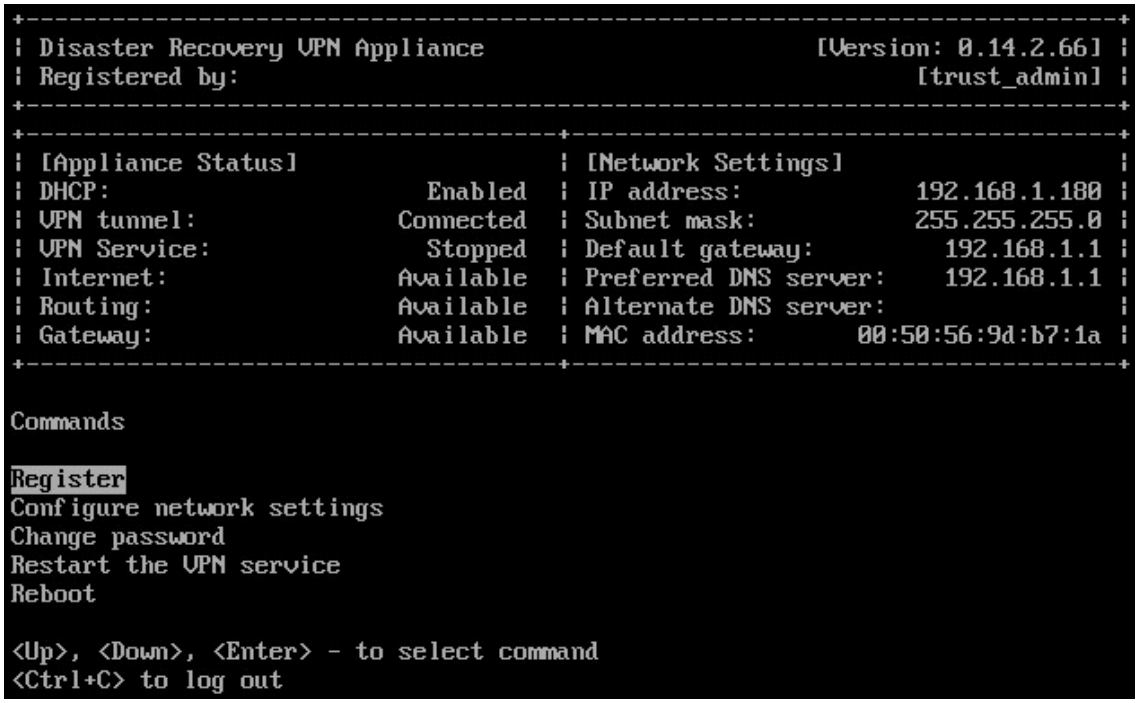
   El sistema empieza a implementar el servidor VPN en la cloud. Este proceso tardará cierto tiempo; mientras tanto, puede continuar con el siguiente paso.

   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.

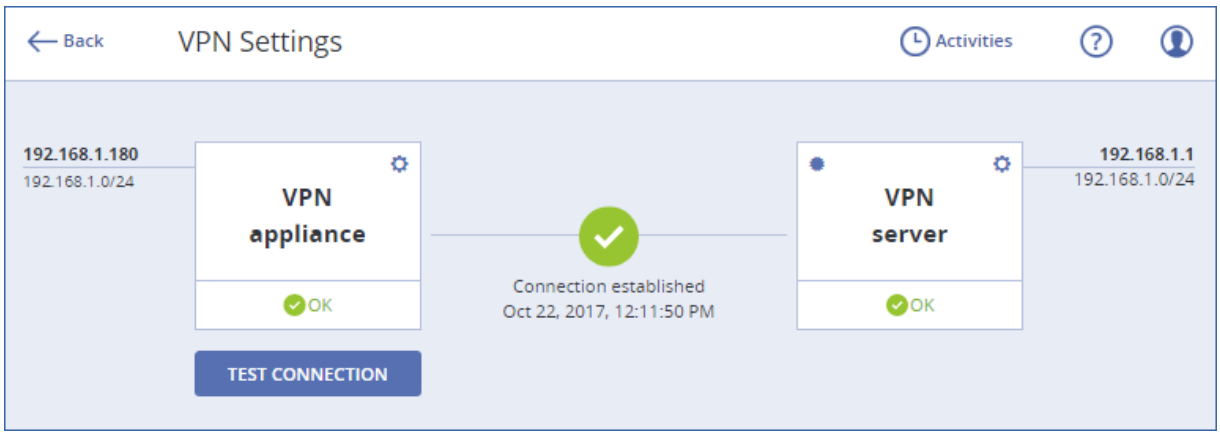
6. Abra la consola del dispositivo e inicie sesión con el usuario y la contraseña "admin"/"admin".



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.

10.2.2 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.

10.2.3 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.

10.2.4 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. 91).

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. 91).
- 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.

10.3 Trabajar con un servidor se recuperación

10.3.1 Creación de un servidor de recuperación

Requisitos previos

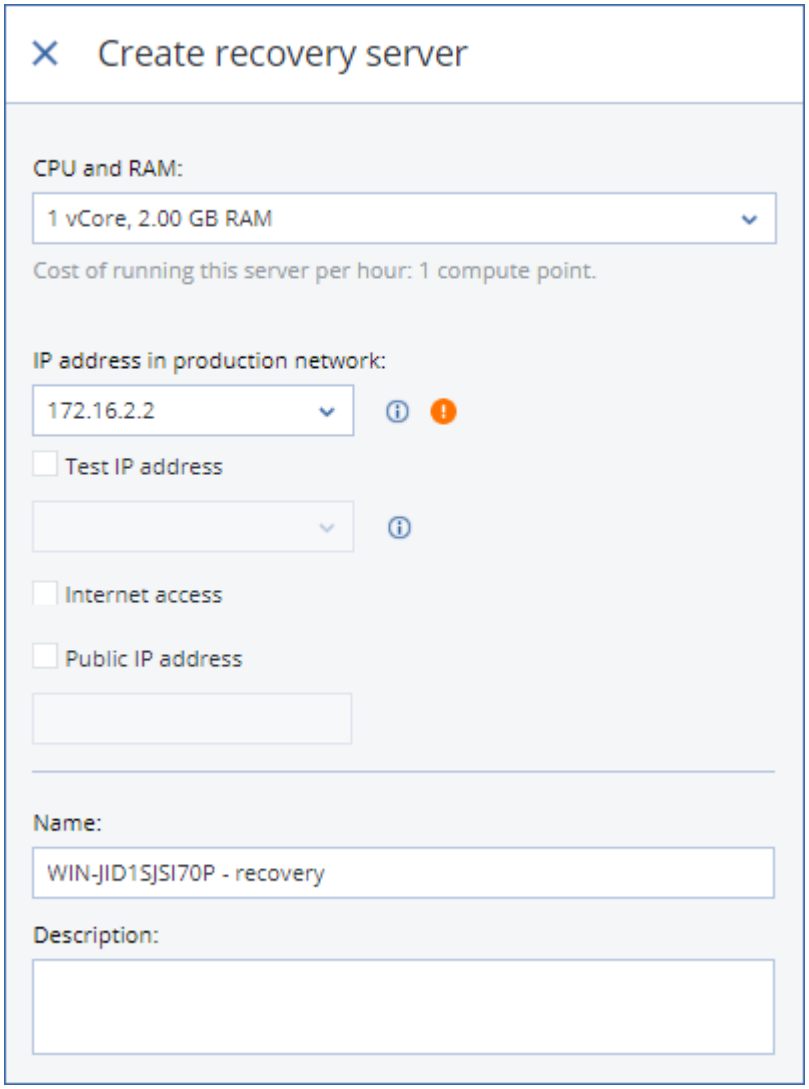
- Los planes de copias de seguridad se deben aplicar al equipo que quiera proteger.
  - Puede realizar copias de seguridad de todo el equipo o únicamente de los discos necesarios para iniciarlo y proporcionar los servicios necesarios.
  - Se debe seleccionar el almacenamiento en la cloud como destino.
  - 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:

