

Acronis



Acronis Backup 12 Update 3

MANUAL DEL USUARIO

Contenido

| | | |
|----------|---|-----------|
| 1 | Novedades en Acronis Backup | 6 |
| 1.1 | Novedades en la actualización 3 | 6 |
| 1.2 | Novedades en la actualización 2 | 6 |
| 1.3 | Novedades en Acronis Backup 12 | 6 |
| 2 | Instalación | 7 |
| 2.1 | Información general acerca de la instalación | 7 |
| 2.2 | Componentes | 9 |
| 2.3 | Requerimientos de software | 11 |
| 2.3.1 | Navegadores web compatibles | 11 |
| 2.3.2 | Sistemas operativos y entornos compatibles | 11 |
| 2.3.3 | Versiones compatibles de Microsoft SQL Server | 14 |
| 2.3.4 | Versiones compatibles de Microsoft Exchange Server | 14 |
| 2.3.5 | Versiones de Microsoft SharePoint compatibles | 14 |
| 2.3.6 | Plataformas de virtualización compatibles | 14 |
| 2.3.7 | Paquetes de Linux | 17 |
| 2.3.8 | Compatibilidad con software de cifrado | 19 |
| 2.4 | Requisitos del sistema | 20 |
| 2.5 | Sistemas de archivos compatibles | 21 |
| 2.6 | Implementación en una instalación | 22 |
| 2.6.1 | Instalación del servidor de gestión | 22 |
| 2.6.2 | Adición de equipos a través de la interfaz web | 24 |
| 2.6.3 | Instalación de agentes localmente | 28 |
| 2.6.4 | Gestión de licencias | 31 |
| 2.7 | Implementación en la nube | 32 |
| 2.7.1 | Preparación | 32 |
| 2.7.2 | Configuración del servidor proxy | 33 |
| 2.7.3 | Instalación de agentes | 34 |
| 2.7.4 | Activación de la cuenta | 35 |
| 2.8 | Implementación de agentes mediante la directiva de grupo | 36 |
| 2.9 | Actualización de agentes | 37 |
| 2.10 | Desinstalación del producto | 38 |
| 3 | Acceso a la consola de copia de seguridad | 39 |
| 4 | Vistas de la consola de copias de seguridad | 39 |
| 5 | Crear copia de seguridad | 40 |
| 5.1 | Apuntes del plan de copias de seguridad | 42 |
| 5.2 | Seleccionar los datos que se incluirán en la copia de seguridad | 43 |
| 5.2.1 | Seleccionar discos/volúmenes | 43 |
| 5.2.2 | Seleccionar archivos/carpetas | 44 |
| 5.2.3 | Seleccionar un estado del sistema | 46 |
| 5.2.4 | Selección de la configuración de ESXi | 47 |
| 5.3 | Seleccionar un destino | 47 |
| 5.3.1 | Acerca de Secure Zone | 48 |
| 5.4 | Planificación | 51 |

| | | |
|----------|--|-----------|
| 5.5 | Reglas de retención | 52 |
| 5.6 | Replicación..... | 52 |
| 5.7 | Cifrado..... | 53 |
| 5.8 | Iniciar una copia de seguridad manualmente | 55 |
| 5.9 | Opciones de copia de seguridad | 55 |
| 5.9.1 | Consolidación de la copia de seguridad | 57 |
| 5.9.2 | Validación de la copia de seguridad..... | 58 |
| 5.9.3 | Seguimiento de bloques modificados (CBT) | 58 |
| 5.9.4 | Tasa de compresión | 58 |
| 5.9.5 | Notificaciones por correo electrónico | 59 |
| 5.9.6 | Manejo de errores | 59 |
| 5.9.7 | Copias de seguridad incrementales/diferenciales rápidas | 60 |
| 5.9.8 | Filtros de archivo | 60 |
| 5.9.9 | Instantánea de la copia de seguridad a nivel de archivo..... | 62 |
| 5.9.10 | Seguridad de nivel de archivo | 62 |
| 5.9.11 | Truncamiento de registros | 63 |
| 5.9.12 | Toma de instantáneas de LVM..... | 63 |
| 5.9.13 | Puntos de montaje..... | 63 |
| 5.9.14 | Instantánea multivolumen | 64 |
| 5.9.15 | Rendimiento | 65 |
| 5.9.16 | Comandos pre/post | 66 |
| 5.9.17 | Comandos previos o posteriores a la captura de datos | 67 |
| 5.9.18 | Planificación..... | 69 |
| 5.9.19 | Copia de seguridad sector por sector | 70 |
| 5.9.20 | División..... | 70 |
| 5.9.21 | Manejo de fallos de la tarea | 70 |
| 5.9.22 | Volume Shadow Copy Service (VSS) | 71 |
| 5.9.23 | Volume Shadow Copy Service (VSS) para equipos virtuales..... | 72 |
| 5.9.24 | Copia de seguridad semanal | 72 |
| 5.9.25 | Registro de sucesos de Windows..... | 72 |
| 6 | Recuperación..... | 73 |
| 6.1 | Recuperación de apuntes | 73 |
| 6.2 | Creación de dispositivos de inicio..... | 73 |
| 6.3 | Recuperar un equipo | 74 |
| 6.3.1 | Equipo físico..... | 74 |
| 6.3.2 | De equipo físico a virtual | 75 |
| 6.3.3 | Equipo virtual..... | 77 |
| 6.3.4 | Recuperar discos usando dispositivos de arranque | 78 |
| 6.3.5 | Uso de Universal Restore..... | 79 |
| 6.4 | Recuperación de archivos..... | 82 |
| 6.4.1 | Recuperación de archivos usando la interfaz web | 82 |
| 6.4.2 | Descargar archivos del almacenamiento en la nube..... | 83 |
| 6.4.3 | Recuperación de archivos usando dispositivos de arranque..... | 84 |
| 6.4.4 | Extracción de archivos desde copias de seguridad locales | 85 |
| 6.5 | Recuperación del estado del sistema | 85 |
| 6.6 | Recuperación de la configuración de ESXi..... | 85 |
| 6.7 | Opciones de recuperación | 86 |
| 6.7.1 | Validación de la copia de seguridad..... | 88 |
| 6.7.2 | Fecha y hora de los archivos..... | 88 |
| 6.7.3 | Manejo de errores | 88 |
| 6.7.4 | Exclusiones de archivos | 89 |

| | | |
|-----------|--|------------|
| 6.7.5 | Seguridad de nivel de archivo | 89 |
| 6.7.6 | Flashback..... | 89 |
| 6.7.7 | Recuperación de ruta completa..... | 89 |
| 6.7.8 | Puntos de montaje..... | 90 |
| 6.7.9 | Rendimiento | 90 |
| 6.7.10 | Comandos pre/post | 90 |
| 6.7.11 | Cambios en el identificador de seguridad (SID)..... | 92 |
| 6.7.12 | Gestión de energía de VM..... | 92 |
| 6.7.13 | Registro de eventos de Windows | 92 |
| 7 | Operaciones con copias de seguridad | 93 |
| 7.1 | Pestaña Copias de seguridad | 93 |
| 7.2 | Montaje de volúmenes desde una copia de seguridad..... | 94 |
| 7.3 | Eliminación de copias de seguridad..... | 94 |
| 8 | Operaciones con los planes de copias de seguridad..... | 95 |
| 9 | Bootable Media Builder | 96 |
| 9.1 | Dispositivos de arranque basados en Linux..... | 96 |
| 9.1.1 | Parámetros de kernel..... | 98 |
| 9.1.2 | Configuraciones de red..... | 99 |
| 9.1.3 | Puerto de red..... | 100 |
| 9.1.4 | Controladores para Universal Restore | 100 |
| 9.2 | Dispositivos de arranque basados en WinPE..... | 101 |
| 9.2.1 | Preparación: WinPE 2.x y 3.x..... | 102 |
| 9.2.2 | Preparación: WinPE 4.0 y posterior | 102 |
| 9.2.3 | Incorporación del complemento de Acronis a WinPE..... | 103 |
| 10 | Protección de dispositivos móviles | 104 |
| 11 | Protección de las aplicaciones | 109 |
| 11.1 | Requisitos previos..... | 110 |
| 11.2 | Copia de seguridad de la base de datos | 111 |
| 11.2.1 | Seleccionar bases de datos de SQL | 111 |
| 11.2.2 | Seleccionar datos de Exchange Server | 112 |
| 11.3 | Copia de seguridad compatible con la aplicación..... | 113 |
| 11.3.1 | Derechos de usuario necesarios | 114 |
| 11.4 | Recuperación de bases de datos SQL | 114 |
| 11.4.1 | Recuperación de bases de datos del sistema..... | 116 |
| 11.4.2 | Adjuntar bases de datos de SQL Server..... | 116 |
| 11.5 | Recuperación de bases de datos de Exchange | 117 |
| 11.5.1 | Montaje de bases de datos de Exchange Server | 118 |
| 11.6 | Recuperación de elementos de buzón de correo y de buzones de correo de Exchange | 119 |
| 11.6.1 | Recuperación de buzones de correo | 120 |
| 11.6.2 | Recuperación de elementos de buzón de correo..... | 121 |
| 12 | Proteger los buzones de correo de Office 365 | 122 |
| 12.1 | Seleccionar buzones de correo de Office 365 | 123 |
| 12.2 | Recuperación de buzones de correo y de elementos de buzón de correo de Office 365..... | 123 |
| 12.2.1 | Recuperación de buzones de correo | 123 |
| 12.2.2 | Recuperación de elementos de buzón de correo..... | 124 |

| | |
|---|------------|
| 13 Operaciones avanzadas con equipos virtuales | 125 |
| 13.1 Ejecución de un equipo virtual desde una copia de seguridad (restauración instantánea).. | 125 |
| 13.1.1 Ejecución del equipo | 125 |
| 13.1.2 Eliminación del equipo..... | 126 |
| 13.1.3 Finalización del equipo..... | 127 |
| 13.2 Replicación de equipos virtuales | 127 |
| 13.2.1 Creación de un plan de replicación..... | 128 |
| 13.2.2 Realización de pruebas en una réplica | 129 |
| 13.2.3 Conmutación por error en una réplica | 130 |
| 13.2.4 Opciones de replicación..... | 131 |
| 13.2.5 Opciones de conmutación por recuperación..... | 132 |
| 13.2.6 Recopilación de una réplica inicial | 132 |
| 13.3 Gestión de entornos de virtualización..... | 133 |
| 13.4 Migración de equipos | 133 |
| 13.5 Agent para VMware: copia de seguridad sin LAN | 134 |
| 13.6 Agente para VMware: privilegios necesarios | 136 |
| 13.7 Equipos virtuales Windows Azure y Amazon EC2..... | 139 |
| 14 Configuración del servidor de gestión..... | 140 |
| 14.1 Servidor de correo electrónico | 140 |
| 14.2 Notificaciones por correo electrónico | 141 |
| 15 Gestión de grupos y cuentas..... | 142 |
| 15.1 Cuentas y grupos | 142 |
| 15.2 Creación de un grupo..... | 143 |
| 15.3 Creación de una cuenta | 143 |
| 15.4 Creación de un informe acerca del uso del servicio | 145 |
| 15.5 Limitación del acceso a la interfaz web | 146 |
| 16 Solución de problemas..... | 147 |
| 17 Glosario..... | 149 |

1 Novedades en Acronis Backup

1.1 Novedades en la actualización 3

- Copia de seguridad y recuperación de los buzones de correo de Office 365 (pág. 122)
- Capacidad de crear y eliminar Secure Zone en la interfaz web (pág. 48)
- Compatibilidad con vSphere 6.5, Red Hat Enterprise Virtualization 3.6 y 4.0, y Microsoft Hyper-V Server 2016 (pág. 14)
- Compatibilidad con Linux con las versiones de kernel 4.7-4.9
- Compatibilidad con Red Hat Enterprise Linux 7.3, Oracle Linux 7.3, CentOS 7.2 and 7.3 y Debian 8.4 y 8.5

1.2 Novedades en la actualización 2

- Compatibilidad con macOS Sierra 10.12

1.3 Novedades en Acronis Backup 12

- Interfaz web nueva y moderna (pág. 39)
- Management Server: una ubicación centralizada para gestionar todas sus copias de seguridad

Instalación

- Implementación local o en la cloud (pág. 7)
- Instalación remota de agentes (pág. 24)

Copia de seguridad de aplicación

- Copia de seguridad de bases de datos de Exchange (pág. 112)
- Copia de seguridad de bases de datos SQL (pág. 111)
- Copia de seguridad compatible con la aplicación de equipos físicos y virtuales (pág. 113)
- Recuperación granular de datos de Exchange (pág. 119)

Virtualización

- Copia de seguridad de equipos virtuales Hyper-V
- Ejecución de un equipo virtual desde una copia de seguridad (Instant Restore) (pág. 125)
- Replicación de equipos virtuales ESXi (pág. 127)
- Optimización WAN para replicación de equipos virtuales (recopilación de réplicas) (pág. 132) — solo en implementaciones en una instalación
- Recuperación de archivos en equipos virtuales ESXi (pág. 82)
- Reconstrucción completa de ESXi (pág. 47)
- Copia de seguridad basada en agentes de equipos virtuales alojados en Windows Azure y Amazon EC2 (pág. 139)
- Flashback: recuperación incremental de equipos virtuales (pág. 89)

Copia de seguridad

- normal de Mac
- Copia de seguridad de dispositivos móviles (pág. 104): solo en implementaciones en la cloud

- Gestión de grupos y cuentas (pág. 142): solo en implementaciones en la cloud
- Búsqueda de archivos y carpetas en una copia de seguridad (pág. 82)
- Filtros de archivo eficaces (pág. 60)

2 Instalación

2.1 Información general acerca de la instalación

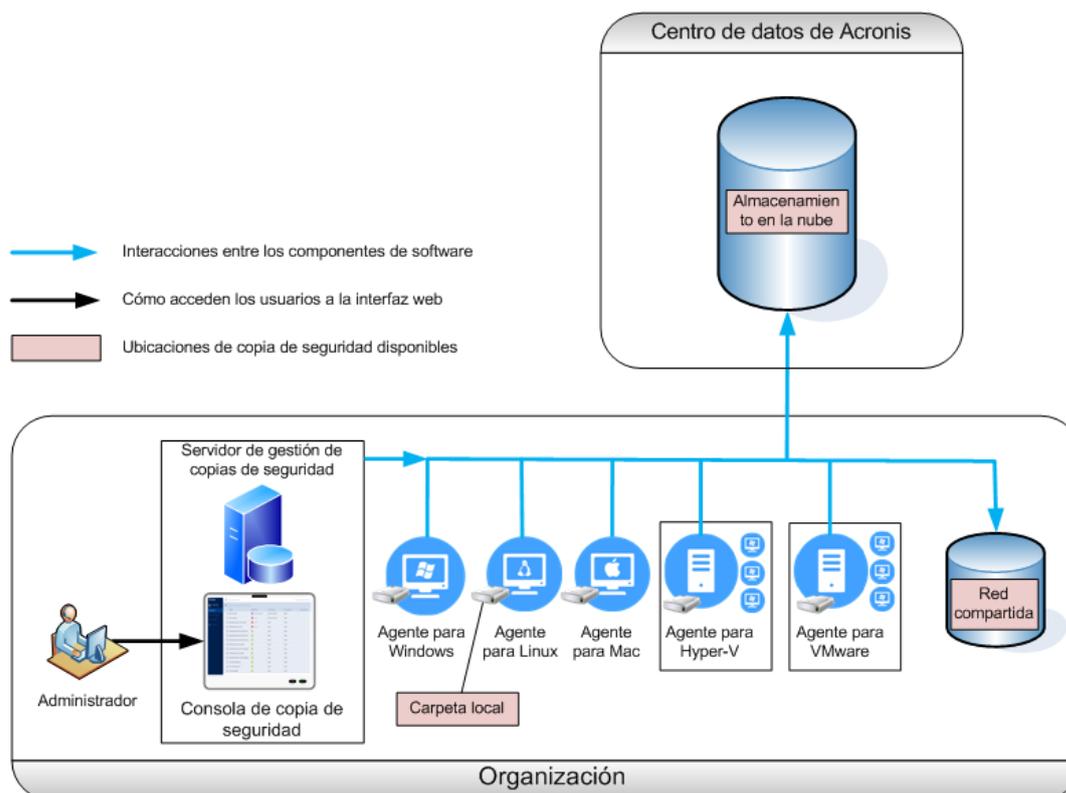
Acronis Backup admite dos métodos de implementación: en una instalación y en la nube. La diferencia principal entre ellos es la ubicación de Acronis Backup Management Server.

Acronis Backup Management Server es el punto central para administrar todas las copias de seguridad. Con la implementación en una instalación, se instala en la red local; con la implementación en la nube, se ubica en uno de los centros de datos de Acronis. La interfaz web a este servidor es lo que se llama una consola de copia de seguridad.

Ambos tipos de implementación requieren la instalación de un agente de copias de seguridad en cada equipo del que desee realizar una copia de seguridad. Los tipos compatibles de almacenamiento también son los mismos: carpetas locales, redes compartidas y Acronis Cloud Storage. El espacio de almacenamiento en la nube se vende aparte de las licencias de Acronis Backup.

Implementación en una instalación

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



Ubicación del servidor de gestión

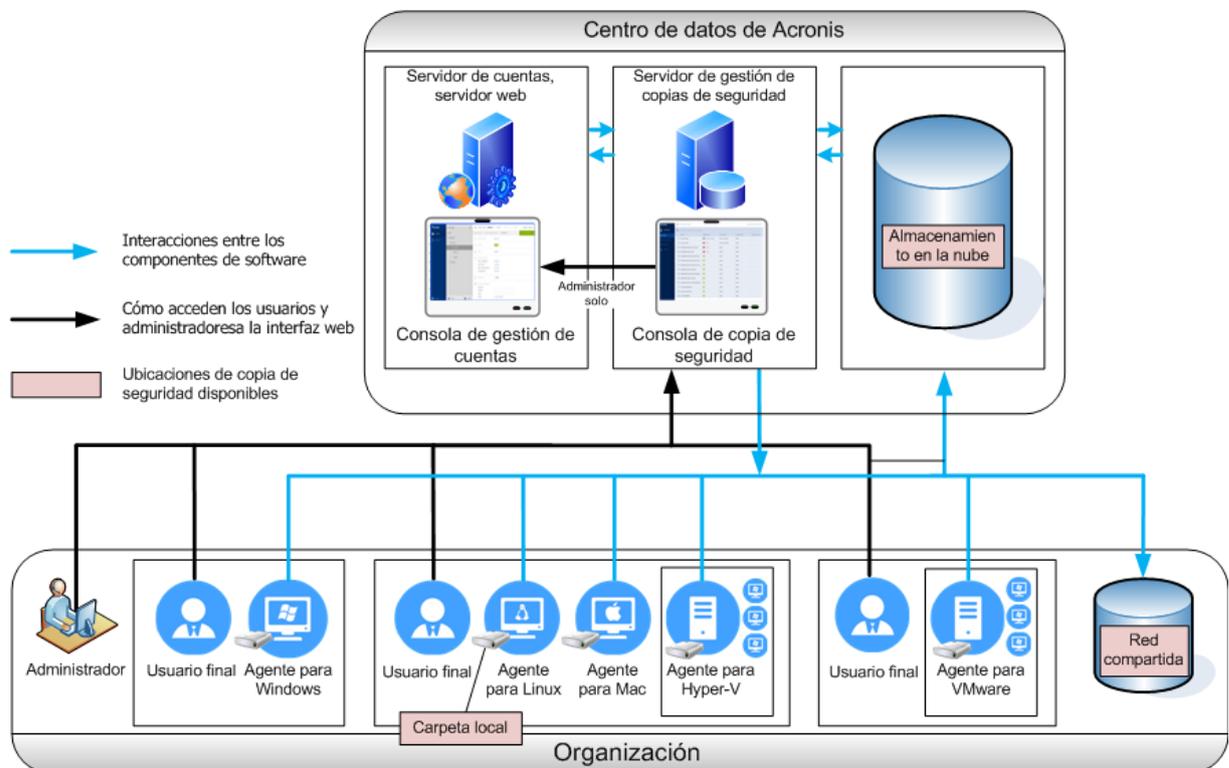
Puede instalar el servidor de gestión en un equipo que ejecute Windows o Linux. Se recomienda la instalación en Windows porque así podrá implementar los agentes en otros equipos desde el servidor de gestión. Se recomienda la instalación en Linux en un entorno exclusivo de Linux. Deberá instalar un agente localmente en los equipos de los que desee realizar copias de seguridad.

Implementación en la nube

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

El acceso al servidor de cuentas le permite crear cuentas de usuarios, establecer cuotas de uso de servicio para ellos y crear grupos de usuarios (unidades) para reflejar la estructura de la organización. Cada usuario podrá acceder a la consola de copia de seguridad, descargarse el agente requerido e instalarlo en sus equipos en cuestión de minutos.

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



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

| Implementación en una instalación | Implementación en la nube |
|--|---|
| <ul style="list-style-type: none"> ▪ Servidor de gestión en una instalación ▪ Se pueden utilizar tanto la licencia de suscripción como la licencia perpetua ▪ Agente para VMware (dispositivo virtual) y Agente para VMware (Windows) ▪ Optimización WAN para la replicación de equipos virtuales (recopilación de réplicas) ▪ Bootable Media Builder ▪ Gestión del disco y de copias de seguridad en dispositivos de arranque ▪ Actualizar desde versiones anteriores de Acronis Backup, incluyendo Acronis Backup para VMware ▪ Participación en el Programa de experiencia del cliente de Acronis | <ul style="list-style-type: none"> ▪ Gestión de grupos y cuentas ▪ Se necesita una licencia de suscripción ▪ Sin Agente para VMware (dispositivo virtual) ▪ Copia de seguridad de dispositivos móviles en la nube |

2.2 Componentes

Agentes

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

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

Tenga en cuenta que Agente para Windows se instala junto con Agent for Exchange, Agente para SQL 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? | Disponibilidad del agente | |
|---|-------------------------------|--|---------------------------|-------|
| | | | Local | Cloud |
| Equipos físicos | | | | |
| Discos, volúmenes y archivos en equipos físicos que ejecutan Windows. | Agente para Windows | En el equipo que se incluirá en la copia de seguridad. | + | + |
| Discos, volúmenes y archivos en equipos físicos que ejecutan Linux. | Agente para Linux | | + | + |
| Discos, volúmenes y archivos en equipos físicos que ejecutan OS X. | Agente para Mac | | + | + |
| Aplicaciones | | | | |

| ¿Qué se va a incluir en las copias de seguridad? | ¿Qué agente se debe instalar? | ¿Dónde se debe realizar la instalación? | Disponibilidad del agente | |
|---|---|--|---------------------------|-------|
| | | | Local | Cloud |
| 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. | + | + |
| Equipos que ejecutan Servicios de dominio de Active Directory | Agente para Active Directory | En el controlador de dominio. | + | + |
| Equipos virtuales | | | | |
| Equipos virtuales VMware ESXi | Agente para VMware (Windows) | En un equipo Windows con acceso de red a vCenter Server y al almacenamiento del equipo virtual.* | + | + |
| | Agente para VMware (dispositivo virtual) | En el servidor ESXi. | + | - |
| Equipos virtuales Hyper-V | Agente para Hyper-V | En el servidor Hyper-V. | + | + |
| Equipos virtuales alojados en Windows Azure. | Los mismo ocurre con los equipos físicos** | En el equipo que se incluirá en la copia de seguridad. | + | + |
| Equipos virtuales alojados en Amazon EC2 | | | + | + |
| Dispositivos móviles | | | | |
| Dispositivos móviles que ejecutan Android. | Aplicación para dispositivos móviles de Android | En el dispositivo móvil que se incluirá en la copia de seguridad. | - | + |
| Dispositivos móviles que ejecutan iOS | Aplicación para dispositivos móviles de iOS | | - | + |

*Si su ESXi usa un almacenamiento conectado a SAN, instale el agente en un equipo conectado al mismo SAN. El agente realizará la copia de seguridad de los equipos virtuales directamente desde el almacenamiento en vez de mediante el servidor ESXi y LAN. Para obtener más información, consulte "Agente para VMware: copia de seguridad sin LAN" (pág. 134).

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

Otros componentes

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

| Componente | Función | ¿Dónde se debe realizar la instalación? | Disponibilidad | |
|---------------------------------------|--|---|----------------|-------|
| | | | Local | Cloud |
| Servidor de gestión | Gestiona los agentes. Proporciona la interfaz web a los usuarios. | En un equipo que ejecuta Windows o Linux. | + | - |
| Bootable Media Builder | Crea dispositivos de arranque. | En un equipo que ejecuta Windows o Linux. | + | - |
| Monitorización de copias de seguridad | Permite a los usuarios monitorizar copias de seguridad fuera de la interfaz web. | En un equipo que ejecuta Windows o OS X. | + | + |
| Herramienta de línea de comandos | Proporciona la interfaz de línea de comandos. | En un equipo que ejecuta Windows o Linux. | + | + |

2.3 Requerimientos de software

2.3.1 Navegadores web compatibles

La interfaz web es compatible con los siguientes navegadores web:

- Google Chrome 29 o posterior
- Mozilla Firefox 23 o posterior
- Opera 16 o posterior
- Windows Internet Explorer 10 o posterior
- Safari 5.1.7 o 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.

2.3.2 Sistemas operativos y entornos compatibles

2.3.2.1 Agentes

Agente para Windows

Windows XP Professional SP3 (x86, x64)

Windows Server 2003/2003 R2: ediciones Standard y Enterprise (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 excepto las ediciones Windows RT (x86, x64)

Windows Server 2012/2012 R2: todas las ediciones

Windows Storage Server 2003/2008/2008 R2/2012/2012 R2

Windows 10: ediciones Home, Pro, Education y Enterprise

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

Agente para 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, excepto Windows RT (solo x64)

Windows Server 2012/2012 R2: todas las ediciones

Windows Storage Server 2008/2008 R2/2012/2012 R2 (solo x64)

Windows 10: ediciones Home, Pro, Education y Enterprise (solo x64)

Windows Server 2016: todas las opciones de instalación, excepto Nano Server (solo x64)

Agente para Linux

Linux con kernel de 2.6.9 a 4.9 y glibc 2.3.4 o posterior

Varias distribuciones Linux x86 y x86_64, incluidas:

Red Hat Enterprise Linux 4.x, 5.x, 6.x, 7.0, 7.1, 7.2 y 7.3

Ubuntu 9.10, 10.04, 10.10, 11.04, 11.10, 12.04, 12.10, 13.04, 13.10, 14.04, 14.10, 15.04, 15.10, 16.04

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

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

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

Oracle Linux 5.x, 6.x, 7.0, 7.1, 7.2 y 7.3: tanto Unbreakable Enterprise Kernel como Red Hat Compatible Kernel

CloudLinux 5.x, 6.x, 7 y 7.1

ClearOS 5.x, 6.x, 7, 7.1

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

Agente para Mac

OS X Mountain Lion 10.8

OS X Mavericks 10.9

OS X Yosemite 10.10

OS X El Capitan 10.11

macOS Sierra 10.12: no admite el sistema de archivos de Apple (APFS)

Agente para VMware (dispositivo virtual)

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

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

Agente para VMware (Windows)

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

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

Agente para Hyper-V

Windows Server 2008 (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: 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

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

En Windows

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

Windows Small Business Server 2008

Windows 7: todas las ediciones (x86, x64)

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

Windows MultiPoint Server 2010/2011/2012

Windows Small Business Server 2011: todas las ediciones

Windows 8/8.1: todas las ediciones excepto las ediciones Windows RT (x86, x64)

Windows Server 2012/2012 R2: todas las ediciones

Windows Storage Server 2008/2008 R2/2012/2012 R2

Windows 10: ediciones Home, Pro, Education y Enterprise

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

En Linux

Linux con kernel de 2.6.18 a 4.9 y glibc 2.3.4 o posterior

Varias distribuciones Linux x86_64, incluyendo:

Red Hat Enterprise Linux 4.x, 5.x, 6.x, 7.0, 7.1, 7.2 y 7.3

Ubuntu 9.10, 10.04, 10.10, 11.04, 11.10, 12.04, 12.10, 13.04, 13.10, 14.04, 14.10, 15.04, 15.10, 16.04

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

SUSE Linux Enterprise Server 10, 11 y 12

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

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

Oracle Linux 5.x, 6.x, 7.0, 7.1, 7.2 y 7.3: tanto Unbreakable Enterprise Kernel como Red Hat Compatible Kernel

CloudLinux 5.x, 6.x, 7 y 7.1

2.3.3 Versiones compatibles de Microsoft SQL Server

- Microsoft SQL Server 2016
- Microsoft SQL Server 2014
- Microsoft SQL Server 2012
- Microsoft SQL Server 2008 R2
- Microsoft SQL Server 2008
- Microsoft SQL Server 2005

2.3.4 Versiones 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.

2.3.5 Versiones de Microsoft SharePoint compatibles

Acronis Backup 12 es compatible con las siguientes versiones de Microsoft SharePoint:

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

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

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

2.3.6 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 | Copia de seguridad desde dentro de un SO huésped |
|------------|--|--|
| VMware | | |

| Plataforma | Copia de seguridad a nivel de hipervisor | Copia de seguridad desde dentro de un SO huésped |
|--|--|--|
| Versiónes de VMware vSphere: 4.1, 5.0, 5.1, 5.5, 6.0 y 6.5 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 | | + |
| Parallels | | |
| Parallels Workstation | | + |
| Parallels Server 4 Bare Metal | | + |
| 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. 53).
- 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.

2.3.7 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: <pre>yum install perl</pre> |
| CentOS Fedora | kernel-devel gcc make | El programa de instalación descargará e instalará los paquetes automáticamente. |
| | perl | Ejecute el siguiente comando: <pre>yum install perl</pre> |
| Ubuntu | linux-headers linux-image gcc make perl | Ejecute los siguientes comandos: <pre>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</pre> |

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

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

Instalación manual de los paquetes

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

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

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

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

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

- En Ubuntu, ejecute el siguiente comando:

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

Ejemplo: Instalación manual de los paquetes en Fedora 14

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

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

```
cat /proc/version
```

El resultado de este comando incluye lo siguiente:

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

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

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

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

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

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

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

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

2.3.8 Compatibilidad con software de cifrado

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

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

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

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

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

Regla común de instalación

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

Cómo utilizar Secure Zone

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

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

Regla común de copia de seguridad

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

Procedimientos de recuperación específicos del software

Microsoft BitLocker Drive Encryption

Para recuperar un sistema cifrado con BitLocker:

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

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

McAfee Endpoint Encryption y PGP Whole Disk Encryption

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

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

2.4 Requisitos del sistema

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

| Componentes que se deben instalar | Espacio de disco ocupado | Consumo de memoria mínimo |
|---|--------------------------|---------------------------|
| Agente para Windows | 850 MB | 150 MB |
| Agente para Windows y uno de los agentes siguientes: <ul style="list-style-type: none">▪ Agente para SQL▪ Agent for Exchange | 950 MB | 170 MB |
| Agente para Windows y uno de los agentes siguientes: <ul style="list-style-type: none">▪ Agente para VMware (Windows)▪ Agente para Hyper-V | 1170 MB | 180 MB |
| Agente para Office 365 | 500 MB | 170 MB |
| Agente para Linux | 720 MB | 130 MB |
| Agente para Mac | 500 MB | 150 MB |
| Solo para implementaciones en una instalación | | |
| Servidor de gestión en Windows | 1,7 GB | 200 MB |
| Servidor de gestión en Linux | 0,6 GB | 200 MB |
| Servidor de gestión y Agente para Windows | 2,4 GB | 360 MB |

| | | |
|--|---------|--------|
| Servidor de gestión y agentes en un equipo que ejecute Windows, Microsoft SQL Server, Microsoft Exchange Server y servicios de dominio de Active Directory | 3,35 GB | 400 MB |
| Servidor de gestión y Agente para Linux | 1,2 GB | 340 MB |

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

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

Un servidor de gestión con un equipo registrado consume 200 MB de memoria. Cada uno de los equipos recientemente registrados contribuye con unos 4 MB al consumo. Por tanto, un servidor con 100 equipos registrados consume aproximadamente 600 MB aparte del sistema operativo y las aplicaciones en funcionamiento. El número máximo de equipos registrado está entre 900 y 1000. Esta limitación procede del SQLite integrado del servidor de gestión.

2.5 Sistemas de archivos compatibles

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

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

| Sistema de archivos | Compatibilidad con | | | | Limitaciones |
|---------------------|--------------------|-----------------------------------|---|-----------------------------------|---|
| | Agentes | Dispositivo de arranque de Win-PE | Dispositivos de arranque basados en Linux | Dispositivos de arranque para Mac | |
| FAT16/32 | Todos los agentes | + | + | + | Sin limitaciones |
| NTFS | | + | + | + | |
| ext2/ext3/ext4 | | + | + | - | |
| HFS+ | Agente para Mac | - | - | + | |
| JFS | Agente para Linux | - | + | - | Los archivos no se pueden excluir de la copia de seguridad del disco. |
| ReiserFS3 | | - | + | - | |
| ReiserFS4 | | - | + | - | |
| ReFS | Todos los agentes | + | + | + | <ul style="list-style-type: none"> ■ Los archivos no se pueden excluir de la copia de seguridad del disco. |

| Sistema de archivos | Compatibilidad con | | | | Limitaciones |
|---------------------|--------------------|-----------------------------------|---|-----------------------------------|--|
| | Agentes | Dispositivo de arranque de Win-PE | Dispositivos de arranque basados en Linux | Dispositivos de arranque para Mac | |
| XFS | | + | + | + | <ul style="list-style-type: none"> No se puede cambiar el tamaño de los volúmenes durante la recuperación |
| Linux swap | Agente para Linux | - | + | - | Sin limitaciones |

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

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

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

2.6 Implementación en una instalación

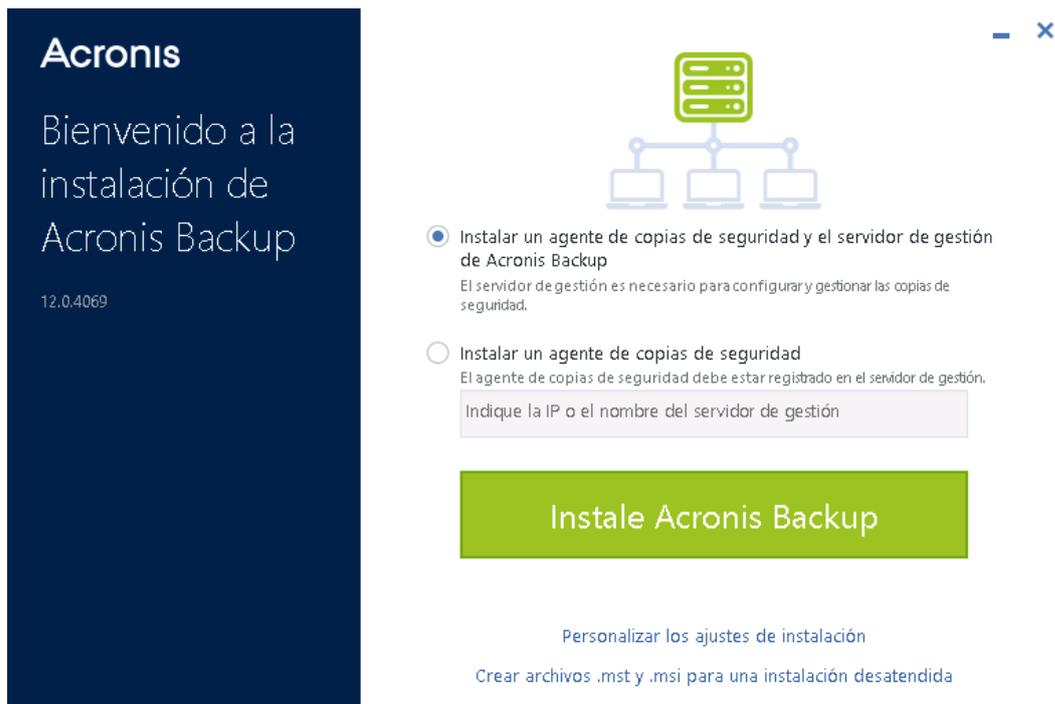
2.6.1 Instalación del servidor de gestión

2.6.1.1 Instalación en Windows

Para instalar el servidor de gestión

- Inicie sesión como administrador e inicie el programa de instalación de Acronis Backup.
- [Opcional] Para cambiar el idioma del programa de instalación, haga clic en **Idioma de instalación**.
- Acepte los términos del acuerdo de licencia y seleccione si el equipo participará en el Programa de experiencia del cliente (PEC) de Acronis.