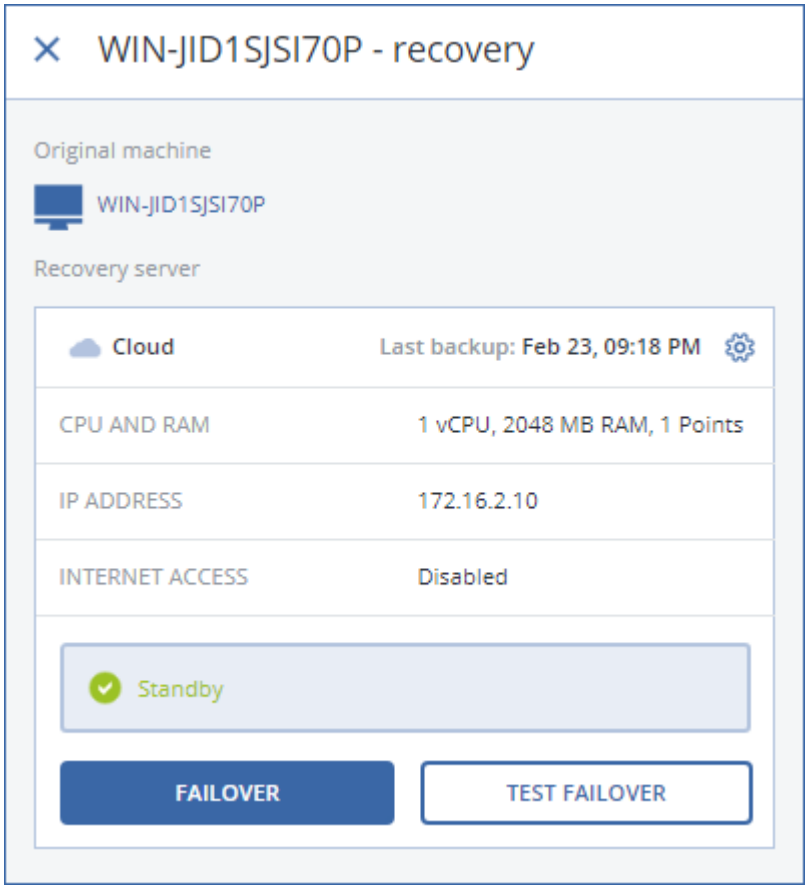
   TCP: 80, 443, 8088, 8443

   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**.



10.3.2 Cómo funciona la conmutación por error

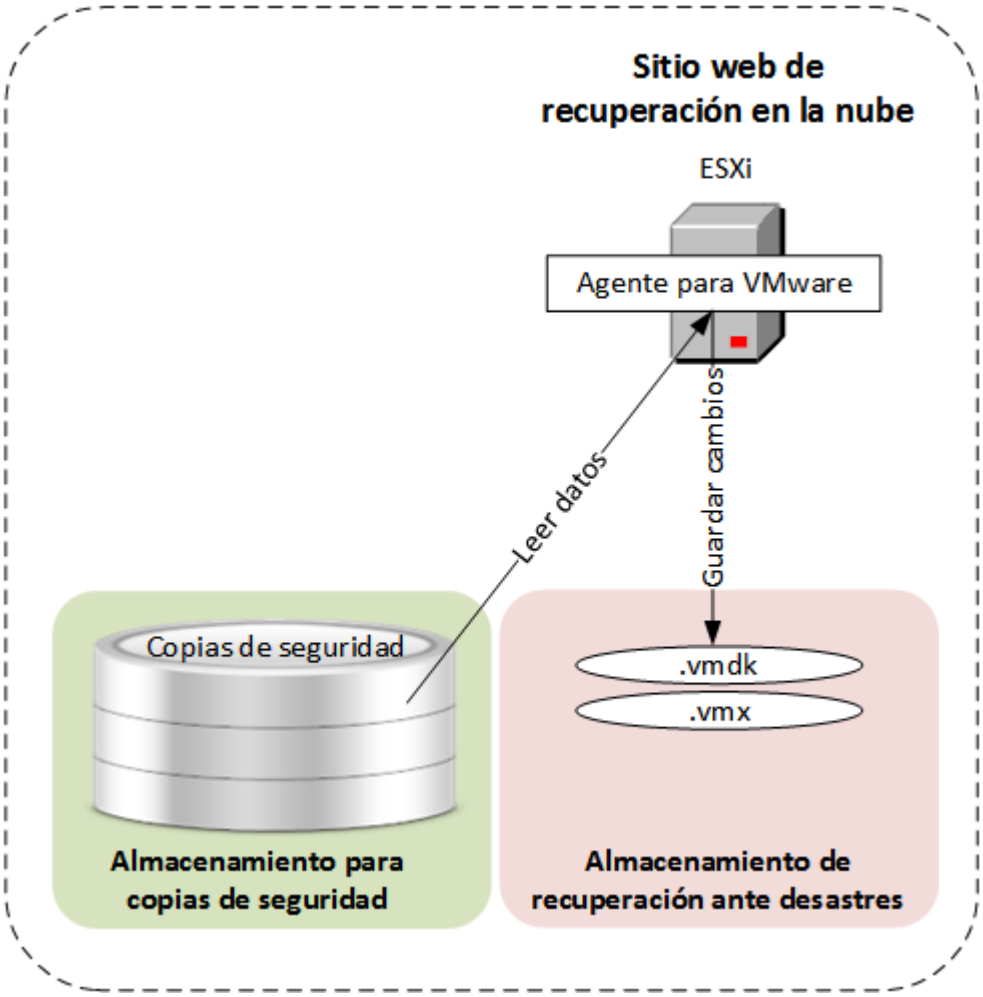
El funcionamiento de la conmutación por error emplea la funcionalidad "ejecutar un equipo virtual desde una copia de seguridad" (pág. 128).

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 real, el equipo virtual se apaga lo antes posible para conseguir el mejor rendimiento. Durante una conmutación por error de prueba, equipo virtual no se apaga. Por lo tanto, puede funcionar más lento, pero ocupa mucho menos espacio en el almacén de datos (almacenamiento de recuperación ante desastres).

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.



10.3.3 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 directa a la cloud" (pág. 91).
   - 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.

10.3.4 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 **Conmutación por error**.
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 iniciado, se crea automáticamente un nuevo plan de copias de seguridad y se aplica a él. 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. 100).

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

10.3.5 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. 69). 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. 65).

   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.

10.4 Trabajar con un servidor principal

10.4.1 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.

10.4.2 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. 100).

10.5 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.

11 Operaciones con copias de seguridad

11.1 Pestaña Copias de seguridad

La pestaña **Copias de seguridad** le permite acceder a todas las copias de seguridad, incluidas las de los equipos, conectados o no, que ya no están registrados en el servicio de copia de seguridad.

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. Un administrador puede visualizar las copias en nombre de cualquier cuenta que pertenezca a dicha unidad o compañía 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.

11.2 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. Los volúmenes se montan en modo de solo lectura.

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).

Para montar un volumen desde una copia de seguridad

1. Busque la ubicación de la copia de seguridad utilizando el Explorador de archivos.
2. Haga doble clic en el archivo de copia de seguridad. Los nombres de los archivos se basan en la siguiente plantilla:

   `<nombre del equipo> - <GUID del plan de 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 el volumen que desea montar y, a continuación, haga clic en **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**.

   El software desmonta el volumen seleccionado.

11.3 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, a continuación, haga clic en el icono de la X.
   - 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, a continuación, haga clic en el signo de la X.
   - Para eliminar el grupo seleccionado, haga clic en **Eliminar**.
4. Confirme su decisión.

12 Operaciones con los planes de copias de seguridad

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 de engranaje que se encuentra al lado del nombre del plan 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 de al lado del nombre del plan de copias de seguridad y después, haga clic 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 de al lado del nombre del plan y después, haga clic en **Borrar**.

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

13 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.

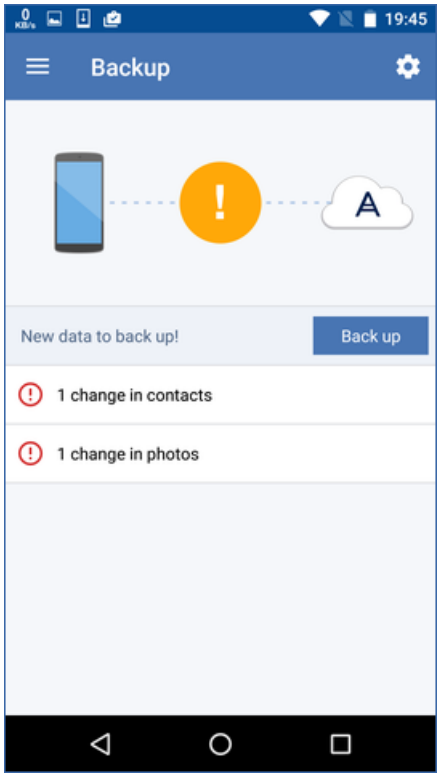
De qué puede realizar una copia de seguridad

- 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 escriba el URL de la consola de copias de seguridad.
2. Inicie sesión con los datos de su cuenta.
3. Haga clic en **Todos los dispositivos** > **Añadir**.
4. En **Dispositivos móviles**, seleccione el tipo de dispositivo.

   Según el tipo de dispositivo, es posible que sea redirigido a App Store o Google Play.
5. [Solo en dispositivos iOS] Haga clic en **Obtener**.
6. Haga clic en **Instalar** para instalar la aplicación de copias de seguridad.

Para iniciar una copia de seguridad de un dispositivo iOS

1. Abra la aplicación de copias de seguridad.
2. Inicie sesión con los datos de su cuenta.
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.

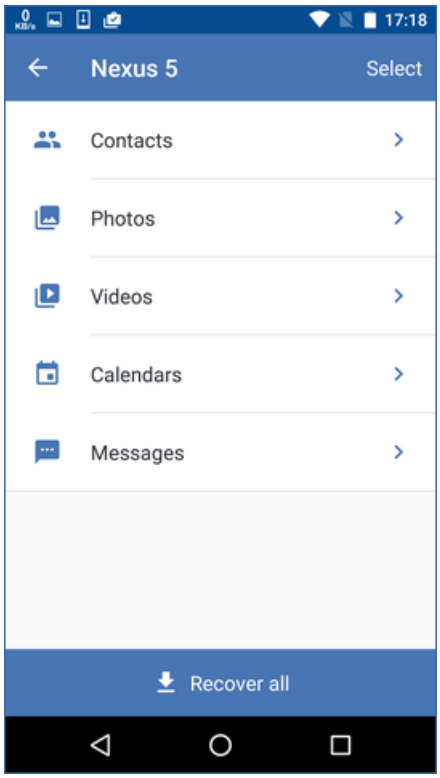
Para iniciar una copia de seguridad de un dispositivo Android

1. Abra la aplicación de copias de seguridad.
2. Inicie sesión con los datos de su cuenta.
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**.

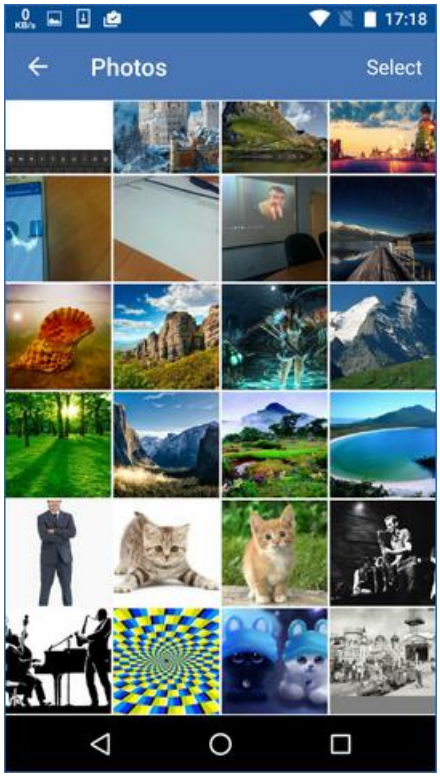
Para recuperar los datos a un dispositivo móvil

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.



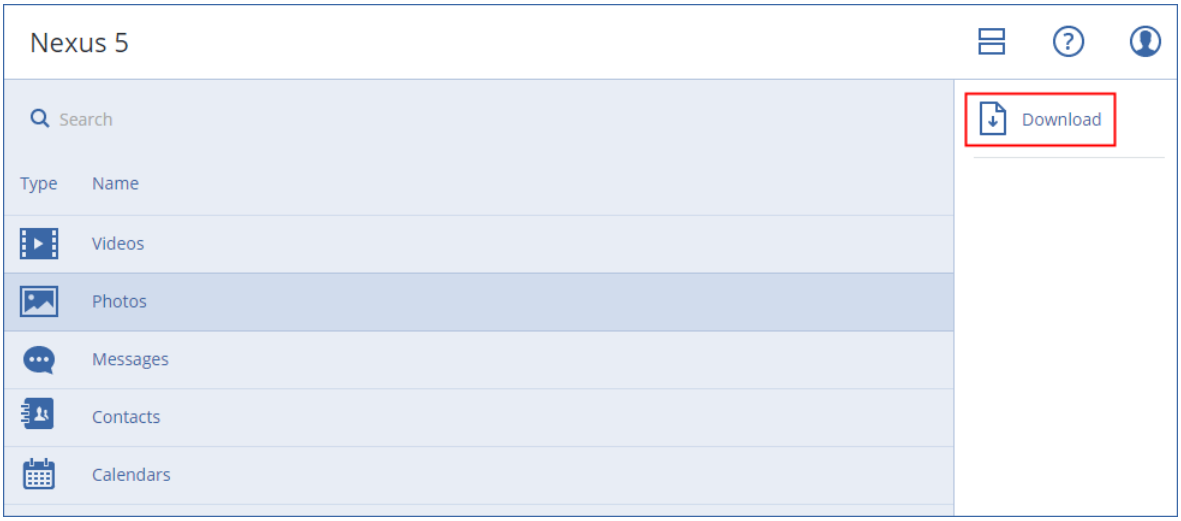
5. Realice uno de los siguientes procedimientos:
   - Para recuperar un único elemento, púlselo.
   - Para recuperar varios elementos, pulse **Seleccionar** y después seleccione las casillas de verificación de los elementos elegidos.



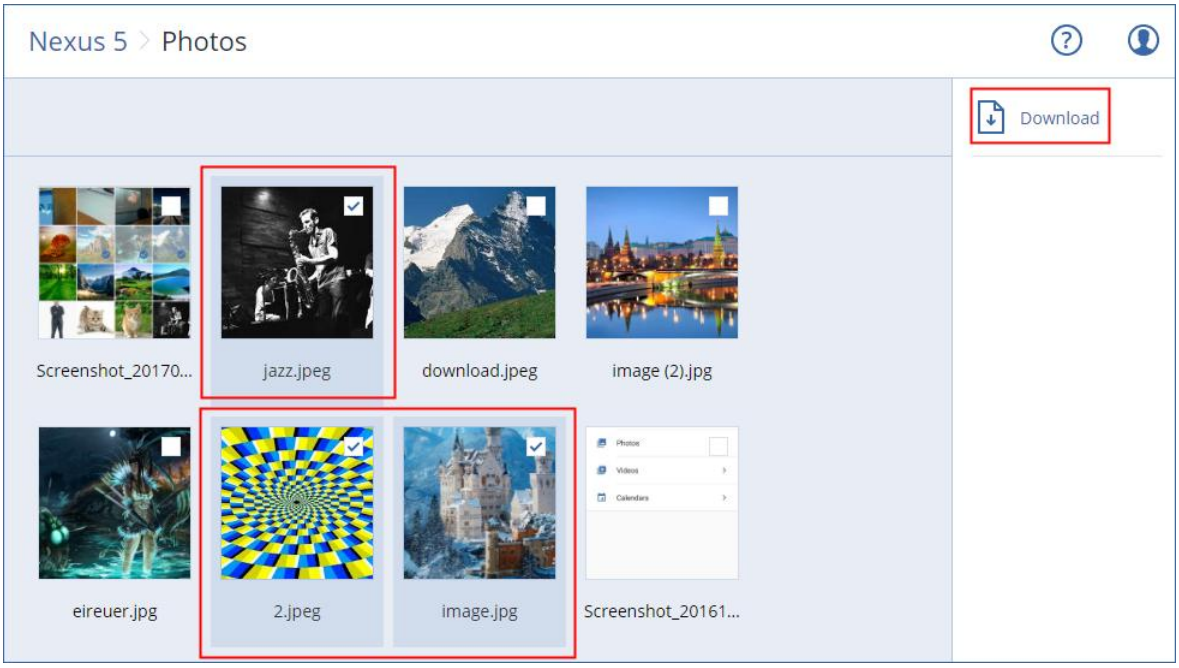
6. Pulse **Recuperar**.