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



De forma predeterminada, se instalarán los componentes siguientes:

- Servidor de gestión
- Agente para Windows
- Otros agentes (Agente para Hyper-V, Agent for Exchange, Agente para SQL y Agente para Active Directory), si se detecta el respectivo hipervisor o aplicación en el equipo
- Bootable Media Builder
- Herramienta de línea de comandos
- Monitorización de copias de seguridad

Puede establecer la configuración haciendo clic en **Personalizar la configuración de la instalación**.

- Continúe con la instalación.
- Cuando haya terminado la instalación, haga clic en **Cerrar**. La consola de copia de seguridad se abrirá en el navegador web predeterminado.

2.6.1.2 Instalación en Linux

Preparación

- Antes de instalar el producto en un sistema que no use el gestor de paquetes RPM, como un sistema Ubuntu, necesita instalar este gestor de forma manual; por ejemplo, ejecutando el siguiente comando (como usuario raíz): **apt-get install rpm**.
- Si desea instalar Agente para Linux junto con el servidor de gestión, asegúrese de que los paquetes de Linux (pág. 17) necesarios se han instalado en el equipo.

Instalación

Para instalar el servidor de gestión

- Ejecute el archivo de instalación como usuario raíz.
- Acepte los términos del acuerdo de licencia.

3. [Opcional] Seleccione los componentes que desea instalar.
De forma predeterminada, se instalarán los componentes siguientes:
 - Servidor de gestión
 - Agente para Linux
 - Bootable Media Builder
4. Especifique el puerto que utilizará un navegador web para acceder al servidor de gestión. El preajuste es 9877.
5. Especifique el puerto que utilizará para la comunicación entre los componentes del producto. El preajuste es 7780.
6. Haga clic en **Siguiente** para proceder con la instalación.
7. Cuando haya terminado la instalación, seleccione **Abrir consola web** y, después, haga clic en **Salir**. La consola de copia de seguridad se abrirá en el navegador web predeterminado.

2.6.2 Adición de equipos a través de la interfaz web

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

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

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

2.6.2.1 Adición de un equipo que ejecute Windows

Preparación

1. Para que la instalación se realice correctamente en un equipo remoto que ejecuta Windows XP, la opción **Panel de control > Opciones de carpeta > Ver > Utilizar uso compartido simple de archivos** se debe *desactivar* en ese equipo.
Para que la instalación se realice correctamente en un equipo remoto que ejecuta Windows Vista o posterior, la opción **Panel de control > Opciones de carpeta > Ver > Uso del asistente para compartir** se debe *desactivar* en ese equipo.
2. Para una instalación correcta en un equipo remoto que *no* sea miembro de un dominio de Active Directory, el control de cuentas de usuario (UAC) debe estar *deshabilitado* (pág. 25).
3. El uso compartido de archivos e impresoras deben estar *habilitado* en el equipo remoto. Para acceder a esta opción:
 - En un equipo con Windows XP con Service Pack 2 o Windows 2003 Server: vaya a **Panel de control > Cortafuegos de Windows > Excepciones > Uso compartido de archivos e impresoras**.
 - En un equipo con Windows Vista, Windows Server 2008, Windows 7 o posterior: vaya a **Panel de control > Cortafuegos de Windows > Centro de redes y uso compartido > Cambiar las configuraciones avanzadas de uso compartido**.
4. Acronis Backup utiliza los puertos TCP 445 y 25001 para la instalación remota. Además, usa el puerto TCP 9876 para la instalación remota y la comunicación entre los componentes.
El puerto 445 se abre automáticamente cuando habilita Compartir archivos e impresoras. Los puertos 9876 y 25001 se abren automáticamente por medio del cortafuegos de Windows. Si usa

un cortafuegos diferente, asegúrese de que estos tres puertos estén abiertos (añadidos a excepciones) para las solicitudes entrantes y salientes.

Una vez que la instalación remota se haya completado, puede quitar los puertos 445 y 25001 de las excepciones. El puerto 25001 se cierra automáticamente por medio del cortafuegos de Windows. El puerto 9876 debe permanecer abierto.

Adición del equipo

1. Haga clic en **Todos los dispositivos > Añadir**.
2. Haga clic en **Windows** o en el botón que se corresponda con la aplicación que desea proteger. Dependiendo del botón en el que haga clic, se seleccionará una de las opciones siguientes:
 - Agente para Windows
 - Agente para Hyper-V
 - Agente para SQL + Agente para Windows
 - Agent for Exchange + Agente para Windows
 - Agente para Active Directory + Agente para Windows
 - Agente para Office 365
3. Especifique el nombre del servidor o la dirección IP del equipo, y las credenciales de una cuenta con privilegios de administración en ese equipo.
4. Haga clic en **Añadir**.

Requisitos del control de cuentas de usuario (UAC)

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

Para deshabilitar UAC

Realice una de las siguientes acciones según el sistema operativo:

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

2.6.2.2 Adición de un equipo que ejecute Linux

1. Haga clic en **Todos los dispositivos > Añadir**.
2. Haga clic en **Linux**. Se descargará el archivo de instalación.
3. En el equipo que desea proteger, ejecute el programa de instalación localmente (pág. 29).

2.6.2.3 Adición de un equipo que ejecute OS X

1. Haga clic en **Todos los dispositivos > Añadir**.

2. Haga clic en **Mac**. Se descargará el archivo de instalación.
3. En el equipo que desea proteger, ejecute el programa de instalación localmente (pág. 29).

2.6.2.4 Adición de un servidor vCenter o ESXi

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

- **Implementación de Agente para VMware (dispositivo virtual) (pág. 26)**
Este es el método recomendado en la mayoría de los casos. El dispositivo virtual se implementará automáticamente en cada servidor gestionado por el vCenter que indique. Puede seleccionar los servidores y personalizar la configuración del dispositivo virtual.
- **Instalación de Agente para VMware (Windows) (pág. 27)**
Puede que quiera instalar Agente para VMware en un equipo físico que ejecute Windows para obtener una copia de seguridad sin LAN o descargada. El agente se implementará automáticamente en el equipo que indique.
 - **Copia de seguridad descargada**
Utilice esta opción si sus servidores ESXi de producción están tan cargados que no sería deseable ejecutar dispositivos virtuales.
 - **Copia de seguridad sin LAN**
Si su ESXi usa un almacenamiento conectado a SAN, instale el agente en un equipo conectado al mismo SAN. El agente realizará la copia de seguridad de los equipos virtuales directamente desde el almacenamiento en vez de mediante el servidor ESXi y LAN. Para obtener más información, consulte "Agente para VMware: copia de seguridad sin LAN" (pág. 134).
- **Registro de un Agente para VMware ya instalado (pág. 27)**
Utilice este método si instaló Agente para VMware (Windows) de forma manual, implementó Agente para VMware (dispositivo virtual) desde una plantilla de OVF (pág. 29) o tuvo que volver a instalar el servidor de gestión.

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

1. Haga clic en **Todos los dispositivos > Añadir**.
2. Haga clic en **VMware ESXi**.
3. Seleccione **Implementar como dispositivo virtual en cada servidor de un vCenter**.
4. Especifique la dirección y las credenciales de acceso de vCenter Server o del servidor ESXi independiente. Le recomendamos utilizar una cuenta que tenga asignado el rol de **Administrador**. En otro caso, proporcione una cuenta con los privilegios necesarios (pág. 136) en el servidor vCenter Server o ESXi.
5. [Opcional] Haga clic en **Configuración** para personalizar la configuración de la implementación:
 - Los servidores ESXi en los que desea implementar el agente (solo si se indicó un vCenter Server en el paso anterior).
 - El nombre del dispositivo virtual.
 - El almacén de datos donde se ubicará el dispositivo.
 - El grupo de recursos o vApp que contendrá el dispositivo.
 - La red a la que se conectará el adaptador de red del dispositivo virtual.
 - Configuración de red del dispositivo virtual. Puede elegir la configuración automática de DHCP o especificar los valores de forma manual incluyendo una dirección IP estática.

6. Haga clic en **Implementar**.

Instalación de Agente para VMware (Windows)

Preparación

Siga los pasos preparatorios descritos en la sección "Adición de un equipo que ejecute Windows" (pág. 24).

Instalación

1. Haga clic en **Todos los dispositivos > Añadir**.
2. Haga clic en **VMware ESXi**.
3. Seleccione **Instalar de forma remota en un equipo que ejecute Windows**.
4. Especifique el nombre del servidor o la dirección IP del equipo, y las credenciales de una cuenta con privilegios de administración en ese equipo. Haga clic en **Conectar**.
5. Especifique la dirección y las credenciales de vCenter Server o del servidor ESXi independiente y, a continuación, haga clic en **Conectar**. Le recomendamos utilizar una cuenta que tenga asignado el rol de **Administrador**. En otro caso, proporcione una cuenta con los privilegios necesarios (pág. 136) en el servidor vCenter Server o ESXi.
6. Haga clic en **Instalar** para instalar el agente.

Registro de un Agente para VMware ya instalado

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

Métodos de registro alternativos:

- Puede registrar Agente para VMware (dispositivo virtual) especificando el servidor de gestión en la interfaz de usuario del dispositivo virtual. Consulte el paso 3 en "Configuración del dispositivo virtual" en la sección "Implementación del Agente para VMware (dispositivo virtual) desde una plantilla de OVF" (pág. 29).
- Agente para VMware (Windows) se registra durante su instalación local (pág. 28).

Para registrar Agente para VMware

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

Si registra *Agente para VMware (dispositivo virtual)*, especifique el nombre del servidor o la dirección IP del dispositivo virtual y las credenciales de vCenter Server o del servidor ESXi independiente donde se ejecuta el dispositivo .

Haga clic en **Conectar**.
5. Especifique el nombre del servidor o la dirección IP de vCenter Server o del servidor ESXi independiente y las credenciales para acceder a él y luego haga clic en **Conectar**. Le recomendamos utilizar una cuenta que tenga asignado el rol de **Administrador**. En otro caso, proporcione una cuenta con los privilegios necesarios (pág. 136) en el servidor vCenter Server o ESXi.
6. Haga clic en **Registrar** para registrar el agente.

2.6.3 Instalación de agentes localmente

2.6.3.1 Instalación en Windows

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

1. Inicie sesión como administrador e inicie el programa de instalación de Acronis Backup.
2. [Opcional] Para cambiar el idioma del programa de instalación, haga clic en **Idioma de instalación**.
3. Acepte los términos del acuerdo de licencia y seleccione si el equipo participará en el Programa de experiencia del cliente (PEC) de Acronis.
4. Seleccione **Instalar un agente de copia de seguridad** y, a continuación, especifique el nombre del servidor o la dirección IP del equipo donde se ha instalado el servidor de gestión.

De forma predeterminada, se instalarán los componentes siguientes:

- Agente para Windows
- Otros agentes (Agente para Hyper-V, Agent for Exchange, Agente para SQL y Agente para Active Directory), si se detecta el respectivo hipervisor o aplicación en el equipo
- Bootable Media Builder
- Herramienta de línea de comandos
- Monitorización de copias de seguridad

Puede establecer la configuración haciendo clic en **Personalizar la configuración de la instalación**.

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

Para instalar Agente para VMware (Windows) o Agente para Office 365

1. Inicie sesión como administrador e inicie el programa de instalación de Acronis Backup.
2. [Opcional] Para cambiar el idioma del programa de instalación, haga clic en **Idioma de instalación**.
3. Acepte los términos del acuerdo de licencia y seleccione si el equipo participará en el Programa de experiencia del cliente (PEC) de Acronis.
4. Haga clic en **Personalizar configuración de la instalación**.
5. Junto a **Qué instalar**, haga clic en **Cambiar**.
6. Seleccione la casilla de verificación **Agente para VMware (Windows) o Agente para Office 365**. Si no desea instalar otros componentes en este equipo, desmarque las casillas de verificación que corresponda. Haga clic en **Realizado** para continuar.
7. Junto a **Acronis Backup Management Server**, haga clic en **Cambiar** y, a continuación, especifique el nombre del servidor o la dirección IP del equipo donde se ha instalado el servidor de gestión. Haga clic en **Realizado** para continuar.
8. [Opcional] Cambiar otras configuraciones de la instalación.
9. Haga clic en **Instalar** para proceder con la instalación.
10. Cuando haya terminado la instalación, haga clic en **Cerrar**.
11. [Solo al instalar el Agente para VMware (Windows)] Siga el procedimiento descrito en la sección "Registro de un Agente para VMware ya instalado" (pág. 27).

2.6.3.2 Instalación en Linux

Preparación

1. Antes de instalar el producto en un sistema que no use el gestor de paquetes RPM, como un sistema Ubuntu, necesita instalar este gestor de forma manual; por ejemplo, ejecutando el siguiente comando (como usuario raíz): **apt-get install rpm**.
2. Asegúrese de que los paquetes de Linux (pág. 17) necesarios se han instalado en el equipo.

Instalación

Para instalar Agente para Linux

1. Como usuario raíz, ejecute el archivo de instalación apropiado (un archivo .i686 o un archivo .x86_64).
2. Acepte los términos del acuerdo de licencia.
3. Desmarque la casilla de verificación **Acronis Backup Management Server** y, a continuación, haga clic en **Siguiente**.
4. Especifique el nombre del servidor o la dirección IP del equipo donde está instalado el servidor de gestión.
5. Haga clic en **Siguiente** para proceder con la instalación.
6. Cuando haya terminado la instalación, haga clic en **Salir**.

Encontrará información sobre la solución de problemas en el siguiente archivo:

/usr/lib/Acronis/BackupAndRecovery/HOWTO.INSTALL

2.6.3.3 Instalación en OS X

Para instalar Agente para Mac

1. Haga doble clic en el archivo de instalación (.dmg).
2. Espere mientras el sistema operativo monta la imagen del disco de instalación.
3. Haga doble clic en **Instalar**.
4. Siga las instrucciones que aparecen en pantalla.

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

Cuando se haya instalado el servidor de gestión, el paquete OVF del dispositivo virtual estará en la carpeta **%ProgramFiles%\Acronis\ESXApliance** (en Windows) o **/usr/lib/Acronis/ESXApliance** (en Linux).

La carpeta contiene un archivo .ovf y dos archivos .vmdk. Asegúrese de que se puede acceder a estos archivos desde el equipo que ejecuta el vSphere Client.

Implementación de la plantilla de OVF

1. Abra vSphere Client e inicie sesión en vCenter Server.
2. En el menú **Archivo**, haga clic en **Implementar la plantilla de OVF**.
3. En **Fuente**, especifique la ruta hacia el paquete OVF del dispositivo virtual.
4. Revise los **Detalles de la plantilla de OVF** y haga clic en **Siguiente**.
5. En **Nombre y ubicación**, introduzca el nombre del dispositivo o deje el nombre predeterminado de **AcronisESXApliance**.
6. En **Servidor/clúster**, seleccione el servidor ESXi en el que se implementará el dispositivo.

7. [Opcional] En **Pool de recursos**, seleccione el grupo de recursos que contendrá el dispositivo.
8. En **Almacenamiento**, deje el almacén de datos predeterminado a menos que no tenga suficiente espacio para el dispositivo virtual. En este caso, seleccione otro almacén de datos. Omita este paso si solo existe un almacén de datos en el servidor.
9. En **Formato de disco**, seleccione cualquier valor que pueda ser necesario. El formato de disco no afecta al rendimiento del dispositivo.
10. En **Asignación de red**, seleccione el modo de puenteo para el adaptador de red.
11. Revise el resumen y haga clic en **Finalizar**. Después de que la implementación se haya realizado correctamente, cierre la ventana de progreso.

Configuración del dispositivo virtual

1. Inicio del dispositivo virtual

En vSphere Client, muestre el **Inventario**, haga clic con el botón derecho sobre el nombre del dispositivo virtual y, a continuación, seleccione **Activar > Encender**. Seleccione la pestaña **Consola**. En la pantalla de inicio de sesión, haga clic en **Cerrar**.

2. vCenter/ESX(i)

En **Opciones del agente**, en **vCenter/ESX(i)**, haga clic en **Cambiar** y especifique el nombre o la dirección IP de vCenter Server. El agente podrá realizar la copia de seguridad y recuperar cualquier equipo virtual gestionado por vCenter Server.

Si no utiliza un vCenter Server, especifique el nombre o la dirección IP del servidor ESXi cuyos equipos virtuales desea incluir en la copia de seguridad y recuperar. Normalmente, las copias de seguridad se ejecutan más rápido cuando el agente realiza las copias de seguridad de equipos virtuales alojados en su propio servidor.

Especifique las credenciales que el agente utilizará para conectarse a vCenter Server o ESXi. Le recomendamos utilizar una cuenta que tenga asignado el rol de **Administrador**. En otro caso, proporcione una cuenta con los privilegios necesarios (pág. 136) en el servidor vCenter Server o ESXi.

Puede hacer clic en **Verificar la conexión** para asegurarse de que las credenciales de acceso son las correctas.

3. Acronis Backup Management Server

En **Opciones del agente**, en **Acronis Backup Management Server**, haga clic en **Cambiar**.

Especifique el nombre del servidor o la dirección IP del equipo donde se instalará el servidor de gestión y las credenciales de acceso de ese equipo.

4. Zona horaria

En **Equipo virtual**, en **Zona horaria**, haga clic en **Cambiar**. Seleccione la zona horaria de su ubicación para asegurar que las operaciones planificadas se ejecutan en el momento apropiado.

El dispositivo virtual está listo para funcionar. Además, puede cambiar las siguientes configuraciones:

■ Configuraciones de red

La conexión de red del agente se configura automáticamente con el Protocolo de configuración de host (DHCP). Para cambiar la configuración predeterminada, en **Opciones del agente**, **eth0**, haga clic en **Cambiar** y especifique las configuraciones de red deseadas.

■ Almacenamientos locales

Puede conectar un disco adicional al dispositivo virtual para que Agente para VMware pueda realizar la copia de seguridad en este almacenamiento conectado localmente. Esta clase de copia de seguridad normalmente es más rápida que una copia de seguridad a través de LAN y no consume el ancho de banda de red.

El tamaño de la unidad de disco virtual debe ser de al menos de 10 GB. Añada el disco al editar los ajustes del equipo virtual y haga clic en **Actualizar**. El enlace **Crear almacenamiento** está ahora disponible. Haga clic en este enlace, seleccione el disco y, a continuación, especifique una etiqueta para este.

Tenga cuidado al añadir un disco ya existente. Una vez creado el almacenamiento, todos los datos incluidos previamente en este disco se perderán.

2.6.4 Gestión de licencias

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

Para comenzar a utilizar Acronis Backup, deberá añadir al menos una clave de licencia al servidor de gestión. Se asigna automáticamente una licencia a un equipo cuando se aplica un plan de copias de seguridad. También puede asignar y revocar licencias de forma manual.

Para añadir una clave de licencia

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

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

Gestión de licencias perpetuas

Para asignar una licencia perpetua a un equipo

1. Haga clic en **Configuración > Licencias**.
2. Seleccione una licencia perpetua.
El software muestra las claves de licencia que corresponden a la licencia seleccionada.
3. Seleccione la clave que se debe asignar.
4. Haga clic en **Asignar**.
El software muestra los equipos a los que se puede asignar la clave seleccionada.
5. Seleccione el equipo y después haga clic en **Realizado**.

Para revocar una licencia perpetua de un equipo

1. Haga clic en **Configuración > Licencias**.
2. Seleccione una licencia perpetua.
El software muestra las claves de licencia que corresponden a la licencia seleccionada. El equipo al que está asignada la clave se muestra en la columna **Asignada a**.
3. Seleccione la clave de licencia que se debe revocar.
4. Haga clic en **Revocar**.

5. Confirme su decisión.

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

Gestión de licencias de suscripción

Para asignar una licencia de suscripción a un equipo

1. Haga clic en **Configuración > Licencias**.
2. Seleccione una licencia de suscripción.
El software muestra los equipos a los que la licencia seleccionada ya está asignada.
3. Haga clic en **Asignar**.
El software muestra los equipos a los que la licencia seleccionada se puede asignar.
4. Seleccione el equipo y después haga clic en **Realizado**.

Para revocar una licencia de suscripción de un equipo

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

2.7 Implementación en la nube

2.7.1 Preparación

Paso 1

Elija el Agente teniendo en cuenta los elementos que va a incluir en la copia de seguridad. Para obtener más información acerca de los agentes, consulte la sección "Componentes" (pág. 9).

Paso 2

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

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

Si desea almacenar los programas de instalación localmente, descargue un paquete que contenga todos los agentes para la instalación en Windows por medio del enlace que hay en la parte inferior de la página **Añadir dispositivos**. Están disponibles los paquetes de 32 bits y 64 bits. Con estos paquetes se puede personalizar la lista de componentes que se instalarán. Estos paquetes también permiten la instalación de interacción, por ejemplo, a través de la directiva de grupo. Este escenario avanzado se describe en "Implementación de agentes a través de la directiva de grupo" (pág. 36).

La instalación en Linux y OS X se realiza desde los programas de instalación habituales.

Todos los programas de instalación precisan conexión a Internet para registrar el equipo en el servicio de copias de seguridad. Si no hay conexión a Internet, la instalación fallará.

Paso 3

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

- **443 y 8443** Se usan estos puertos para acceder a la consola de copia de seguridad, registrar los agentes, descargar los certificados, obtener la autorización del usuario y descargar archivos desde el almacenamiento en la nube.
- **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. 33) para saber si debe configurar estos valores en cada equipo que ejecute un agente de copia de seguridad.

2.7.2 Configuración del servidor proxy

Los agentes de copia de seguridad pueden transferir datos a través de un servidor proxy HTTP.

Para la instalación del agente es necesario tener conexión a Internet. 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. En Linux y OS X, debe especificar la configuración de proxy antes de la instalación.

Puede usar los siguientes procedimientos para especificar la configuración del proxy antes de la instalación del agente o para cambiarla más adelante.

En Linux

1. Cree el archivo **/etc/Acronis/Global.config** y ábralo con un editor de texto.
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. En caso contrario, reinicie el agente ejecutando el siguiente comando en cualquier directorio:

```
sudo service acronis_mms restart
```

En OS X

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
```

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
```

2.7.3 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. Haga clic en **Instalar**.
4. Especifique las credenciales de la cuenta a la que se debe asignar el equipo.

5. Haga clic en **Mostrar la configuración del proxy** si desea comprobar o modificar el nombre de servidor, la dirección IP y el puerto del servidor proxy. De lo contrario, omita este paso. Si hay un servidor proxy habilitado en Windows, se detectará y usará automáticamente.
6. [Solo al instalar el Agente para VMware] Especifique la dirección y las credenciales de acceso del servidor vCenter Server o ESXi independiente de cuyos equipos virtuales el agente realizará la copia de seguridad. Le recomendamos utilizar una cuenta que tenga asignado el rol de **Administrador**. En otro caso, proporcione una cuenta con los privilegios necesarios (pág. 136) en el servidor vCenter Server o ESXi.
7. [Solamente cuando instale en un controlador de dominio] Especifique la cuenta de usuario en la que se ejecutará el servicio de Agente. Por razones de seguridad, el programa de instalación no crea automáticamente nuevas cuentas en un controlador de dominio.
8. Haga clic en **Iniciar instalación**.

Puede cambiar la ruta de instalación y la cuenta del servicio de Agente haciendo clic en **Personalizar la configuración de instalación** en el primer paso del asistente de instalación.

En Linux

1. Asegúrese de que el equipo está conectado a Internet.
2. Ejecute el archivo de instalación como usuario raíz.
3. Especifique las credenciales de la cuenta a la que se debe asignar el equipo.
4. Seleccione las casillas de verificación de los agentes que desea instalar. Los agentes disponibles son los siguientes:
 - **Agente para Linux**
 - **Agente para Virtuozzo**El Agente para Virtuozzo no se puede instalar sin el Agente para Linux.
5. Complete el proceso de instalación.

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

En OS X

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. Especifique las credenciales de la cuenta a la que se debe asignar el equipo.
7. Complete el proceso de instalación.

2.7.4 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.

2.8 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 **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: 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. Copie el programa de instalación en la carpeta que ha creado.
4. Inicie el programa de instalación.
5. Haga clic en **Crear archivos .mst y .msi para instalar sin supervisión**.
6. Si se le piden, facilite las credenciales de la cuenta a la que se deben asignar los equipos.
7. Compruebe o modifique la configuración de instalación que se añadirá al archivo .mst.
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. Entonces, podrá mover o borrar el archivo del programa de instalación .exe.

Paso 2: Configuración de objetos de directiva de grupo

1. Conéctese al controlador de dominio como un administrador de dominio y, si el dominio tiene más de un controlador de dominio, conéctese a cualquiera de ellos como un administrador de dominio.
2. Si tiene pensado implementar un Agente en una unidad organizacional, asegúrese de que la unidad organizacional existe en el dominio. De lo contrario, omita este paso.
3. En el menú **Inicio**, seleccione **Herramientas administrativas** y haga clic en **Equipos y usuarios de Active Directory** (en Windows Server 2003) o en **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 organizacional 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 organizacional y después haga clic en **Crear GPO en este dominio y haga un enlace 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 después haga clic en **Editar**.
 - En Windows Server 2008 y en Windows Server 2012, bajo **Objetos de directiva de grupo**, haga clic con el botón derecho del ratón sobre el objeto de directiva de grupo y después, haga clic en **Editar**.
 7. En el complemento del editor de objeto de directiva de grupo, expanda **Configuración del equipo**.
 8. En Windows Server 2003 y Windows Server 2008:
 - Expanda **Configuración de software**.
 En Windows Server 2012:
 - 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 **Software de implementación**, haga clic en **Avanzado** y después en **Aceptar**.
 12. En la pestaña **Modificaciones**, haga clic en **Añadir** y seleccione la transformación .mst que creó anteriormente.
 13. Haga clic en **Aceptar** para cerrar el cuadro de diálogo Implementar **software**.

2.9 Actualización de agentes

- Implementación en una instalación: para actualizar los agentes, primero actualice el servidor de gestión y luego repita la instalación del agente localmente o mediante la interfaz web.
- Implementación en la nube: los agentes se actualizan automáticamente en cuanto se publica una nueva versión. Si la actualización automática falla por algún motivo, siga el procedimiento que se describe a continuación.

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

Para actualizar una agente en una implementación en la nube

1. Haga clic en **Configuración > Agentes**.
El software muestra la lista de equipos. Los equipos con versiones de agentes obsoletas tienen un signo de exclamación naranja.
2. Seleccione los equipos en los que desea actualizar los agentes. Los equipos deben estar conectados.
3. Haga clic en **Actualizar agente**.
El proceso de actualización se muestra en la columna de estado de cada equipo.

2.10 Desinstalación del producto

Si desea quitar componentes de producto individuales de un equipo, ejecute el programa de instalación, elija modificar el producto y desmarque la selección de los componentes que desea quitar. Los enlaces a los programas de instalación están presentes en la página **Descargas** (haga clic en el icono de cuenta en la esquina superior derecha > **Descargas**).

Si desea quitar todos los componentes de producto de un equipo, siga los pasos que se describen a continuación.

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

En Windows

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

No marque esta casilla de verificación si va a desinstalar un agente, pero tiene previsto volverlo a instalar. Si selecciona la casilla de verificación, el equipo podría duplicarse en la consola de copia de seguridad y las copias de seguridad del antiguo equipo podrían no asociarse al nuevo equipo.

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

En Linux

1. Como usuario raíz, ejecute **/usr/lib/Acronis/BackupAndRecovery/uninstall/uninstall**.
2. [Opcional] Seleccione la casilla de verificación **Limpiar todos los rastros del producto (Eliminar los registros, tareas, bóvedas y opciones de configuración del producto)**.

No marque esta casilla de verificación si va a desinstalar un agente, pero tiene previsto volverlo a instalar. Si selecciona la casilla de verificación, el equipo podría duplicarse en la consola de copia de seguridad y las copias de seguridad del antiguo equipo podrían no asociarse al nuevo equipo.

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

En OS X

1. Haga doble clic en el archivo de instalación (.dmg).
2. Espere mientras el sistema operativo monta la imagen del disco de instalación.
3. Dentro de la imagen, haga doble clic en **Desinstalar**.
4. Si se le pide, proporcione las credenciales del administrador.
5. Confirme su decisión.
6. Si tiene previsto volver a instalar el agente, omita este paso. En caso contrario, en la consola de copia de seguridad, haga clic en **Configuración** > **Agentes**, seleccione el equipo donde se instaló el agente y, a continuación, haga clic en **Eliminar**.

Eliminación de Agente para VMware (dispositivo virtual)

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

3 Acceso a la consola de copia de seguridad

Introduzca la dirección de la página de inicio de sesión en la barra de direcciones del navegador web y, a continuación, indique el nombre de usuario y la contraseña.

Implementación en una instalación

La dirección de la página de inicio de sesión es la dirección IP o el nombre del equipo donde se ha instalado el servidor de gestión.

Para poder iniciar sesión, debe ser miembro del grupo de **Acronis Centralized Admins** en el equipo donde se haya instalado el servidor de gestión. De manera predeterminada, este grupo incluye a todos los miembros del grupo de **administradores**. Si el servidor de gestión se ha instalado en Linux, solo se permitirá iniciar sesión al usuario raíz.

Implementación en la nube

La dirección de la página de inicio de sesión es <https://backup.acronis.com/>. El nombre de usuario y la contraseña serán los mismos que los de su cuenta de Acronis.

Si su cuenta la creó el administrador de copias de seguridad, deberá activar la cuenta y establecer la contraseña haciendo clic en el enlace del correo electrónico de activación.

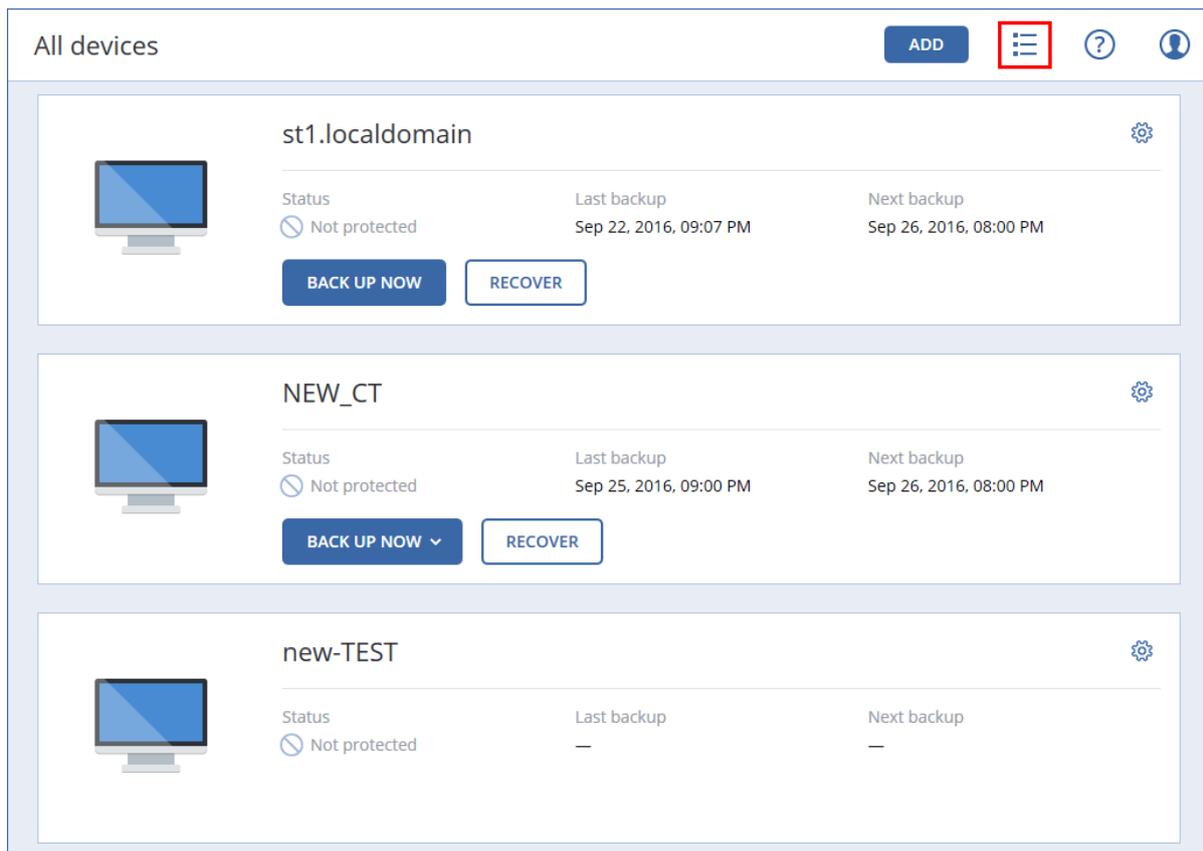
Cambio de idioma

Una vez que haya iniciado la sesión, puede cambiar el idioma de la interfaz web haciendo clic en el icono de la figura humana que hay en la esquina superior derecha.

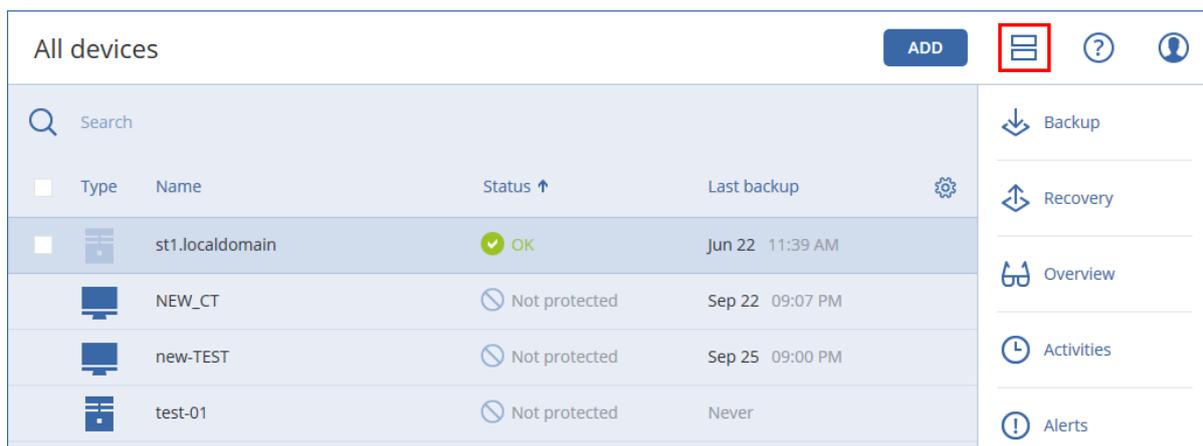
4 Vistas de la consola de copias de seguridad

La consola de copias de seguridad tiene dos vistas: una simple y una de tabla. Para cambiar el tipo de vista, haga clic en el icono correspondiente en la esquina superior derecha.

La vista simple admite un número reducido de equipos.



La vista de tabla se habilita automáticamente si el número de equipos aumenta considerablemente.



Las dos vistas proporcionan acceso a las mismas operaciones y características. Este documento detalla el acceso a operaciones desde la vista de tabla.

5 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.