Para acceder a los datos a través de la consola de copias de seguridad

1. En un equipo, abra un explorador y escriba el URL de la consola de copias de seguridad.
2. Inicie sesión con los datos de su cuenta.
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).

14 Protección de las aplicaciones

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.

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. 113) Bases de datos como archivos (pág. 113)	Todo el equipo (pág. 65) Bases de datos a una instancia activa de SQL Server (pág. 113) Bases de datos como archivos (pág. 113)	Todo el equipo (pág. 65)
Microsoft Exchange Server	Bases de datos a un servidor activo de Exchange (pág. 115) Bases de datos como archivos (pág. 115) Recuperación granular en un servidor activo de Exchange (pág. 117)	Todo el equipo (pág. 65) Bases de datos a un servidor activo de Exchange (pág. 115) Bases de datos como archivos (pág. 115) Recuperación granular en un servidor activo de Exchange (pág. 117)	Todo el equipo (pág. 65)
Servidores de bases de datos de Microsoft SharePoint	Bases de datos a una instancia activa de SQL Server (pág. 113) Bases de datos como archivos (pág. 113) Recuperación granular mediante SharePoint Explorer	Todo el equipo (pág. 65) Bases de datos a una instancia activa de SQL Server (pág. 113) Bases de datos como archivos (pág. 113) Recuperación granular mediante SharePoint Explorer	Todo el equipo (pág. 65)
Servidor web front-end de Microsoft SharePoint	-	-	Todo el equipo (pág. 65)
Servicios de dominio de Active Directory	-	Todo el equipo (pág. 65)	-

14.1 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) esté habilitada.
- En los equipos virtuales, la opción de copia de seguridad Volume Shadow Copy Service (VSS) para equipos virtuales (pág. 62) 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.

14.2 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. 109).

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. 29).

14.2.1 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. 52).

Para seleccionar bases de datos de SQL

1. Haga clic en **Microsoft SQL**.

   Se muestran los equipos que tienen instalado el Agente para SQL.
2. Busque los datos de los que desea realizar la copia de seguridad.

   Haga doble clic sobre un equipo para ver las instancias de SQL Server que contiene. Haga doble clic sobre una instancia para ver las bases de datos que contiene.

3. Seleccione los datos de los que desea realizar la copia de seguridad. Puede seleccionar las instancias completas o bases de datos individuales.
   - Si selecciona las instancias completas de SQL Server, se realizarán copias de seguridad de todas las bases de datos actuales y de todas las bases de datos que se añadan a las instancias seleccionadas en el futuro.
   - 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 copias de seguridad** o **Administradores** en el equipo y miembro de la función **administrador del sistema** en cada una de las instancias de las que va a realizar la copia de seguridad.

14.2.2 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 premisos 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	Bases de datos	Pertenencia al grupo de funciones **Administración de servidores**.

Una copia de seguridad completa contiene todos los datos seleccionados de Exchange Server.

Una copia de seguridad incremental contiene los bloques cambiados de los archivos de la base de datos, los archivos de control y una pequeña cantidad de archivos de acceso que son más recientes que el punto de control de la base de datos correspondiente. Ya que los cambios en los archivos de la base de datos están incluidos en la copia de seguridad, no hay necesidad de realizar copias de seguridad de todos los registros de acceso de transacción desde la copia de seguridad anterior. Después de una recuperación, únicamente se necesita reproducir el acceso que sea más reciente que el punto de control. Esto garantiza una recuperación más rápida y que la copia de seguridad de la base de datos se realice con éxito, aun con el registro circular habilitado.

Los archivos de registro de transacción quedan truncados después de cada copia de seguridad realizada con éxito.

Para seleccionar datos de Exchange Server

1. Haga clic en **Microsoft Exchange**.

   Se mostrarán los equipos que tengan instalado el Agente para Exchange.
2. Busque los datos de los que desea realizar la copia de seguridad.

   Haga doble clic sobre el equipo para ver las bases de datos (grupos de almacenamiento) que contiene.
3. Seleccione los datos de los que desea realizar la copia de seguridad. Si se le pide, proporcione las credenciales para acceder a los datos.
4. Haga clic en **Copia de seguridad**.

14.3 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. 52). Los registros de transacción de Exchange solo se truncan en los equipos virtuales. Puede habilitar la opción de copia de seguridad completa de VSS si quiere truncar los registros de transacción de Exchange en un equipo físico.
4. Si un dominio contiene más de un controlador de dominios y desea recuperar alguno de ellos, se realizará una restauración no autorizada y no habrá reversión USN alguna después de la recuperación.

¿Qué necesito para usar la copia de seguridad compatible con la aplicación?

En un equipo físico, hay que tener instalado Agente para SQL o Agent for Exchange además de Agente para Windows. En un equipo virtual no es necesario instalar ningún agente; se presupone que Agente para VMware (Windows) hace una copia de seguridad del equipo.

En las secciones "Requisitos previos" (pág. 109) y "Derechos de usuario necesarios" (pág. 112) se recogen otros requisitos.

14.3.1 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.

14.4 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, auditorías 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. 115).

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. 114).

Para recuperar bases de datos SQL.

1. Si recupera desde una copia de seguridad de base de datos, haga clic en **Microsoft SQL**. De lo contrario, omita este paso.
2. Seleccione el equipo 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. Realice uno de los siguientes procedimientos:

   - Si la copia de seguridad se encuentra en el almacenamiento compartido o en la cloud (es decir, otros agentes pueden acceder a ella), haga clic en **Seleccionar equipo**, seleccione un equipo conectado que tenga instalado Agente para SQL y, a continuación, seleccione un punto de recuperación.
   - Seleccione un punto de recuperación en la pestaña de copias de seguridad (pág. 100).

   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.
5. Realice uno de los siguientes procedimientos:
   - Si recupera desde una copia de seguridad de base de datos, haga clic en **Recuperar bases de datos SQL**.
   - Si recupera desde una copia de seguridad compatible con la aplicación, haga clic en **Recuperar** > **Bases de datos SQL**.
6. Seleccione los datos que desea recuperar. Haga doble clic sobre una instancia para ver las bases de datos que contiene.

7. Si desea recuperar las bases de datos como archivos, haga clic en **Recuperar como archivos**, seleccione una carpeta local o de red donde guardar los archivos y haga clic en **Recuperar**. De lo contrario, omita este paso.
8. Haga clic en **Recuperar**.
9. 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.
10. [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.
11. Haga clic en **Iniciar recuperación**.

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

14.4.1 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.

14.4.2 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**.

14.5 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	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. 117).

Si solo usa Agente para VMware, el único método de recuperación disponible será la recuperación de bases de datos como archivos.

Para recuperar los datos de Exchange

Nos referiremos tanto a las bases de datos como a los grupos de almacenamiento como «bases de datos» a lo largo de este procedimiento.

1. Si recupera desde una copia de seguridad de base de datos, haga clic en **Microsoft Exchange**. De lo contrario, omita este paso.
2. Seleccione el equipo 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:

   - 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, a continuación, seleccione un punto de recuperación.
   - Seleccione un punto de recuperación en la pestaña de copias de seguridad (pág. 100).

   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.
5. Haga clic en **Recuperar** > **Bases de datos de Exchange**.
6. Seleccione los datos que desea recuperar.
7. Si desea recuperar las bases de datos como archivos, haga clic en **Recuperar como archivos**, seleccione una carpeta local o de red donde guardar los archivos y haga clic en **Recuperar**. De lo contrario, omita este paso.
8. Haga clic en **Recuperar**. Si se le pide, proporcione las credenciales para acceder a Exchange Server.
9. 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.

10. Haga clic en **Iniciar recuperación**.

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

14.5.1 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 Clean Shutdown (cierre limpio) 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 2016: http://technet.microsoft.com/es-es/library/aa998871.aspx
- Exchange 2013: http://technet.microsoft.com/es-es/library/aa998871(v=EXCHG.150).aspx
- Exchange 2010: http://technet.microsoft.com/es-es/library/aa998871(v=EXCHG.141).aspx
- Exchange 2007: http://technet.microsoft.com/es-es/library/aa998871(v=EXCHG.80).aspx

14.6 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 y de copias de seguridad compatibles con la aplicación.

Generalidades

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 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.

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.

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. Los elementos de buzón de correo siempre se recuperan en la carpeta **Elementos recuperados** del buzón de correo de destino.

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.

14.6.1 Recuperación de buzones de correo

1. Si recupera desde una copia de seguridad de base de datos, haga clic en **Microsoft Exchange**. De lo contrario, omita este paso.
2. Seleccione el equipo 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:

   - 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 Agente para VMware y, a continuación, seleccione un punto de recuperación.
   - Seleccione un punto de recuperación en la pestaña de copias de seguridad (pág. 100).

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. 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. 121).
9. [Opcional] Haga clic en **Base de datos para volver a crear buzones de correo faltantes** para cambiar la base de datos seleccionada automáticamente.
10. Haga clic en **Iniciar recuperación**.
11. Confirme su decisión.

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

14.6.2 Recuperación de elementos de buzón de correo

1. Si recupera desde una copia de seguridad de base de datos, haga clic en **Microsoft Exchange**. De lo contrario, omita este paso.
2. Seleccione el equipo 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:

   - 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 Agente para VMware y, a continuación, seleccione un punto de recuperación.
   - Seleccione un punto de recuperación en la pestaña de copias de seguridad (pág. 100).

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.

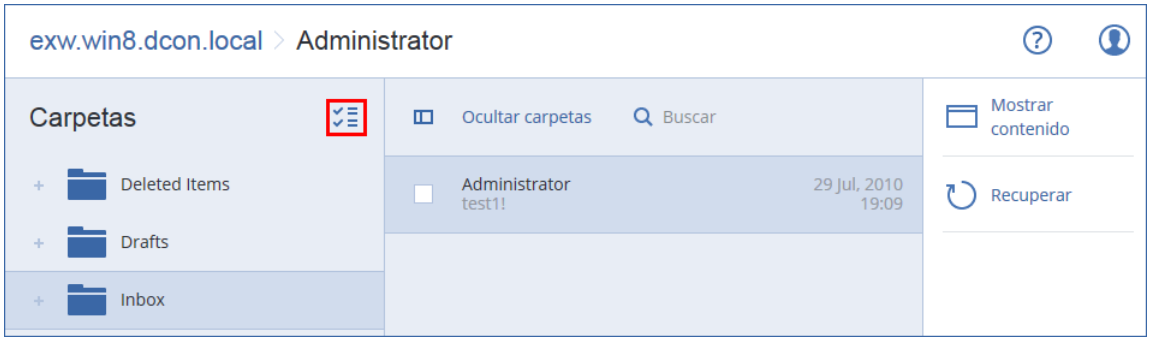
   Tiene a su disposición las siguientes opciones de búsqueda. No se pueden usar caracteres comodín.

   - 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. 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. 121).
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 o se selecciona un equipo de destino que no es el original, debe indicar el buzón de correo de destino.
11. Haga clic en **Iniciar recuperación**.
12. Confirme su decisión.

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

14.6.3 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.

15 Proteger 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?

Agente para Office 365

En función de la configuración elegida por el proveedor de servicios, es posible que necesite instalar Agente para Office 365 de manera local o utilizar el agente instalado en la nube.

Cuando se utiliza Agente para Office 365 instalado en la nube, se aplican las siguientes limitaciones:

- El único destino de copia de seguridad disponible es el almacenamiento en la nube.
- La copia de seguridad se realiza una vez al día. La programación de copia de seguridad no se puede cambiar. La copia de seguridad no se puede iniciar de forma manual.

Importante *Solo puede haber un Agente para Office 365 en una organización (grupo empresarial).*

Cuenta de administrador global.

Para realizar copias de seguridad y recuperar buzones de correo de Office 365, su cuenta debe tener la función de administrador global en Microsoft Office 365. 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.

¿Qué elementos de datos pueden recuperarse?

Los siguientes elementos pueden recuperarse de la copia de seguridad de buzones de correo:

- Buzones de correo

- Carpetas de correo electrónico
- Mensajes de correo electrónico
- Eventos del calendario
- Tareas
- Contactos
- Entradas del diario
- Notas

Puede usar la búsqueda para localizar los elementos.

Cuando se recupera un buzón de correo sobre un buzón de correo existente, los elementos anteriores que tengan los mismos ID se sobrescriben.

Al recuperar elementos de buzón de correo no se sobrescribe nada. Los elementos de buzón de correo siempre se recuperan en la carpeta **Elementos recuperados** del buzón de correo de destino.

Limitaciones

- No se puede realizar una copia de seguridad de los buzones de correo de archivo (**Archivo local**).
- No se admite la recuperación en un buzón de correo nuevo. 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 en una organización de Microsoft Office 365 diferente ni en Microsoft Exchange Server local.

15.1 Añadir buzones de correo de Office 365

Para añadir buzones de correo de Office 365

1. Haga clic en **Dispositivos** > **Añadir** > **Microsoft Office 365**.
2. Tiene lugar uno de los siguientes procesos:
   - El software empieza a implementar Agente para Office 365 en la nube.
   - El software le sugiere que instale Agente para Office 365. Descargue el agente e instálelo en un equipo que ejecute Windows y esté conectado a Internet.
3. Después de completar la instalación, haga clic en **Dispositivos** > **Microsoft Office 365**, y luego indique las credenciales del administrador global de Office 365.

Importante *Solo puede haber un Agente para Office 365 en una organización (grupo empresarial).*

15.2 Seleccionar buzones de correo de Office 365

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. 29).

Para seleccionar buzones de correo de Microsoft Office 365

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**.

15.3 Recuperación de buzones de correo y de elementos de buzón de correo de Office 365

15.3.1 Recuperación de buzones de correo

1. Haga clic en **Microsoft Office 365**.
2. Seleccione el buzón de correo que desea recuperar y, a continuación, haga clic en **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. 100) y, a continuación, haga clic en **Mostrar copias de seguridad**.
3. Seleccione un punto de recuperación. Tenga en cuenta que los puntos de recuperación se filtran por ubicación.
4. Haga clic en **Recuperar** > **Buzón de correo**.
5. En **Buzón de correo de destino** puede consultar, cambiar o especificar el buzón de correo de destino.

   De manera predeterminada se selecciona el buzón de correo original. Si este buzón de correo no existe, debe indicar el buzón de correo de destino.
6. Haga clic en **Iniciar recuperación**.

15.3.2 Recuperación de elementos de buzón de correo

1. Haga clic en **Microsoft Office 365**.
2. Seleccione el buzón de correo que contenía originalmente los elementos que desea recuperar y, a continuación, haga clic en **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. 100) 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. En **Buzón de correo de destino** puede consultar, cambiar o especificar el buzón de correo de destino.

   De manera predeterminada se selecciona el buzón de correo original. Si este buzón de correo no existe, debe indicar el buzón de correo de destino.
8. Haga clic en **Iniciar recuperación**.
9. Confirme su decisión.

Los elementos de buzón de correo siempre se recuperan en la carpeta **Elementos recuperados** del buzón de correo de destino.

15.4 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. Haga clic en **Especificar credenciales**.
3. 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.

16 Active Protection

Active Protection protege el sistema del software malicioso conocido como ransomware, el cual cifra los archivos y pide un rescate para obtener la clave de encriptación.