The screenshot shows a configuration window for a backup plan titled "Entire machine to Cloud Storage". The window has a title bar with a pencil icon and a gear icon. Below the title bar, there are several rows of configuration options:

| | |
|------------------|---|
| WHAT TO BACK UP | Entire machine ▼ |
| WHERE TO BACK UP | Cloud Storage |
| SCHEDULE | Monday to Friday at 11:00 PM |
| HOW LONG TO KEEP | Monthly: 6 months Weekly: 4 weeks Daily: 7 days |
| ENCRYPTION | <input type="checkbox"/> Off ⓘ |

At the bottom of the configuration area, there is a large blue button labeled "APPLY".

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 **Aplicar**.

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 **Añadir plan de copias de seguridad**.

El software muestra planes de copias de seguridad creados previamente.



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

5.1 Apuntes del plan de copias de seguridad

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. 43) Normas de directiva (pág. 43) Filtros de archivo (pág. 60) | Cloud (pág. 47) Carpeta local (pág. 47) Carpeta de red (pág. 47) NFS (pág. 47)* Secure Zone (pág. 47)** | Siempre incremental (archivo único) (pág. 51) Siempre completas (pág. 51) Completas semanalmente, incrementales | Por antigüedad de las copias de seguridad (norma única/por conjunto de copias de seguridad) (pág. 52) Por número de copias de seguridad (pág. 52) Guardar indefinidamente (pág. 52) |
| Discos/volúmenes (equipos virtuales) | Normas de directiva (pág. 43) Filtros de archivo (pág. 60) | Cloud (pág. 47) Carpeta local (pág. 47) Carpeta de red (pág. 47) NFS (pág. 47)* | diariamente (pág. 51) Personalizadas (F-D-I) (pág. 51) | |
| Archivos (sólo equipos físicos) | Selección directa (pág. 44) Normas de directiva (pág. 44) Filtros de archivo (pág. 60) | Cloud (pág. 47) Carpeta local (pág. 47) Carpeta de red (pág. 47) NFS (pág. 47)* Secure Zone (pág. 47)** | Siempre completas (pág. 51) Completas semanalmente, incrementales diariamente (pág. 51) Personalizadas (F-D-I) (pág. 51) | |

| | | | | |
|---------------------------------|------------------------------|--|--|--|
| Configuración de ESXi | Selección directa (pág. 47) | Carpeta local (pág. 47) Carpeta de red (pág. 47) NFS (pág. 47)* | | |
| Estado del sistema | Selección directa (pág. 46) | Cloud (pág. 47) Carpeta local (pág. 47) Carpeta de red (pág. 47) | Siempre completas (pág. 51) Completas semanalmente, incrementales diariamente (pág. 51) Personalizadas (F-I) (pág. 51) | |
| Bases de datos SQL | Selección directa (pág. 111) | | | |
| Bases de datos de Exchange | Selección directa (pág. 112) | | | |
| Buzones de correo de Office 365 | Selección directa (pág. 123) | | Siempre incremental (archivo único) (pág. 51) | Por número de copias de seguridad (pág. 52) Guardar indefinidamente (pág. 52) |

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

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

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

5.2.1 Seleccionar discos/volúmenes

Un 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. 60).

Selección directa

La selección directa está disponible únicamente para los equipos físicos.

1. En **De qué realizar copias de seguridad**, seleccione **Discos/volúmenes**.
2. Haga clic en **Elementos para incluir en la copia de seguridad**.
3. En **Seleccionar elementos para incluir en la copia de seguridad**, seleccione **Directamente**.
4. Para cada uno de los equipos que se incluyen en el plan de copias de seguridad, seleccione las casillas que se encuentran al lado de los discos o volúmenes que se van a incluir en la copia de seguridad.
5. Haga clic en **Realizado**.

Usar las normas de política

1. En **De qué realizar copias de seguridad**, seleccione **Discos/volúmenes**.
2. Haga clic en **Elementos para incluir en la copia de seguridad**.

3. En **Seleccionar elementos para incluir en la copia de seguridad**, seleccione **Usar las normas de política**.
4. Seleccione cualquiera de las normas predefinidas, escriba sus propias normas o combine las dos. Las normas de política se aplicarán a todos los equipos incluidos en el plan de copias de seguridad. Si ninguno de los datos del equipo cumple como mínimo una de las normas, la copia de seguridad fallará cuando se inicie en ese equipo.
5. Haga clic en **Realizado**.

Normas para Windows, Linux y OS X

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

Normas para Windows

- La letra de unidad (por ejemplo: **C:**) selecciona el volumen con la letra de unidad especificada.
- **[Fixed Volumes (Physical machines)]** seleccione todos los volúmenes de los equipos físicos, además de los dispositivos extraíbles. Los volúmenes fijos incluyen aquellos en dispositivos SCSI, ATAPI, ATA, SSA, SAS y SATA, y conjuntos RAID.
- **[BOOT+SYSTEM]** selecciona los volúmenes del sistema y de arranque. Esta combinación es el conjunto mínimo de datos que garantiza la recuperación del sistema operativo desde la copia de seguridad.
- **[Disk 1]** selecciona el primer disco del equipo, incluidos todos los volúmenes de ese disco. Para seleccionar otro disco, escriba el número correspondiente.

Normas para Linux

- **/dev/hda1** selecciona el primer volumen en el primer disco duro IDE.
- **/dev/sda1** selecciona el primer volumen en el primer disco duro SCSI.
- **/dev/md1** selecciona el primer disco duro de software RAID.

Para seleccionar otros volúmenes básicos, especifique **/dev/xdyN**, donde:

- «x» corresponde al tipo de disco
- «y» corresponde al número de disco (a para el primer disco, b para el segundo disco y así sucesivamente)
- «N» es el número de volumen.

Para seleccionar un volumen, especifique su nombre junto con el nombre del grupo del volumen. Por ejemplo, para realizar copias de seguridad de dos volúmenes lógicos, **lv_root** y **lv_bin**, que pertenecen al grupo de volumen **vg_mymachine**, especifique:

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

Normas para OS X

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

5.2.2 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. 60).

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.
 - 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 OS X

- Ruta completa a un archivo o directorio.
- Plantillas:
 - **[All Profiles Folder]** selecciona **/Users**. En esta carpeta se ubican todos los perfiles de usuario de manera predeterminada.

Ejemplos:

- Para realizar una copia de seguridad de **file.txt** en su escritorio, especifique **/Users/<username>/Desktop/file.txt**. En este caso, <username> es su nombre de usuario.
- Para realizar copias de seguridad de todos los directorios de inicio de los usuarios, especifique **/Users**.
- Para realizar copias de seguridad del directorio donde están instaladas las aplicaciones, especifique **/Applications**.

5.2.3 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

5.2.4 Selección de la configuración de ESXi

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

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

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

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

Requisitos previos

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

Para seleccionar una configuración de ESXi

1. 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.

5.3 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.

- **Carpeta NFS** (disponible para equipos que ejecutan OS X o Linux)
Busque la carpeta NFS requerida o introduzca la ruta con el siguiente formato:
`nfs://<host name>/<exported folder>/<subfolder>`
Luego haga clic en el botón de la flecha.
No se puede realizar una copia de seguridad en una carpeta NFS protegida con contraseña.
- **Secure Zone** (disponible si está en todos los equipos seleccionados)
Secure Zone es una partición segura que está en un disco del equipo incluido en la copia de seguridad. Esta partición debe crearse manualmente antes de configurar una copia de seguridad. Para obtener información sobre cómo crear Secure Zone y sus ventajas y limitaciones, consulte "Acerca de Secure Zone" (pág. 48).

5.3.1 Acerca de Secure Zone

Secure Zone es una partición segura que está en un disco del equipo incluido en la copia de seguridad. La partición puede almacenar copias de seguridad de discos o archivos de este equipo.

Si el disco presenta un error físico, las copias de seguridad almacenadas en Secure Zone podrían perderse. Esa es la razón por la que Secure Zone no debe ser la única ubicación donde se almacene una copia de seguridad. En entornos empresariales, se puede pensar en Secure Zone como una ubicación intermedia utilizada para realizar copias de seguridad cuando una ubicación normal no está disponible temporalmente o se conecta a partir de un canal lento u ocupado.

Motivos para usar Secure Zone.

Secure Zone:

- Permite la recuperación de un disco en el mismo disco en donde reside la copia de seguridad del disco.
- Constituye un método rentable y práctico para la protección de datos ante un funcionamiento defectuoso del software, ataques de virus o errores humanos.
- Elimina la necesidad de medios o conexiones de red diferentes para realizar copias de seguridad o recuperar los datos. Esto es muy útil para los usuarios itinerantes.
- Puede funcionar como destino primario cuando se usa la replicación de copias de seguridad.

Limitaciones

- Secure Zone no se puede organizar en un Mac.
- Secure Zone es una partición en un disco básico. No puede organizarse en un disco dinámico ni crearse como volumen lógico (administrado por LVM).
- Secure Zone tiene el formato de sistema de archivos FAT32. Como FAT32 tiene un límite de tamaño de archivos de 4 GB, las copias de seguridad de mayor tamaño se dividen al guardarse en Secure Zone. Esto no afecta al procedimiento de recuperación ni a la velocidad.
- Secure Zone no admite el formato de copia de seguridad de archivo único (pág. 149). Al cambiar el destino a Secure Zone en un plan de copias de seguridad que tiene el esquema de copias de seguridad **Siempre incremental (archivo único)**, este cambia a **Completas semanalmente, incrementales diariamente**.

Cómo la creación de Secure Zone transforma el disco

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

- Si no hay espacio sin asignar suficiente o no hay al final del disco, pero sí hay espacio sin asignar entre volúmenes, estos últimos se moverán para agregar más espacio sin asignar al final del disco.
- Cuando se recopile todo el espacio sin asignar y el mismo siga siendo insuficiente, el software sacará espacio libre de los volúmenes que seleccione, de forma proporcional, reduciendo el tamaño de los volúmenes.
- Sin embargo, debería haber espacio libre en un volumen para que el sistema operativo y las aplicaciones puedan funcionar; por ejemplo, para crear archivos temporales. El software no reducirá un volumen en el que el espacio libre ocupe el 25 % o menos del tamaño total del volumen. El software continuará reduciendo los volúmenes de forma proporcional únicamente cuando todos los volúmenes del disco tengan el 25 % o menos espacio libre.

Como se deduce de esto, no es recomendable especificar el tamaño máximo posible para Secure Zone. Acabará sin espacio libre en ningún volumen, lo que puede hacer que el sistema operativo o las aplicaciones funcionen de forma inestable e incluso que no puedan iniciarse.

Importante: Para mover o cambiar el tamaño del volumen desde el que se arranca el sistema actualmente, es necesario reiniciar.

Cómo crear Secure Zone

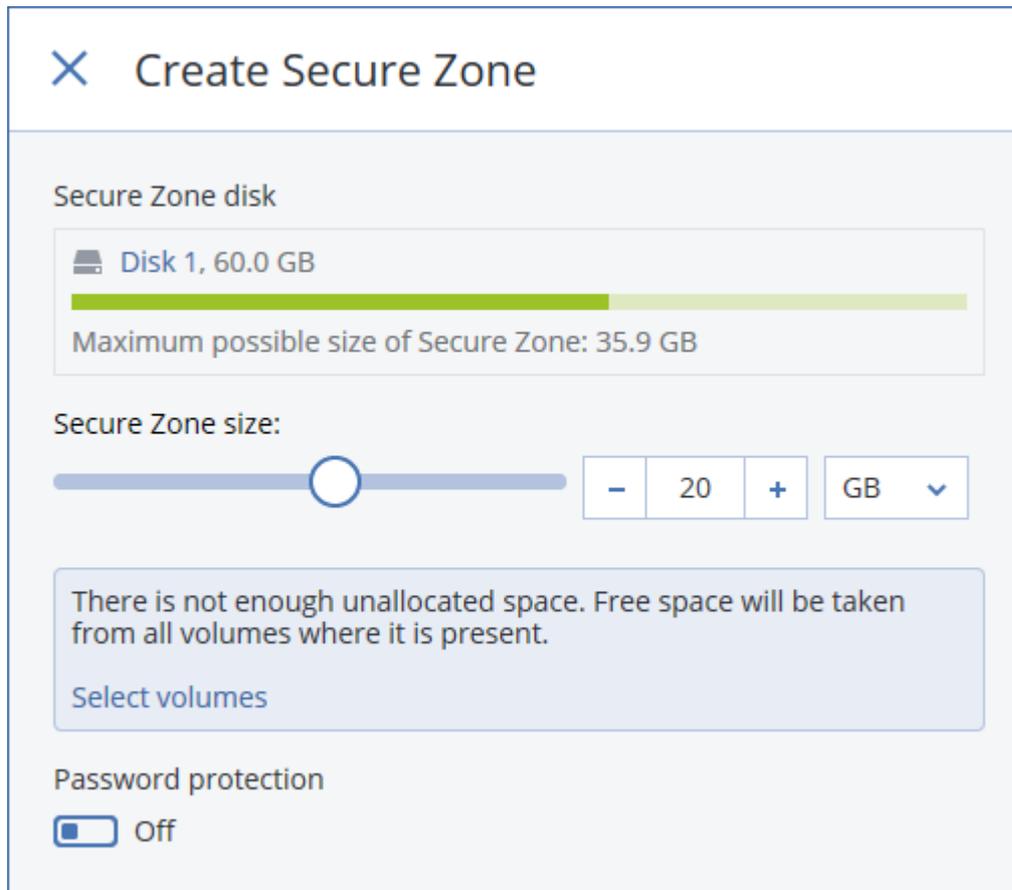
1. Seleccione el equipo en el que desea crear Secure Zone.
2. Haga clic en **Generalidades > Crear Secure Zone**.
3. En el **disco Secure Zone**, haga clic en **Seleccionar** y, a continuación, elija el disco rígido (si hay más de uno) en el que desea crear la zona.

El software calcula el tamaño máximo posible de Secure Zone.

4. Indique el tamaño de Secure Zone o arrastre el deslizador para seleccionarlo entre los mínimos y los máximos.

El tamaño mínimo es de aproximadamente 50 MB, de acuerdo con la geometría del disco duro. El tamaño máximo es igual al espacio sin asignar del disco más el espacio libre total de todos los volúmenes del disco.

- Si el espacio sin asignar no es suficiente para el tamaño que ha indicado, el software obtendrá el espacio libre de los volúmenes existentes. De manera predeterminada, se seleccionan todos los volúmenes. Si desea excluir algunos volúmenes, haga clic en **Seleccionar volúmenes**. De lo contrario, omita este paso.



- [Opcional] Habilite el conmutador **Protección mediante contraseña** y especifique una contraseña.

La contraseña es obligatoria para acceder a las copias de seguridad ubicadas en Secure Zone. No se necesita contraseña para realizar una copia de seguridad en Secure Zone, salvo que dicha copia de seguridad se haga en un dispositivo de arranque.

- Haga clic en **Crear**.

El software muestra la distribución esperada de la partición. Haga clic en **Aceptar**.

- Espere mientras el software crea Secure Zone.

Ahora puede escoger Secure Zone en **Dónde realizar copias de seguridad** al crear un plan de copias de seguridad.

Cómo eliminar Secure Zone

- Seleccione un equipo con Secure Zone.
- Haga clic en **Generalidades**.
- Haga clic en el icono de engranaje situado junto a **Secure Zone** y después, haga clic en **Eliminar**.
- [Opcional] Seleccione los volúmenes a los que desea agregar el espacio liberado de la zona. De manera predeterminada, se seleccionan todos los volúmenes.

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

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

5. Haga clic en **Eliminar**.

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

5.4 Planificación

Los parámetros de planificación dependen del destino de la copia de seguridad.

Quando 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.*

Quando 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. 149). 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 en las implementaciones en la cloud, con un valor máximo de demora establecido en 30 minutos. En el caso de implementaciones locales, de manera predeterminada todas las copias de seguridad se inician según la planificación.*

5.5 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. 149) 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.*

5.6 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. 47).
3. En **Cuánto tiempo guardarlas**, especifique las reglas de retención, tal como se describe en "Reglas de retención" (pág. 52).

5.7 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, la ruta es `%ProgramFiles%\BackupClient` para las implementaciones en la cloud y `%ProgramFiles%\Acronis` para las implementaciones locales.
 - En Linux: `/usr/sbin/acropsh -m manage_creds --set-password <encryption_password>`

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, la ruta es %ProgramFiles%\BackupClient para las implementaciones en la cloud y %ProgramFiles%\Acronis para las implementaciones locales.

- En Linux: `/usr/sbin/acropsh -m manage_creds --reset`

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.

5.8 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.

5.9 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, OS X).
- 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 | OS X | Windows | Linux | OS X | ESXi | Hyper-V | Windows |
|---|---------|-------|------|---------|-------|------|------|---------|----------|
| Consolidación de la copia de seguridad (pág. 57) | + | + | + | + | + | + | + | + | - |
| Validación de la copia de seguridad (pág. 58) | + | + | + | + | + | + | + | + | + |
| Seguimiento de bloques modificados (CBT) (pág. 58) | + | - | - | - | - | - | + | + | - |
| Tasa de compresión (pág. 58) | + | + | + | + | + | + | + | + | + |
| Notificaciones por correo electrónico (pág. 59) | + | + | + | + | + | + | + | + | + |
| Manejo de errores (pág. 59) | | | | | | | | | |
| Reintentar si se produce un error. | + | + | + | + | + | + | + | + | + |
| No mostrar mensajes ni diálogos durante el procesamiento (modo silencioso) | + | + | + | + | + | + | + | + | + |
| Ignorar los sectores defectuosos | + | + | + | + | + | + | + | + | - |
| Reintentar si se produce un error durante la creación de instantáneas de VM | - | - | - | - | - | - | + | + | - |
| Copias de seguridad incrementales/diferenciales rápidas (pág. 60) | + | + | + | - | - | - | - | - | - |
| Instantánea de la copia de seguridad a nivel de archivo (pág. 62) | - | - | - | + | + | + | - | - | - |
| Seguridad a nivel de archivo (pág. 62) | - | - | - | + | - | - | - | - | - |
| Filtros de archivo (pág. 60) | + | + | + | + | + | + | + | + | - |
| Truncamiento de registros (pág. 63) | - | - | - | - | - | - | + | + | Solo SQL |
| Toma de instantáneas de LVM (pág. 63) | - | + | - | - | - | - | - | - | - |
| Puntos de montaje (pág. 63) | - | - | - | + | - | - | - | - | - |
| Instantánea multivolumen (pág. 64) | + | - | - | + | - | - | - | - | - |
| Rendimiento (pág. 65) | + | + | + | + | + | + | + | + | + |
| Comandos previos/posteriores (pág. 66) | + | + | + | + | + | + | + | + | + |

| | Copia de seguridad a nivel de discos | | | Copia de seguridad a nivel de archivos | | | Equipos virtuales | | SQL y Exchange |
|---|--------------------------------------|-------|------|--|-------|------|-------------------|---------|----------------|
| | Windows | Linux | OS X | Windows | Linux | OS X | ESXi | Hyper-V | Windows |
| Comandos previos o posteriores a la captura de datos (pág. 67) | + | + | + | + | + | + | - | - | + |
| Planificación (pág. 69) | | | | | | | | | |
| 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. 70) | + | + | - | - | - | - | + | + | - |
| División (pág. 70) | + | + | + | + | + | + | + | + | + |
| Manejo de fallos de la tarea (pág. 70) | + | + | + | + | + | + | + | + | + |
| Volume Shadow Copy Service (VSS) (pág. 71) | + | - | - | + | - | - | - | + | + |
| Volume Shadow Copy Service (VSS) para equipos virtuales (pág. 72) | - | - | - | - | - | - | + | + | - |
| Copia de seguridad semanal (pág. 72) | + | + | + | + | + | + | + | + | + |
| Registro de eventos de Windows (pág. 72) | + | - | - | + | - | - | + | + | + |

5.9.1 Consolidación de la copia de seguridad

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

El valor predeterminado es: **Deshabilitado**.

La consolidación es el proceso de combinar dos o más copias de seguridad subsiguientes en una sola.

Si esta opción está habilitada, una copia de seguridad que debería eliminarse durante la limpieza se consolida con la siguiente copia de seguridad dependiente (incremental o diferencial).

Si no, la copia de seguridad se retiene hasta que se puedan eliminar todas las dependientes. Esto ayuda a evitar una consolidación que requeriría mucho tiempo, pero necesita espacio extra para almacenar copias de seguridad cuya eliminación se ha postergado. El número de copias de seguridad o su antigüedad puede superar los valores indicados en las reglas de retención.

Importante: Tenga en cuenta que la consolidación es solo un método para eliminar y no una alternativa a la eliminación. La copia de seguridad resultante no tendrá los datos que estaban en la copia de seguridad eliminada y que no estaban en la copia de seguridad incremental o diferencial retenida.

5.9.2 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. 125) en el entorno de ESXi o Hyper-V.

5.9.3 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.

5.9.4 Tasa de compresión

Esta opción define el tasa de compresión que se aplicará a los datos que se incluyen en la copia de seguridad. Los niveles disponibles son: **Ninguno, Normal y Alto**.

El preajuste es: **Normal**.

Un tasa de compresión mayor implica que el proceso de copia de seguridad requiere más tiempo, pero la copia de seguridad resultante ocupa menos espacio.

El tasa de compresión de datos óptimo dependerá del tipo de datos que se incluyen en la copia de seguridad. Por ejemplo, ni siquiera la máxima compresión conseguirá reducir significativamente el

tamaño de la copia de seguridad si esta contiene archivos esencialmente comprimidos, como .jpg, .pdf o .mp3. Sin embargo, los formatos como .doc o .xls se comprimirán correctamente.

5.9.5 Notificaciones por correo electrónico

Esta opción permite configurar notificaciones por correo electrónico relacionadas con errores, advertencias y copias de seguridad completadas correctamente.

Esta opción solo está disponible en implementaciones locales. En el caso de las implementaciones en la cloud, los ajustes se configuran en cada cuenta cuando se crea una cuenta (pág. 143).

El preajuste es: **Usar los ajustes predeterminados.**

Puede utilizar los ajustes predeterminados o anularlos mediante los valores personalizados que se especificarán únicamente para este plan. Los ajustes predeterminados se configuran como se describe en "Notificaciones por correo electrónico" (pág. 141).

Importante: *Cambiar los ajustes predeterminados afecta a todos los planes de copias de seguridad que usan estos ajustes.*

Antes de habilitar esta opción, asegúrese de que se han configurado los ajustes del **Servidor de correo electrónico** (pág. 140).

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

1. Seleccione **Personalizar los ajustes de este plan de copias de seguridad**.
2. En el campo **Direcciones de correo electrónico de los destinatarios**, escriba la dirección de correo electrónico de destino. Puede introducir varias direcciones separadas por punto y coma.
3. Seleccione los tipos de notificaciones que quiere que se envíen. Los tipos disponibles son los siguientes:
 - **Errores**
 - **Advertencias**
 - **Copias de seguridad correctas**

El asunto de los mensajes de correo electrónico se basa en la plantilla siguiente: **[asunto] [nombre de equipo] [nombre de plan de copias de seguridad]**. La variable **[subject]** (asunto) se reemplazará por una de las siguientes frases: **Copia de seguridad correcta**, **Copia de seguridad con errores**, **Copia de seguridad correcta con advertencias**.

5.9.6 Manejo de errores

Estas opciones le permiten que establezca como se manejarán los errores que puedan suceder durante la copia de seguridad.

Reintentar si se produce un error.

El valor predeterminado: **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.

Nota Si se selecciona el almacenamiento en la nube como destino primario o secundario, el valor de la opción se establece automáticamente en **Habilitado**. **Cantidad de intentos: 300**.

No mostrar mensajes ni diálogos durante el procesamiento (modo silencioso)

El valor predeterminado: **Habilitado**.

Cuando se habilite el modo silencioso, el programa manejará automáticamente las situaciones que requieran interacción del usuario (a excepción del manejo de sectores defectuosos que se definen con otra opción). Si una operación no puede continuar sin la acción del usuario, ésta fallará. Los detalles de la operación, incluyendo los errores, si los hubiera, pueden encontrarse en el registro de la operación.

Ignorar los sectores defectuosos

El valor predeterminado: **Deshabilitado**.

Cuando esta opción está deshabilitada, cada vez que el programa encuentre un sector defectuoso, se asignará a la actividad de copia de seguridad el estado **Interacción necesaria**. Para realizar una copia de seguridad de información válida en un disco que se está dañando rápidamente, habilite ignorar sectores defectuosos. Se realizará una copia de seguridad del resto de los datos y podrá montar la copia de seguridad del disco resultante y extraer los archivos válidos a otro disco.

Reintentar si se produce un error durante la creación de instantáneas de VM

El valor predeterminado es: **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 correcta o se agote el número de intentos especificados, lo que suceda primero.

5.9.7 Copias de seguridad incrementales/diferenciales rápidas

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

El valor predeterminado: **Habilitado**.

La copia de seguridad incremental o diferencial sólo captura los cambios en los datos. Para acelerar el proceso de copia de seguridad, el programa determina si un archivo ha cambiado por su tamaño y la fecha/hora en la que se guardó por última vez. Si deshabilita esta característica, el programa compara el contenido completo del archivo con el que esté almacenado en la copia de seguridad.

5.9.8 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 es eficaz para copias de seguridad a nivel de archivo, salvo si el destino es Cloud Storage.

- **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 del archivo o carpeta, empezando con la letra de unidad (cuando haga una copia de seguridad de Windows) o con el directorio raíz (cuando haga una copia de seguridad de Linux o de OS X).

Puede usar una barra diagonal en la ruta de archivo o carpeta (como en **C:/Temp/File.tmp**) tanto en Windows como en Linux/OS X. 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 usar uno o más 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 signo de pregunta (?) sustituye exactamente un carácter en el nombre del archivo. Por ejemplo, el criterio **Doc?.txt** coincide con archivos como **Doc1.txt** y **Docs.txt**, pero no con los archivos **Doc.txt** o **Doc11.txt**.

Excluir archivos y carpetas ocultos

Seleccione esta casilla de verificación para omitir los archivos y carpetas que tengan el atributo **Oculto** (para los sistemas de archivos compatibles con Windows) o que empiecen con un punto (.)

(para los sistemas de archivos en Linux, como Ext2 y Ext3). Si una carpeta está oculta, se excluirán todos sus contenidos (incluso los archivos que no se encuentren ocultos).

Excluir archivos y carpetas del sistema

Esta opción está vigente solo para sistemas de archivos compatibles con Windows. Seleccione esta casilla de verificación para omitir archivos y carpetas con el atributo **Sistema**. Si una carpeta tiene el atributo **Sistema**, se excluirán todos sus contenidos (incluso los archivos que no tengan el atributo **Sistema**).

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

5.9.9 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.

5.9.10 Seguridad de nivel de archivo

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

Esta opción define si realiza copia de seguridad de permisos para archivos NTFS junto a los archivos.

El valor predeterminado: **Habilitado**.

Cuando se habilita esta opción, se hace una copia de seguridad de los archivos y las carpetas con los permisos originales de lectura, escritura o ejecución de archivos por cada usuario o grupo de usuarios. Si restaura un archivo o carpeta protegidos en un equipo sin la cuenta de usuario especificada en los permisos, es posible que no pueda leer ni modificar este archivo.

Si esta opción está deshabilitada, los archivos y las carpetas recuperados heredarán los permisos de la carpeta donde se recupera o del disco (si se recupera en la raíz).

Otra opción es desactivar la recuperación (pág. 89) de la configuración de seguridad. El resultado será el mismo: los archivos heredarán los permisos de la carpeta principal.

5.9.11 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 esta opción está habilitada, una base de datos solo se puede recuperar a un momento específico de una copia de seguridad que haya creado este software. Deshabilite esta opción si realiza copias de seguridad de los registros de transacción usando el motor nativo de copia de seguridad de Microsoft SQL Server. Podrá aplicar los registros de transacción después de una recuperación y, por lo tanto, recuperar una base de datos a cualquier momento específico.

5.9.12 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.

5.9.13 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. 90)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. 90)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 una copia 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. 90)Puntos de montaje**.

Si selecciona la casilla de verificación para el volumen C y deshabilita la opción **Puntos de montaje**, la carpeta **C:\Datos1** en su copia de seguridad estará vacía.

Si selecciona la casilla de verificación para la carpeta **Datos1**, **Carpeta1** o **Carpeta2**, las carpetas marcadas se incluirán en la copia de seguridad como carpetas normales, sin importar el estado de la opción de los **Puntos de montaje**.

5.9.14 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. 62) determina si se tomará una instantánea durante la copia de seguridad a nivel de archivo).

Esta opción determina si se tomarán las instantáneas de varios volúmenes al mismo tiempo o una a una.

El valor predeterminado es: **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.

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

5.9.16 Comandos pre/post

Esta opción le permite definir los comandos a ejecutar automáticamente antes y después del proceso de copia de seguridad.

El siguiente esquema describe cuando se ejecutan los comandos pre/post.

| | | |
|----------------------------------|--------------------------|------------------------------------|
| Comando de precopia de seguridad | Crear copia de seguridad | Comando de Post-copia de seguridad |
|----------------------------------|--------------------------|------------------------------------|

Ejemplos de como se pueden usar los comandos pre/post:

- Eliminación de archivos temporales antes de comenzar la copia de seguridad.
- Configuración de un producto antivirus de terceros antes de comenzar la copia de seguridad.
- Copia selectiva de copias de seguridad en otra ubicación. Esta opción puede ser útil porque la replicación configurada en un plan de copias de seguridad copia *todas* las copias de seguridad a ubicaciones posteriores.

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

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

5.9.16.1 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 |
| No realizar la copia de seguridad hasta que finalice la ejecución de comandos | Seleccionado | Seleccionado | Borrado | Borrado |
| Resultado | | | | |
| | Valor | Realizar la copia de seguridad después | N/D | Realizar la copia de seguridad al mismo |

| | | | | |
|--|--|--|--|---|
| | <p>predeterminado</p> <p>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.</p> | de que se ejecute el comando a pesar del éxito o fallo de la ejecución | | tiempo que se ejecuta el comando, independientemente del resultado de la ejecución del comando. |
|--|--|--|--|---|

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

5.9.16.2 Comando de Post-copia de seguridad

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

1. Habilite el conmutador **Ejecutar un comando tras la copia de seguridad**.
2. En el campo **Comando...**, escriba un comando o busque un archivo de proceso por lotes.
3. En el campo **Directorio de trabajo**, especifique la ruta del directorio donde se ejecutará el comando o archivo de proceso por lotes.
4. En el campo **Argumentos**, especifique los argumentos de ejecución del comando, si fuera necesario.
5. Active la casilla de verificación **Hacer que la copia de seguridad falle si falla la ejecución del comando** si cree que la ejecución correcta del comando es fundamental. El comando se considerará fallido si su código de salida no es igual a cero. Si la ejecución del comando falla, el estado de la copia de seguridad será **Error**.

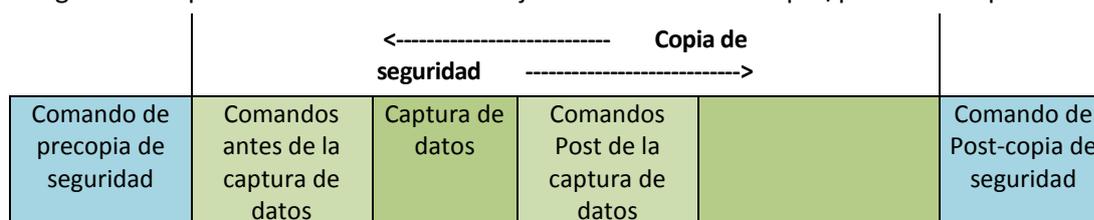
Cuando no se marca la casilla de verificación, los resultados de la ejecución del comando no afectarán al éxito o fallo de la copia de seguridad. Puede realizar un seguimiento de la ejecución de comandos desde la pestaña **Actividades**.

6. Haga clic en **Realizado**.

5.9.17 Comandos previos o posteriores a la captura de datos

La opción le permite definir los comandos que se ejecutarán automáticamente antes y después de la captura de datos (es decir, tomar la instantánea de los datos). La captura de datos se realiza al comienzo del procedimiento de copia de seguridad.

El siguiente esquema describe cuando se ejecutan los comandos pre/post de la captura de datos.



Si la opción (pág. 71) Volume Shadow Copy Service está habilitada, la ejecución de los comandos y las acciones de Microsoft VSS se sucederán tal y como se indica a continuación:

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

El uso de comandos previos y posteriores a la captura de datos permite suspender y reanudar una base de datos o una aplicación que no sean compatibles con VSS. Como la captura de datos tarda unos segundos, el tiempo de inactividad de la base de datos o la aplicación será mínimo.

5.9.17.1 Comandos antes de la captura de datos

Para especificar un comando o archivo por lotes para que se ejecute antes de la captura de datos

1. Habilite el conmutador **Ejecutar un comando antes de la captura de datos**.
2. En el campo **Comando...**, escriba un comando o busque un archivo de proceso por lotes. El programa no admite comandos interactivos, es decir, comandos que requieran la intervención del usuario (por ejemplo, "pause").
3. En el campo **Directorio de trabajo**, especifique una ruta en donde se ejecutará el comando o archivo por lotes.
4. En el campo **Argumentos**, especifique los argumentos de ejecución del comando, si fuera necesario.
5. Dependiendo del resultado que desee obtener, seleccione la opción apropiada tal y como se describe en la siguiente tabla.
6. Haga clic en **Realizado**.

| Casilla de verificación | Selección | | | |
|---|---|---|--------------|---|
| Hacer que la copia de seguridad falle si falla la ejecución del comando* | Seleccionado | Borrado | Seleccionado | Borrado |
| No realizar la captura de datos hasta que finalice la ejecución de comandos | Seleccionado | Seleccionado | Borrado | Borrado |
| Resultado | | | | |
| | Valor predeterminado Realizar la captura de datos solo después de que se ejecute el comando correctamente. Hacer que la copia de seguridad falle si falla la ejecución del comando. | Realizar la captura de datos después de que se ejecute el comando a pesar del éxito o fallo de la ejecución | N/D | Realizar la captura de datos al mismo tiempo que se ejecuta el comando, independientemente del resultado de la ejecución del comando. |

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

5.9.17.2 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 |
| No realizar la copia de seguridad hasta que finalice la ejecución de comandos | Seleccionado | Seleccionado | Borrado | Borrado |
| Resultado | | | | |
| | Valor predeterminado Continúe la copia de seguridad solo después de que se ejecute el comando correctamente. | Continúe la copia de seguridad después de que se ejecute el comando a pesar del éxito o fallo de su ejecución. | N/D | Continuar la copia de seguridad al mismo tiempo que se ejecuta el comando, independientemente del resultado de la ejecución del comando. |

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

5.9.18 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 valor predeterminado es:

- Implementación en una instalación: **Iniciar todas las copias de seguridad según lo planificado.**
- Implementación en la nube: **Distribuir las horas de inicio de la copia de seguridad en una ventana 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 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.

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

5.9.19 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. 58) se define en **Ninguno**). El software cambia automáticamente al modo sector por sector al hacer copias de seguridad de unidades con sistemas de archivos no reconocidos o incompatibles.

5.9.20 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.

5.9.21 Manejo de fallos de la tarea

Esta opción determina el comportamiento del programa cuando falla la ejecución de un plan de copias de seguridad.

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: **Deshabilitado**.

5.9.22 Volume Shadow Copy Service (VSS)

Esta opción solo sirve para los sistemas operativos 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 valor predeterminado: **Habilitado. Seleccionar automáticamente el proveedor de instantáneas.**

Puede seleccionar una de las siguientes opciones:

- **Seleccionar automáticamente el proveedor de instantáneas**
Seleccione automáticamente entre el proveedor de instantáneas de hardware, los proveedores de instantáneas de software y Microsoft Software Shadow Copy Provider.
- **Usar Microsoft Software Shadow Copy Provider**
Recomendamos seleccionar esta opción cuando realice una copia de seguridad de los servidores de la aplicación (Microsoft Exchange Server, Microsoft SQL Server, Microsoft SharePoint o Active Directory).