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.

Active Protection está disponible para los agentes que se inicien con la versión 12.0.4290. Para actualizar un agente, siga las instrucciones de "Actualización de agentes" (pág. 25).

Cómo funciona

Active Protection controla los procesos que se ejecutan en el equipo protegido. Si el proceso de un tercero intenta cifrar algún archivo, Active Protection genera una alerta y lleva a cabo otras acciones, si así se ha especificado en la configuración.

Además de proteger los archivos, 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 los registros de arranque maestro de los equipos protegidos.

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 Active Protection

Todas las opciones de configuración de Active Protection se incluyen en el plan Active Protection. Este plan puede aplicarse a varios equipos.

En una organización (grupo empresarial) solo puede haber un plan Active Protection. Solo los administradores de la compañía y los administradores de niveles superiores pueden aplicar, modificar o revocar el plan.

Aplicación del plan 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 los registros de arranque maestro de los dispositivos. No recomendamos deshabilitar esta función.

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**.

17 Protección de los sitios web

Un sitio web puede resultar dañado como resultado de un acceso no autorizado o un ataque de malware. Realice una copia de seguridad de su sitio web si desea revertirlo con facilidad a un estado saludable, en caso de que resulte dañado.

¿Qué necesito para realizar una copia de seguridad de un sitio web?

El sitio web tiene que ser accesible mediante el protocolo SFTP o SSH. No necesita instalar un agente, solo añada el sitio web como se ha descrito anteriormente en esta sección.

¿Qué elementos se pueden incluir en copias de seguridad?

Puede realizar copia de seguridad de los siguientes elementos:

- **Archivos de contenido del sitio web**

  Todos los archivos accesibles para la cuenta que especifique para la conexión SFTP o SSH.
- **Bases de datos enlazadas (si hay alguna) alojadas en servidores MySQL.**

  Todas las bases de datos accesibles para la cuenta MySQL que especifique.

Si su sitio web emplea bases de datos, le recomendamos que haga copias de seguridad de los archivos y las bases de datos, para poder recuperarlas a un estado consistente.

Limitaciones

- La única ubicación de copia de seguridad disponible para la copia de seguridad del sitio web es el almacenamiento en la nube.
- No se puede aplicar un plan de copias de seguridad a varios sitios web. Cada sitio web 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 sitio web.
- Las opciones de copia de seguridad no están disponibles.

17.1 Copia de seguridad de un sitio web

Para añadir un sitio web y configurar su copia de seguridad

1. Haga clic en **Dispositivos** > **Añadir**.
2. Haga clic en **Sitio web**.
3. Configure los siguientes parámetros de acceso para el sitio web:
   - En **Nombre del sitio web**, cree y escriba un nombre para su sitio web. Este nombre aparecerá en la consola de copia de seguridad.
   - En **Host**, especifique el nombre del host o la dirección IP que se usará para acceder al sitio web mediante SFTP o SSH. Por ejemplo, `my.server.com` o `10.250.100.100`.
   - En **Puerto**, especifique el número de puerto.

- En **Nombre de usuario** y **Contraseña**, especifique las credenciales de la cuenta que se puede utilizar para acceder al sitio web mediante SFTP o SSH.

  Importante *Solo se realizará copia de seguridad de los archivos que sean accesibles para la cuenta especificada.*

  En lugar de una contraseña, puede especificar su clave SSH privada. Para ello, seleccione la opción **Usar clave SSH privada en lugar de una contraseña** y luego especifique la clave.

4. Haga clic en **Siguiente**.
5. Si su sitio web utiliza bases de datos MySQL, configure los parámetros de acceso para las bases de datos. En caso contrario, haga clic en **Omitir**.
   a. En **Tipo de conexión**, seleccione cómo acceder a las bases de datos desde la nube:
      - **Mediante SSH desde el host**: Se accederá a las bases de datos mediante el host especificado en el paso 3.
      - **Conexión directa**: Se accederá a las bases de datos directamente. Seleccione esta configuración solo si se puede acceder a las bases de datos desde Internet.

   b. En **Host**, especifique el nombre o la dirección IP del host donde se está ejecutando el servidor MySQL.
   c. En **Puerto**, especifique el número de puerto para la conexión TCP/IP al servidor. El número del puerto predeterminado es 3306.
   d. En **Nombre de usuario** y **Contraseña**, especifique las credenciales de la cuenta de MySQL.

      Importante *Solo se realizará copia de seguridad de los archivos que sean accesibles para la cuenta especificada.*

   e. Haga clic en **Crear**.
6. El software muestra una nueva plantilla de plan de copias de seguridad. Modifique la configuración si fuera necesario y luego haga clic en **Aplicar**.

Para cambiar la configuración de la conexión

1. Seleccione el sitio web en **Dispositivos** > **Sitios web**.
2. Haga clic en **Generalidades**.
3. Haga clic en el icono de lápiz situado al lado del sitio web o en los parámetros de conexión de la base de datos.
4. Realice los cambios necesarios y luego haga clic en **Guardar**.

Para modificar el plan de copias de seguridad

1. Seleccione el sitio web en **Dispositivos** > **Sitios web**.
2. Haga clic en **Copia de seguridad**.
3. 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**.
4. Realice los cambios necesarios y luego haga clic en **Guardar cambios**.

17.2 Recuperar un sitio web

Para recuperar un sitio web

1. Seleccione el sitio web que desea recuperar en **Dispositivos** > **Sitios web**.

   Puede buscar los sitios web por el nombre. No se pueden usar caracteres comodín.
2. Haga clic en **Recuperación**.
3. Seleccione el punto de recuperación.

4. Haga clic en **Recuperar** y luego seleccione lo que desea recuperar: **Archivos/carpetas** o **bases de datos SQL** (si hay alguna).

   Para asegurarse de que su sitio web está en buen estado, le recomendamos que recupere los archivos y las bases de datos, no importa el orden.
5. Dependiendo de su elección en el paso anterior, siga uno de los procedimientos descritos a continuación:

Para recuperar los archivos/carpetas del sitio web

1. 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 acerca del uso de los caracteres comodín, consulte "Filtros de archivo" (pág. 50).
2. Seleccione los archivos que desea recuperar.
3. 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.
4. Haga clic en **Recuperar** y luego confirme la acción.

   Las carpetas y los archivos seleccionados se recuperarán en su ubicación original.

Para recuperar las base de datos

1. Seleccione las bases datos que desea recuperar.
2. Si desea guardar las bases de datos 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.
3. Haga clic en **Recuperar** y luego confirme la acción.

   Las bases de datos seleccionadas se recuperarán en la ubicación original.

18 Operaciones especiales con equipos virtuales

18.1 Ejecución de un equipo virtual desde una copia de seguridad (restauración instantánea)

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 o en una carpeta local del equipo en el que está instalado el Agente para VMware o el Agente para Hyper-V. Si selecciona una carpeta de red, debe ser accesible desde ese equipo. Un equipo virtual también se puede ejecutar desde una copia de seguridad almacenada en la cloud, pero el rendimiento será más lento porque la operación requiere una lectura intensa mediante accesos aleatorios de la copia de seguridad.
- La copia de seguridad debe contener un equipo completo o todos los volúmenes necesarios para que el sistema operativo se inicie.
- Pueden usarse las copias de seguridad tanto de los equipos físicos como de los virtuales. No pueden usarse las copias de seguridad de *contenedores* Virtuozzo.

18.1.1 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. 100).
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.

18.1.2 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.

18.1.3 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.

18.2 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. 135) 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. 134)

  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. 134)

  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.

18.2.1 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. 135).
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: 

18.2.2 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.

18.2.3 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. 135)

  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. 135)

  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. 135)

  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.

18.2.3.1 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.

18.2.3.2 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**.

18.2.3.3 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. 136).
7. Haga clic en **Iniciar recuperación**.
8. Confirme su decisión.

18.2.4 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. 48).

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. 49).

Comandos previos/posteriores

Esta opción se parece a la opción de copia de seguridad "Comandos previos/posteriores" (pág. 56).

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. 62).

18.2.5 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" (pág. 80).