Deshabilite esta opción si la base de datos es incompatible con VSS. Las instantáneas se realizan con más rapidez, pero no es posible garantizar la coherencia de los datos de aplicaciones cuyas transacciones no se hayan completado en el momento de la toma de la instantánea. Puede usar los comandos previos o posteriores a la captura de datos (pág. 67) 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 todas las transacciones, y especifique los comandos Post de la captura de datos que reanudarán las operaciones después de tomar las instantáneas.

Habilitar la copia de seguridad completa de VSS

Al habilitar esta opción, se truncarán los registros de Microsoft Exchange Server y de las demás aplicaciones compatibles con VSS (excepto para Microsoft SQL Server) después de cada copia de seguridad completa, incremental o diferencial a nivel de disco.

El valor predeterminado es: **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. 63).

5.9.23 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. 59) y la copia de seguridad de aplicaciones está deshabilitada, se realiza una copia de seguridad activa. Si la copia de seguridad de aplicaciones está habilitada, la copia de seguridad falla.

Si esta opción está deshabilitada, se realiza una instantánea activa. Se hará una copia de seguridad del equipo virtual en un estado de coherencia con bloqueos.

5.9.24 Copia de seguridad semanal

Esta opción determina las copias de seguridad que se consideran "semanales" en las reglas de retención y los esquemas de copias de seguridad. Una copia de seguridad "semanal" es la primera copia de seguridad creada una vez comenzada la semana.

El valor predeterminado es: **Lunes**.

5.9.25 Registro de sucesos de Windows

Esta opción sólo funciona en los sistemas operativos de Windows.

Esta opción define si los agentes tienen que recopilar los eventos de las operaciones de copia de seguridad en el registro de eventos de aplicación de Windows (para ver este registro, ejecute eventvwr.exe o seleccione **Panel de control > Herramientas administrativas > Visor de eventos**). Puede filtrar los eventos que quiere recopilar.

El valor predeterminado: **Deshabilitado**.

6 Recuperación

6.1 Recuperación de apuntes

La siguiente tabla resume los métodos de recuperación disponibles. Use la tabla para elegir el método de recuperación que más le convenga.

| Qué recuperar | Método de recuperación |
|-----------------------------------|---|
| Equipo físico (Windows o Linux) | Uso de la interfaz web (pág. 74) Uso de dispositivos de arranque (pág. 78) |
| Equipo físico (Mac) | Uso de dispositivos de arranque (pág. 78) |
| Equipo virtual (VMware o Hyper-V) | Uso de la interfaz web (pág. 77) Uso de dispositivos de arranque (pág. 78) |
| Configuración de ESXi | Uso de dispositivos de arranque (pág. 85) |
| Archivos/Carpetas | Uso de la interfaz web (pág. 82) Descargar archivos del almacenamiento en la cloud (pág. 83) Uso de dispositivos de arranque (pág. 84) Extraer archivos de copias de seguridad locales (pág. 85) |
| Estado del sistema | Uso de la interfaz web (pág. 85) |
| Bases de datos SQL | Uso de la interfaz web (pág. 114) |
| Bases de datos de Exchange | Uso de la interfaz web (pág. 117) |
| Buzones de correo de Exchange | Uso de la interfaz web (pág. 119) |
| Buzones de correo de Office 365 | Uso de la interfaz web (pág. 123) |

Nota para los usuarios de Mac

- A partir de El Capitan 10.11, ciertos archivos de sistema, carpetas y procesos se marcan para su protección con el atributo de archivo extendido `com.apple.rootless`. Esta característica se llama Protección de integridad del sistema (SIP, por sus siglas en inglés). Los archivos protegidos incluyen aplicaciones previamente instaladas y la mayoría de carpetas en las ubicaciones `/system`, `/bin`, `/sbin`, `/usr`.
Los archivos y carpetas protegidos no pueden sobrescribirse durante una recuperación realizada mediante el sistema operativo. Si necesita sobrescribir los archivos protegidos, realice la recuperación mediante dispositivos de arranque.
- A partir de macOS Sierra 10.12, puede mover los archivos que raramente utiliza a iCloud con la función Almacenar en la cloud. Se conservan espacios físicos reducidos de estos archivos en el sistema de archivos. Estos espacios se incluyen en la copia de seguridad en lugar de los archivos originales.
Cuando se recupera un espacio en la ubicación original, este se sincroniza con iCloud y, por lo tanto, el archivo original está disponible. Cuando se recupera un espacio en una ubicación diferente, este no se puede sincronizar y, por lo tanto, el archivo original no está disponible.

6.2 Creación de dispositivos de inicio

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

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

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

Para crear dispositivos de arranque en Windows o Linux

1. Descargue el archivo ISO del 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.

De forma alternativa, puede crear un dispositivo de arranque utilizando Bootable Media Builder (pág. 96).

Para crear dispositivos de arranque 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 arranque.

Aviso Toda la información del disco se borrará.

3. Haga clic en **Crear**.
4. Espere mientras el software crea el dispositivo de arranque.

6.3 Recuperar un equipo

6.3.1 Equipo físico

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

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

- 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. 93).
- Recupere el equipo como se describe en "Recuperar discos usando dispositivos de inicio" (pág. 78).

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. 78). El dispositivo le permite elegir los discos que desea recuperar y asignarlos manualmente.



RECUPERAR A
Equipo físico ▾

EQUIPO DE DESTINO
ABR11MMS

ASIGNACIÓN DE DISCOS
Disk 1 → Disk 1

INICIAR RECUPERACIÓN

OPCIONES DE RECUPERACIÓN

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**.

6.3.2 De equipo físico a virtual

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

Para más información sobre la migración P2V, consulte "Migración de equipos" (pág. 133).

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. 93).
 - Recupere el equipo como se describe en "Recuperar discos usando dispositivos de inicio" (pág. 78).
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**.

6.3.3 Equipo virtual

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

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

Para recuperar un equipo virtual

1. Realice uno de los siguientes procedimientos:
 - Seleccione un equipo incluido en la copia de seguridad, haga clic en **Recuperación** y luego seleccione un punto de recuperación.
 - Seleccione un punto de recuperación en la pestaña Copias de seguridad (pág. 93).
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. 74). En caso contrario, le recomendamos que realice la migración V2P utilizando un dispositivo de arranque (pág. 78).

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** o **Hyper-V**).
 - b. Seleccione si desea realizar la recuperación en un equipo nuevo o en otro ya existente.
 - c. Seleccione el servidor y especifique el nuevo nombre de equipo, o bien seleccione un equipo de destino existente.
 - d. Haga clic en **Aceptar**.
5. [Opcional] Al recuperar en un equipo nuevo, también puede hacer lo siguiente:
 - Haga clic en **Almacén de datos** para ESXi o **Ruta** para Hyper-V y, a continuación, seleccione el almacén de datos (almacenamiento) para el equipo virtual.
 - Haga clic en **Configuración de VM** para cambiar el tamaño de la memoria, el número de procesadores y las conexiones de red del equipo virtual.

RECUPERAR A
Equipo virtual ▾

EQUIPO DE DESTINO
New machine en 10.250.151.182 **Nuevo**

ALMACÉN DE DATOS
datastore-share-iscsi-bender

CONFIGURACIÓN DE VM
Memoria: 1.00 GB
Procesadores virtuales: 1
Adaptadores de red: 0

INICIAR RECUPERACIÓN  OPCIONES DE RECUPERACIÓN

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

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

6.3.4 Recuperar discos usando dispositivos de arranque

Para obtener información sobre cómo crear dispositivos de inicio, consulte "Crear dispositivos de arranque" (pág. 73).

Para recuperar discos usando dispositivos de arranque.

1. Inicie el equipo de destino usando dispositivos 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 las copias de seguridad**, seleccione los discos que desea recuperar. Haga clic en **Aceptar** para confirmar su selección.
9. 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.

10. [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.
11. [Opcional] Haga clic en **Opciones de recuperación** para especificar configuraciones adicionales.
12. Haga clic en **Aceptar** para comenzar la recuperación.

6.3.5 Uso de Universal Restore

Los sistemas operativos más recientes siguen pudiendo arrancarse cuando se recuperan en un hardware diferente, incluidas las plataformas VMware o Hyper-V. Si un sistema operativo recuperado no arranca, utilice la herramienta Universal Restore para actualizar los controladores y los módulos que sean críticos para el inicio del sistema operativo.

Universal Restore se puede aplicar a Windows y Linux.

Para aplicar Universal Restore

1. Inicie el equipo desde el dispositivo de arranque.
2. Haga clic en **Aplicar Universal Restore**.

3. Si existen varios sistemas operativos en el equipo, escoja aquel donde desea aplicar Universal Restore.
4. [Solo para Windows] Configure los ajustes adicionales (pág. 80).
5. Haga clic en **Aceptar**.

6.3.5.1 Universal Restore en Windows

Preparación

Preparar los controladores

Antes de aplicar Universal Restore a un sistema operativo de Windows, asegúrese de contar con los controladores para el nuevo controlador HDD y el conjunto de chips. Estos controladores son críticos para iniciar el sistema operativo. Utilice el CD o DVD suministrado por el proveedor del hardware o descargue los controladores del sitio web del proveedor. Los archivos de controlador deben tener la extensión *.inf. Si descarga los controladores en el formato *.exe, *.cab o *.zip, extráigalos con una aplicación de terceros.

Se recomienda almacenar los controladores para todo el hardware utilizado en su organización en un mismo depósito, ordenados según el tipo de dispositivo o las configuraciones de hardware. Puede conservar una copia del depósito en un DVD o una unidad de memoria flash; elija algunos controladores y añádalos al dispositivo de arranque; cree un dispositivo de inicio personalizado con los controladores necesarios (y la configuración de red necesaria) para cada uno de sus servidores. O bien, simplemente especifique la ruta al depósito cada vez que utilice Universal Restore.

Compruebe el acceso a los controladores en el entorno de inicio

Asegúrese de tener acceso al dispositivo con controladores cuando trabaje con el dispositivo de arranque. Utilice el dispositivo basado en WinPE si el dispositivo está disponible en Windows, pero el dispositivo basado en Linux no lo detecta.

Configuración de Universal Restore

Búsqueda automática de controladores

Especifique el lugar donde el programa debe buscar los controladores de la capa de abstracción del hardware (HAL), el controlador de disco duro y los adaptadores de red:

- Si los controladores se encuentran en el disco de un proveedor u otro medio extraíble, active la opción **Buscar en medios extraíbles**.
- Si los controladores se encuentran en una carpeta en red o en el dispositivo de arranque, especifique la ruta a la carpeta al hacer clic en **Añadir carpeta**.

Además, Universal Restore buscará la carpeta de almacenamiento de controladores predeterminada de Windows. Su ubicación está determinada en el valor de registro **DevicePath**, que se puede encontrar en la clave de registro

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion. Esta carpeta de almacenamiento generalmente es `WINDOWS\inf`.

Universal Restore ejecutará la búsqueda recursiva en todas las subcarpetas de la carpeta especificada, encontrará los controladores de HAL y de disco duro más apropiados entre todos los que estén disponibles y los instalará en el sistema. Universal Restore también busca el controlador de adaptadores de red y, una vez encontrado, transmite al sistema operativo la ruta de ese controlador. Si el hardware cuenta con varias tarjetas de interfaz de red, Universal Restore intentará configurar los controladores de todas las tarjetas.

Instalar de todos maneras los controladores de los dispositivos de almacenamiento masivo

Necesita este ajuste si:

- El hardware posee un controlador de almacenamiento masivo como RAID (en especial NVIDIA RAID) o un adaptador de canal de fibra.
- Ha migrado un sistema a un equipo virtual que utiliza un controlador de disco duro SCSI. Utilice los controladores SCSI incluidos con el software de virtualización o descargue las últimas versiones de los controladores del sitio web del fabricante del software.
- Si la búsqueda automática de controladores no ayuda a iniciar el sistema.

Especifique los controladores adecuados al hacer clic en **Añadir controlador**. Los controladores definidos aquí se instalarán, con las advertencias adecuadas, incluso si el programa encuentra un controlador mejor.

Proceso de Universal Restore

Después de especificar los ajustes necesarios, haga clic en **Aceptar**.

Si Universal Restore no encuentra un controlador compatible en las ubicaciones especificadas, mostrará un mensaje sobre el dispositivo problemático. Realice uno de los siguientes procedimientos:

- Añada el controlador a cualquiera de las ubicaciones especificadas anteriormente y haga clic en **Reintentar**.
- Si no recuerda la ubicación, haga clic en **Ignorar** para continuar con la recuperación. Si el resultado no es satisfactorio, vuelva a aplicar Universal Restore. Al configurar la operación, especifique el controlador necesario.

Una vez que Windows se inicie, ejecutará el procedimiento estándar para instalar un nuevo hardware. El controlador de adaptadores de red se instalará silenciosamente si el controlador tiene la firma de Microsoft Windows. De lo contrario, Windows solicitará confirmación para instalar el controlador sin firma.

Después, podrá configurar la conexión de red y especificar los controladores para el adaptador de vídeo, USB y otros dispositivos.

6.3.5.2 Universal Restore en Linux

Universal Restore puede aplicarse a los sistemas operativos de Linux con una versión de kernel 2.6.8 o superior.

Cuando Universal Restore se aplica a un sistema operativo de Linux, actualiza un sistema de archivos temporal conocido como el disco RAM inicial (initrd). Esto garantiza que el sistema operativo pueda iniciarse en el nuevo hardware.

Universal Restore añade módulos para el nuevo hardware (incluyendo los controladores de dispositivo) al disco RAM inicial. Como regla general, localiza los módulos necesarios en el directorio **/lib/modules**. Si Universal Restore no puede encontrar un módulo que necesita, registra el nombre de archivo del módulo en el registro.

Universal Restore puede modificar la configuración del cargador de arranque GRUB. Esto puede ser necesario, por ejemplo, para garantizar la capacidad de arranque cuando el nuevo equipo posee una distribución del volumen diferente al equipo original.

Universal Restore nunca modifica el kernel Linux.

Reversión al disco RAM inicial original

Puede revertir al disco RAM inicial original, si fuera necesario.

El disco RAM inicial está almacenado en el equipo en un archivo. Antes de actualizar el disco RAM inicial por primera vez, Universal Restore guarda una copia del mismo en el mismo directorio. El nombre de la copia es el nombre del archivo seguido del sufijo **_acronis_backup.img**. Esta copia no se sobrescribirá si ejecuta Universal Restore más de una vez (por ejemplo, después de añadir controladores faltantes).

Para volver al disco RAM inicial original, realice cualquiera de las siguientes acciones:

- Cambie el nombre de la copia adecuadamente. Por ejemplo, ejecute un comando similar al siguiente:

```
mv initrd-2.6.16.60-0.21-default_acronis_backup.img  
initrd-2.6.16.60-0.21-default
```

- Especifique la copia en la línea **initrd** de la configuración del cargador de inicio GRUB.

6.4 Recuperación de archivos

6.4.1 Recuperación de archivos usando la interfaz web

1. Seleccione el equipo que contenía originalmente los datos que desea recuperar.
2. Haga clic en **Recuperación**.
3. Seleccione el punto de recuperación. Tenga en cuenta que los puntos de recuperación se filtran por ubicación.

Si el equipo seleccionado es físico y no está conectado a Internet, no se muestran los puntos de recuperación. Seleccione un punto de recuperación en la pestaña de copias de seguridad (pág. 93) o use otros métodos de recuperación:

- Descargue los archivos desde el almacenamiento en la nube (pág. 83)
- Use dispositivos de arranque (pág. 84)

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 "Filtros de archivo" (pág. 60).

6. Seleccione los archivos que desea recuperar.
7. Si desea guardar los archivos como 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 es un equipo con un agente o un equipo virtual ESXi).
- El equipo donde está instalado Agente para Hyper-V (si los archivos proceden de un equipo virtual Hyper-V). Los archivos de un equipo virtual Hyper-V no se pueden recuperar en el equipo original.

Este es el equipo de destino para la recuperación. Si es necesario, puede seleccionar otro equipo.

9. [Solo al recuperar en un equipo virtual ESXi] Proporcione las credenciales de un usuario del sistema invitado. El usuario debe pertenecer al grupo de **administradores** de Windows o ser un usuario raíz en Linux.
10. 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
11. Haga clic en **Iniciar recuperación**.
12. Seleccione una de las opciones de sobrescritura de archivos:
 - **Sobrescribir archivos existentes**
 - **Sobrescribir un archivo existente si es más antiguo**
 - **No sobrescribir archivos existentes**

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

6.4.2 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.

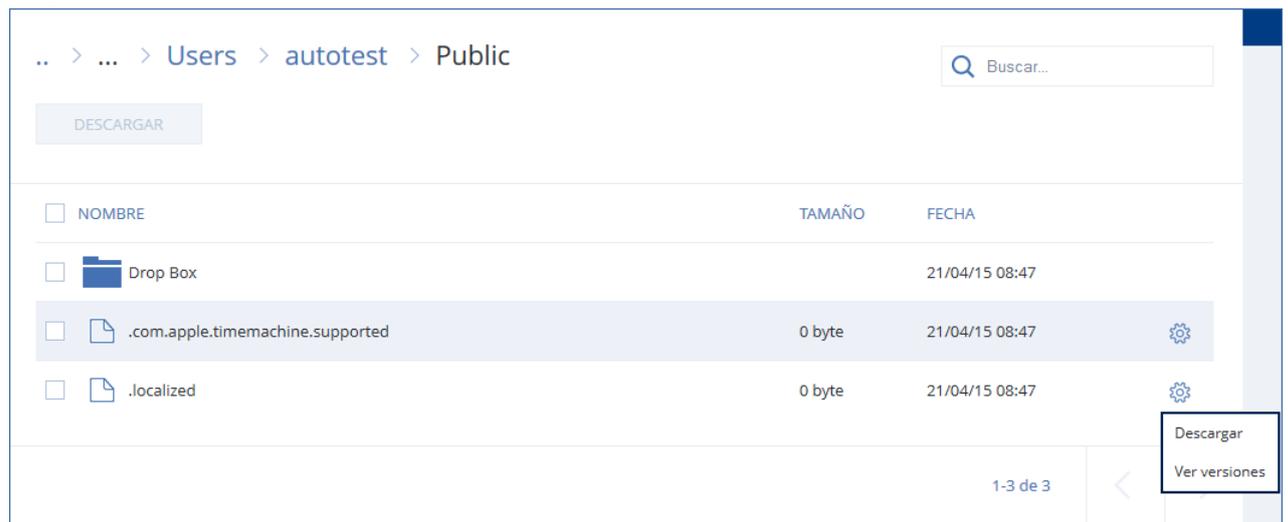
Para descargar archivos del almacenamiento en la nube

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.

| NOMBRE | FECHA | TAMAÑO |
|---|----------------|-----------------|
|  Backup #1 | 03/06/15 04:52 | Tamaño: 1,57 MB |

[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**.