Rendimiento

Esta opción se parece a la opción de recuperación "Rendimiento" (pág. 82).

Comandos pre/post

Esta opción se parece a la opción de recuperación "Comandos pre/post" (pág. 82).

Gestión de energía de VM

Esta opción se parece a la opción de recuperación "Gestión de energía de VM" (pág. 84).

18.3 Gestión de entornos de virtualización

Puede visualizar los entornos de vSphere, Hyper-V y Virtuozzo en su presentación nativa. Cuando el agente correspondiente esté instalado y registrado, aparecerá la pestaña **VMware**, **Hyper-V** o **Virtuozzo** en **Dispositivos**.

En la pestaña **VMware** se pueden modificar las credenciales de acceso a vCenter Server o al servidor ESXi independiente sin tener que reinstalar el agente.

Para modificar las credenciales de acceso a vCenter Server o al servidor ESXi

1. En **Dispositivos**, haga clic en **VMware**.
2. Haga clic en **Servidores y clústeres**.
3. En la lista de **Servidores y clústeres** (situada a la derecha del árbol de **Servidores y clústeres**), seleccione vCenter Server o el servidor ESXi independiente que se especificó durante la instalación del Agente para VMware.
4. Haga clic en **Generalidades**.
5. En **Credenciales**, haga clic en el nombre de usuario.
6. Especifique las nuevas credenciales de acceso y, a continuación, haga clic en **Aceptar**.

18.4 Migración de equipos

Puede realizar la migración de un equipo recuperando su copia de seguridad en un equipo no original.

La siguiente tabla resume las opciones de migración disponibles.

Tipo de equipo incluido en la copia de seguridad	**Destinos de recuperación disponibles**				
	Equipo físico	Equipo virtual ESXi	Equipo virtual Hyper-V	Equipo virtual Virtuozzo	Contenedor Virtuozzo
Equipo físico	+	+	+	-	-
Equipo virtual VMware ESXi	+	+	+	-	-
Equipo virtual Hyper-V	+	+	+	-	-
Equipo virtual Virtuozzo	+	+	+	+	-
Contenedor Virtuozzo	-	-	-	-	+

Para obtener instrucciones sobre cómo realizar la migración, consulte las siguientes secciones:

- Physical-to-virtual (P2V) - "Equipo físico a virtual" (pág. 66)
- Virtual-to-virtual (V2V) - "Equipo virtual" (pág. 67)
- Virtual-to-physical (V2P) - "Equipo virtual" (pág. 67) o "Recuperación de discos usando dispositivos de arranque" (pág. 69)

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.

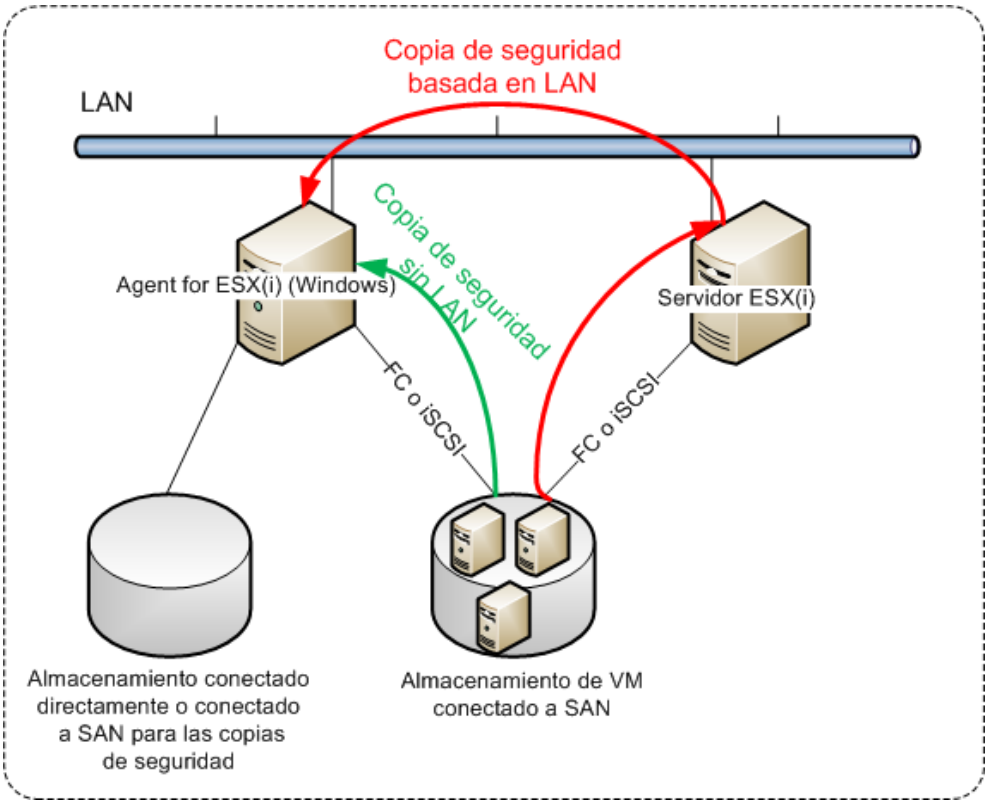
Los dispositivos le permiten hacer lo siguiente:

- Elegir discos o volúmenes independientes para la recuperación.
- Asignar de forma manual los discos de la copia de seguridad a los discos del equipo de destino.
- Volver a crear los volúmenes lógicos (LVM) o software RAID de Linux en el equipo de destino.
- Proporcionar los controladores del hardware específico que sea fundamental para la capacidad de arranque del sistema.

18.5 Agent para VMware: copia de seguridad sin LAN

Si su ESXi usa un almacenamiento conectado a SAN, instale el agente en un equipo conectado al mismo SAN. El agente realizará la copia de seguridad de los equipos virtuales directamente desde el almacenamiento en vez de mediante el servidor ESXi y LAN. Esta capacidad se llama copia de seguridad sin LAN.

El diagrama a continuación ilustra una copia de seguridad basada en LAN y sin LAN. El acceso sin LAN a los equipos virtuales está disponible si posee canal de fibra (FC) o red de área de almacenamiento iSCSI. Para eliminar completamente la transferencia de los datos incluidos en la copia de seguridad a través de la LAN, almacene las copias de seguridad en un disco local del equipo del agente o en un almacenamiento SAN conectado.



Para permitir que el agente acceda al almacén de datos directamente

1. Instale el Agente para VMware en un equipo que ejecute Windows y esté conectado a vCenter Server.
2. Conecte el número de unidad lógica (LUN) que aloja el almacén de datos en el equipo. Considere el siguiente escenario:
   - Use el mismo protocolo (iSCSI o FC) que se utiliza para la conexión del almacén de datos con el ESXi.
   - *No debe* iniciar el LUN y, además, debe mostrarse como disco "desconectado" en **Gestión del disco**. Si Windows inicia el LUN, este puede resultar dañado o ilegible en VMware vSphere.

Como resultado, el agente utilizará el modo de transporte SAN para acceder a los discos virtuales, es decir, leerá los sectores LUN sin procesar en iSCSI/FC sin reconocer el sistema de archivos VMFS, que Windows no detecta.

Limitaciones

- En vSphere 6.0 y versiones posteriores, el agente no puede utilizar el modo de transporte de SAN si algunos de los discos de equipo virtual están ubicados en un Volumen Virtual de VMware (VVol) y otros no. Las copias de seguridad de dichos equipos virtuales fallarán.
- Los equipos virtuales cifrados, presentados en VMware vSphere 6.5, se incluirán en la copia de seguridad mediante LAN, incluso si configura el modo de transporte SAN para el agente. El agente recurrirá al transporte NBD, pues VMware no es compatible con el transporte SAN para realizar copias de seguridad de discos virtuales cifrados.

Ejemplo

Si está utilizando un SAN de iSCSI, configure el iniciador de iSCSI en el equipo que ejecute Windows y en el que esté instalado Agente para VMware.

Para configurar la directiva SAN

1. Inicie sesión como administrador, ejecute 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

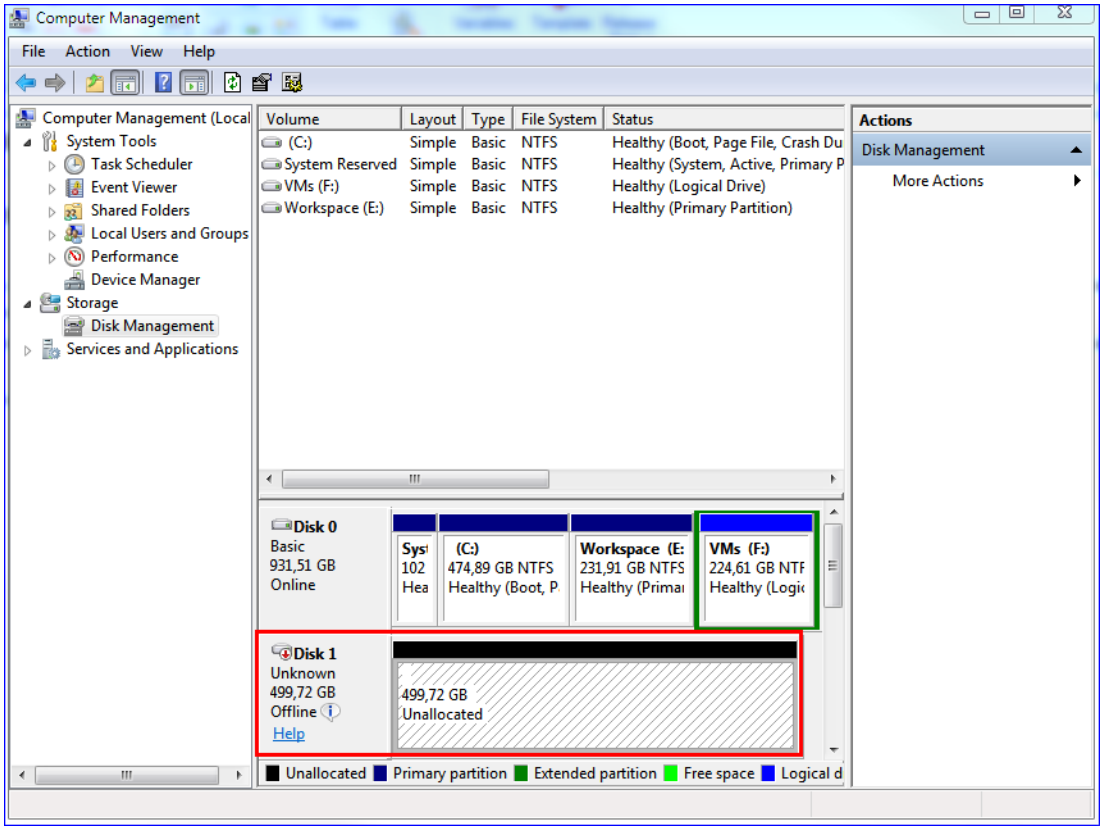
1. Vaya al **Panel de control** > **Herramientas administrativas** > **Iniciador de iSCSI**.

   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.



18.6 Agente para VMware: privilegios necesarios

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 en un momento posterior, consulte la sección "Gestionar entornos de virtualización" (pág. 136).

		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**
Operaciones criptográficas (primeros pasos con vSphere 6.5)	**Agregar disco**	+*			
	Acceso directo	+*			
Almacén de datos	**Asignar espacio**		+	+	+

		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**
	Examinar almacén de datos				+
	Configurar los almacenes de datos	+	+	+	+
	Operaciones con archivos de bajo nivel				+
Global	**Licencias**	+	+	+	+
	Deshabilitar métodos	+	+	+	
	Habilitar métodos	+	+	+	
Servidor > Configuración	**Configuración de partición de almacenamiento**				+
Servidor > Operaciones locales	**Crear VM**				+
	Eliminar VM				+
	Reconfigurar VM				+
Red	**Asignar red**		+	+	+
Recurso	**Asignar equipo virtual a pool de recursos**		+	+	+
Equipo virtual > Configuración	**Añadir disco existente**	+	+		+
	Añadir disco nuevo		+	+	+
	Añadir o quitar dispositivo		+		+
	Avanzado	+	+	+	
	Cambiar recuento de CPU		+		
	Seguimiento de cambios de disco	+		+	
	Disco arrendado	+		+	
	Memoria		+		
	Quitar disco	+	+	+	+
	Cambiar nombre		+		
	Establecer anotación				+

		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**
	Configuración		+	+	+
Equipo virtual >Operaciones de huésped	**Ejecución de programa de operación de huésped**	+**			
	Consultas de operación de huésped	+**			
	Modificaciones de operaciones de huésped	+**			
Equipo virtual > **Interacción**	**Adquirir vale de control de huésped** (en vSphere 4.1 y 5.0)				+
	Configurar dispositivo de CD		+	+	
	Gestión del sistema operativo huésped por VIX API (en vSphere 5.1 y versiones posteriores)				+
	Apagar			+	+
	Encender		+	+	+
Equipo virtual > **Inventario**	**Crear desde existente**		+	+	+
	Crear nuevo		+	+	+
	Registrar				+
	Quitar		+	+	+
	Anular el registro				+
Equipo virtual > **Aprovisionamiento**	**Permitir acceso a disco**		+	+	+
	Permitir acceso a disco de solo lectura	+		+	
	Permitir descarga de equipo virtual	+	+	+	+
Equipo virtual > **Estado**	**Crear instantánea**	+		+	+
	Eliminar instantánea	+		+	+

		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**
vApp	**Agregar equipo virtual**				+

* Este privilegio solo es obligatorio para realizar copias de seguridad de equipos cifrados.

** Este privilegio solo es obligatorio para copias de seguridad compatibles con aplicaciones.

18.7 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 con un equipo físico. No obstante, el equipo se cuenta como virtual al definir las cuotas del número de equipos.

La diferencia con respecto a un equipo físico es que 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 objeto de la copia de seguridad tal y como se ha descrito en "Equipo físico" (pág. 65). Al configurar la recuperación, seleccione el equipo nuevo como el equipo de destino.

18.8 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. 60) 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 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
```

19 Administración de cuentas de usuario y unidades de organización

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 haga clic en **Gestionar cuentas** en la esquina superior izquierda de la consola de copias de seguridad. 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.

Los proveedores de servicios gestionados también pueden especificar cuotas para las empresas de sus clientes de una forma similar.

Crear 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, buzones de correo o sitios web que un usuario puede proteger. Están disponibles las cuotas siguientes:

- **Almacenamiento en la cloud**
- **Estaciones de trabajo**
- **Servidores**
- **Equipos virtuales**
- **Dispositivos móviles**
- **Buzones de correo de Office 365**
- **Sitios web**
- **Copia de seguridad local**

Se considera que un equipo, un dispositivo, un buzón de correo o un sitio web 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 supera el uso por encima del límite para esta cuota o la cuota se establece en 0, no es posible crear servidores principales ni de recuperación, agregar discos a los servidores principales existentes, 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 supera el uso por encima del límite para esta cuota, todos los servidores principales y de recuperación se apagan. 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 establece en 0 o 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 supera 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 establece en 0 o 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 supera el uso por encima del límite para esta cuota o la cuota se establece en 0, no es posible 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:

- **Enviar notificaciones empresariales** (habilitado de forma predeterminada)

  Las notificaciones sobre cuotas superadas.

- **Error al realizar copia de seguridad**, **Copia de seguridad completada con advertencias** y **Copia de seguridad completada** (deshabilitado de forma predeterminada)

  Las notificaciones sobre los resultados de la copia de seguridad en 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 de uso

El informe sobre el uso del servicio de copia de seguridad incluye los datos siguientes sobre una empresa o 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.

20 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. Seleccione el equipo del que desea recopilar los registros.
2. Haga clic en **Actividades**.
3. Haga clic en **Recopilar información del sistema**.
4. Si se lo pide el navegador web, indique dónde quiere guardar el archivo.

21 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. 148). 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 y las incrementales subsiguientes se guardan en un único archivo .tib o .tibx, en lugar de en 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.