6.4.3 Recuperación de archivos usando dispositivos de arranque

Para obtener información sobre cómo crear dispositivos de arranque, consulte "Crear dispositivos de arranque" (pág. 73).

Para recuperar archivos mediante un dispositivo de arranque

1. Inicie el equipo de destino usando el dispositivo de arranque.
2. Haga doble clic en **Gestionar este equipo a nivel local** o en **Dispositivos de rescate de arranque**, dependiendo del tipo de dispositivo que use.
3. Si en la red hay un servidor proxy habilitado, haga clic en **Herramientas > Servidor proxy** y, a continuación, especifique nombre de servidor/dirección IP y puerto del servidor proxy. De lo contrario, omita este paso.
4. En la pantalla de inicio, haga clic en **Recuperar**.
5. Haga clic en **Seleccionar datos** y después haga clic en **Examinar**.
6. Especifique la ubicación de la copia de seguridad:
 - Para recuperar datos desde un almacenamiento en la cloud, seleccione **Almacenamiento en la cloud**. Especifique las credenciales de la cuenta a la que está asignado el equipo del que se hizo la copia de seguridad.
 - Para recuperar datos desde una carpeta local o de red, vaya a la carpeta ubicada en **Carpetas locales** o **Carpetas de red**.Haga clic en **Aceptar** para confirmar su selección.
7. Seleccione la copia de seguridad desde la que desea recuperar los datos. Si se le pide, escriba la contraseña para la copia de seguridad.
8. En **Contenido de la copia de seguridad**, seleccione **Carpetas/archivos**.
9. Seleccione los datos que desea recuperar. Haga clic en **Aceptar** para confirmar su selección.

10. En **Dónde recuperar**, especifique una carpeta. Opcionalmente, puede prohibir la sobrescritura de versiones de archivos más recientes o excluir algunos archivos de la recuperación.
11. [Opcional] Haga clic en **Opciones de recuperación** para especificar configuraciones adicionales.
12. Haga clic en **Aceptar** para comenzar la recuperación.

6.4.4 Extracción de archivos desde 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, FAT23, NTFS, ReFS, Ext2, Ext3, Ext4, XFS, o HFS+.
- La copia de seguridad debe almacenarse en una carpeta local, en una red compartida (SMB/CIFS) o en Secure Zone (zona segura).

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 incluidos en la copia de seguridad.
5. Busque la carpeta requerida.
6. Copie los archivos requeridos en cualquier carpeta del sistema de archivos.

6.5 Recuperación del estado del sistema

1. Seleccione el equipo para el que desea recuperar el estado del sistema.
2. Haga clic en **Recuperación**.
3. Seleccione un punto de recuperación del estado del sistema. Tenga en cuenta que los puntos de recuperación se filtran por ubicación.
4. Haga clic en **Recuperar el estado del sistema**.
5. Confirme si desea sobrescribir el estado del sistema con su respectiva copia de seguridad.

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

6.6 Recuperación de la configuración de ESXi

Para recuperar una configuración de ESXi, se necesita un dispositivo de arranque basado en Linux. Para obtener información sobre cómo crear dispositivos de arranque, consulte "Crear dispositivos de arranque" (pág. 73).

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.

6.7 Opciones de recuperación

Para modificar las opciones de recuperación, haga clic en **Opciones de recuperación** al configurar la recuperación.

Disponibilidad de las opciones de recuperación

El conjunto de opciones de recuperación disponibles depende de:

- El entorno en el que opera el agente que efectúa la recuperación (Windows, Linux, OS X 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 | OS X | Dispositivo de arranque | ESXi y Hyper-V | Windows |
| Validación de la copia de seguridad (pág. 88) | + | + | + | + | + | + | + | + | + |
| Fecha y hora de los archivos (pág. 88) | - | - | - | + | + | + | + | - | - |
| Manejo de errores (pág. 88) | + | + | + | + | + | + | + | + | + |
| Exclusiones de archivos (pág. 89) | - | - | - | + | + | + | + | - | - |
| Seguridad a nivel de archivo (pág. 89) | - | - | - | + | + | + | + | - | - |
| Flashback (pág. 89) | - | - | - | - | - | - | - | + | - |
| Recuperación de ruta completa (pág. 89) | - | - | - | + | + | + | + | - | - |
| Puntos de montaje (pág. 90) | - | - | - | + | - | - | - | - | - |
| Rendimiento (pág. 90) | + | + | - | + | + | + | - | + | + |
| Comandos previos/posteriores (pág. 90) | + | + | - | + | + | + | - | + | + |
| Cambios en el identificador de seguridad (SID) (pág. 92) | + | - | - | - | - | - | - | - | - |
| Gestión de energía de VM (pág. 92) | - | - | - | - | - | - | - | + | - |

| | Discos | | | Archivos | | | | Equipos virtuales | SQL y Exchange |
|--|---------|-------|-------------------------|----------|-------|------|-------------------------|-------------------|----------------|
| | Windows | Linux | Dispositivo de arranque | Windows | Linux | OS X | Dispositivo de arranque | ESXi y Hyper-V | Windows |
| Registro de eventos de Windows (pág. 92) | + | - | - | + | - | - | - | Solo Hyper-V | + |

6.7.1 Validación de la copia de seguridad

Esta opción define si se valida la copia de seguridad para garantizar que no se corrompió la copia de seguridad, antes de recuperar los datos.

El valor predeterminado: **Deshabilitado**.

La validación calcula una suma de comprobación por cada bloque de datos guardado en la copia de seguridad. La única excepción es la validación de las copias de seguridad a nivel de archivo que se encuentran en el almacenamiento en la nube. Estas copias de seguridad se validan comprobando la coherencia de la metainformación guardada en la copia de seguridad.

La validación lleva bastante tiempo, incluso cuando se trata de copias de seguridad incrementales o diferenciales, que son de pequeño tamaño. Esto se debe a que la operación valida no solo los datos contenidos físicamente en la copia de seguridad, sino también todos los datos recuperables al seleccionar la copia de seguridad. Esto exige acceso a las copias de seguridad creadas anteriormente.

6.7.2 Fecha y hora de los archivos

Esta opción solo sirve al recuperar archivos.

Esta opción define si recuperar la fecha y hora de los archivos a partir de la copia de seguridad o si asignar a los archivos la fecha y hora actuales.

Si esta opción está habilitada, se asignará a los archivos la fecha y hora actuales.

El valor predeterminado es: **Habilitado**.

6.7.3 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.

6.7.4 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*.

6.7.5 Seguridad de nivel de archivo

Esta opción sólo es eficaz para la recuperación desde archivos de Windows de copia de seguridad a nivel de archivo.

Esta opción define si realiza la recuperación de permisos para archivos NTFS junto a los archivos.

El valor predeterminado: **Habilitado**.

Si se preservan los permisos NTFS durante la copia de seguridad (pág. 62), puede elegir entre recuperar los permisos o permitir que los archivos hereden los permisos NTFS de la carpeta desde donde se recuperan.

6.7.6 Flashback

Esta opción funciona cuando Agente para VMware o Agente para Hyper-V realizan la recuperación en un equipo virtual.

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

El valor predeterminado es: **Habilitado**.

6.7.7 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**.

6.7.8 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. 63) habilitada.

El valor predeterminado es: **Deshabilitado**.

Esta opción solo funciona cuando selecciona para la recuperación una carpeta que se encuentra en un nivel superior al punto de montaje en la jerarquía. Si selecciona las carpetas de recuperación dentro del punto de montaje mismo, los elementos seleccionados se recuperarán sin importar el valor de la opción de **Puntos de montaje**.

Nota Tenga en cuenta que si el volumen no está montado en el momento de la recuperación, los datos se recuperarán directamente a la carpeta que había sido el punto de montaje en el momento de la copia de seguridad.

6.7.9 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.

6.7.10 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.

6.7.10.1 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.

6.7.10.2 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.

6.7.11 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.

6.7.12 Gestión de energía de VM

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

Apagar los equipos virtuales de destino al iniciar la recuperación

El valor predeterminado es: **Habilitado**.

La recuperación en un equipo virtual existente no es posible si el equipo está en línea, por lo que este se apaga una vez comenzada la recuperación. Se desconectará a los usuarios de los equipos y se perderán los datos que no se hayan guardado.

Desmarque la casilla de verificación para esta opción si prefiere apagar el equipo virtual antes de la recuperación.

Encienda el equipo virtual de destino cuando haya finalizado la recuperación.

El valor predeterminado es: **Deshabilitado**.

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

6.7.13 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**.

7 Operaciones con copias de seguridad

7.1 Pestaña Copias de seguridad

La pestaña **Copias de seguridad** muestra las copias de seguridad de todos los equipos que se han registrado en el servidor de gestión. Esto incluye equipos fuera de línea y equipos que ya no están registrados.

Las copias de seguridad almacenadas en una ubicación compartida (como un recurso compartido de SMB o NFS) son visibles para todos los usuarios que dispongan del permiso de lectura para dicha ubicación.

En el caso del almacenamiento en la cloud, los usuarios solo tienen acceso a sus propias copias de seguridad. En una implementación de la cloud, un administrador puede ver las copias de seguridad en nombre de cualquier cuenta que pertenezca al mismo grupo y a sus grupos secundarios. Esta cuenta se elige indirectamente en **Equipo desde el cual examinar**. La pestaña **Copias de seguridad** muestra las copias de seguridad de todos los equipos que se han registrado a lo largo de la historia de una misma cuenta, al registrar este equipo.

Las ubicaciones de copia de seguridad que se usan en los planes de copias de seguridad se añaden automáticamente a la pestaña **Copias de seguridad**. Para añadir una carpeta personalizada (por ejemplo, un dispositivo USB extraíble) a la lista de ubicaciones de copia de seguridad, haga clic en **Examinar** y especifique la ruta de la carpeta.

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

1. En la pestaña **Copias de seguridad**, seleccione la ubicación en la que se almacenan las copias de seguridad.

El software muestra todas las copias de seguridad que su cuenta tiene permiso para visualizar en la ubicación seleccionada. Las copias de seguridad se combinan en grupos. Los nombres de los grupos se basan en la siguiente plantilla:

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

2. Seleccione un grupo del que desee recuperar los datos.
3. [Opcional] Haga clic en **Cambiar** junto a **Equipo desde el cual examinar** y, a continuación, seleccione otro equipo. Algunas copias de seguridad solo pueden examinarse mediante agentes específicos. Por ejemplo, debe seleccionar un equipo que ejecute el Agente para SQL para examinar las copias de seguridad de las bases de datos de Microsoft SQL Server.

Importante: Tenga en cuenta que **Equipo desde el cual examinar** es un destino predeterminado para realizar una recuperación desde una copia de seguridad de un equipo físico. Después de seleccionar un punto de recuperación y hacer clic en **Recuperar**, compruebe la configuración de **Equipo de destino** para asegurarse de que desea recuperar en este equipo determinado. Para cambiar el destino de recuperación, especifique otro equipo en **Equipo desde el cual examinar**.

4. Haga clic en **Mostrar copias de seguridad**.
5. Seleccione el punto de recuperación.

7.2 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.

7.3 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 copia de seguridad que desea eliminar y, a continuación, haga clic en el icono de la papelera de reciclaje.
 - 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 copia de seguridad que desea eliminar y, a continuación, haga clic en el icono de la papelera de reciclaje.
 - Para eliminar el grupo seleccionado, haga clic en **Eliminar**.
4. Confirme su decisión.

8 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.

9 Bootable Media Builder

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

Bootable Media Builder se instala de forma predeterminada al instalar el servidor de gestión. Puede instalar Media Builder por separado o en cualquier equipo que ejecute Windows o Linux. Los sistemas operativos compatibles son los mismos que para los agentes correspondientes.

¿Por qué utilizar Media Builder?

El dispositivo de arranque disponible para su descarga en la consola de copia de seguridad solo se puede utilizar para recuperación. Este medio se basa en un kernel Linux. A diferencia de Windows PE, no permite inyectar controladores personalizados sobre la marcha.

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

¿32 o 64 bits?

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

Recuerde que en la mayoría de los casos, necesitará un medio de 64 bits para arrancar un equipo que utiliza la interfaz extensible del firmware unificada (UEFI).

9.1 Dispositivos de arranque basados en Linux

Para crear un dispositivo de arranque basado en Linux

1. Inicie Bootable Media Builder.
2. Especifique la clave de licencia. La licencia no se asignará ni volverá a asignarse. Determina la funcionalidad que se habilitará en el medio creado. Sin las claves de licencia, solo podrá crear medios para recuperación.

3. Seleccione **Tipo de dispositivo de arranque: Predeterminado (dispositivo de arranque basado en Linux)**.

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

- Un dispositivo con un manejo de volúmenes estilo Linux muestra los volúmenes como, por ejemplo, hda1 y sdb2. Intenta reconstruir los dispositivos MD y los volúmenes lógicos (LVM) antes de comenzar una recuperación.
- Un dispositivo con un manejo de volúmenes estilo Windows muestra los volúmenes como, por ejemplo, C: y D: Proporciona acceso a los volúmenes dinámicos (LDM).

4. [Opcional] Especifique los parámetros del kernel Linux. Separe los diferentes parámetros con espacios.

Por ejemplo, para poder seleccionar un modo de visualización para el agente de arranque cada vez que se inicia el dispositivo, escriba: **vga=ask**

Para obtener una lista de parámetros, consulte Parámetros del kernel (pág. 98).

5. Seleccione los componentes que se ubicarán en el medio: el agente de arranque y/o Universal Restore.

Utilizando un medio con el agente de arranque, puede realizar operaciones de copia de seguridad, recuperación y gestión del disco en cualquier hardware compatible con PC, incluyendo recuperación de cero.

Universal Restore le permite arrancar un sistema operativo recuperado en un hardware diferente o en un equipo virtual si hay problemas con la capacidad de arranque del sistema. La herramienta localiza e instala los controladores de dispositivos que son críticos para el inicio del sistema operativo, como los controladores de almacenamiento, placa madre o conjunto de chips.

6. [Opcional] Especifique el intervalo de tiempo de espera para el menú de arranque además del componente que se iniciará automáticamente en el tiempo de espera.

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

Si configura, por ejemplo, **10 s** para el agente de arranque el agente se iniciará 10 segundos después de que se muestre el menú. Esto habilita el funcionamiento in situ sin interacción al arrancar desde WDS/RIS.

7. [Opcional] Especifique la configuración de inicio de sesión remota: el nombre de usuario y la contraseña que se deben especificar en una cadena de comando si la utilidad **acrocmbd** se instala en un equipo distinto. Si deja estas casillas sin marcar, no es necesario que el comando contenga credenciales.

8. [Opcional] Especifique la configuración de red (pág. 99): La configuración TCP/IP que será asignada a los adaptadores de red del equipo.

9. [Opcional] Especifique un puerto de red (pág. 100): El puerto TCP que el agente de arranque escucha para las conexiones entrantes.

10. [Opcional] Si hay un servidor proxy habilitado en la red, especifique su nombre de servidor/dirección IP y puerto.

11. Seleccione el tipo de dispositivo que desea crear. Puede:

- Crear CD, DVD u otro dispositivo de arranque, como una unidad de memoria flash USB, si la BIOS del hardware permite el arranque desde tales dispositivos.
- Crear una imagen ISO para grabarla posteriormente en un disco vacío o conectarla a un equipo virtual.
- Cargar los componentes seleccionados en WDS/RIS.

12. [Opcional] Añadir controladores del sistema Windows que usará Universal Restore (pág. 100). Esta ventana aparece si se añade Universal Restore al medio y se selecciona otro medio que no sea WDS/RIS.
13. Si así se le indica, especifique el nombre del servidor/dirección IP y las credenciales de WDS/RIS, o una ruta al archivo ISO del medio.
14. Compruebe su configuración en la pantalla de resumen y haga clic en **Continuar**.

9.1.1 Parámetros de kernel

Esta ventana le permite especificar uno o más parámetros del kernel de Linux. Se aplicarán automáticamente cuando se ejecute el dispositivo de arranque.

Estos parámetros se utilizan comúnmente cuando hay problemas mientras se trabaja con el dispositivo de arranque. Normalmente, puede dejar este campo vacío.

También puede especificar cualquiera de estos parámetros pulsando F11 mientras está en el menú de inicio.

Parámetros

Cuando especifique varios parámetros, sepárelos con espacios.

acpi=desactivada

Desactiva la interfaz de alimentación de configuración avanzada (ACPI). Puede utilizar este parámetro cuando experimente problemas con la configuración de un hardware en particular.

noapic

Desactiva el Controlador de interrupciones programable avanzado (APIC). Puede utilizar este parámetro cuando experimente problemas con la configuración de un hardware en particular.

vga=ask

Solicita que seleccione el modo de video que utilizará la interfaz gráfica de usuario del dispositivo de arranque. Sin el parámetro **vga**, el modo vídeo se detecta automáticamente.

vga=mode_number

Especifica el modo de video que utilizará la interfaz gráfica de usuario del dispositivo de arranque. El número de modo aparece en *mode_number* en formato hexadecimal, por ejemplo: **vga=0x318**. La resolución de la pantalla y el número de colores correspondiente a un número de modo puede ser diferente en equipos diferentes. Recomendamos utilizar primero el parámetro **vga=ask** para seleccionar un valor para *mode_number*.

silencio

Desactiva la muestra de mensajes de inicio cuando el kernel de Linux se está cargando y ejecuta la consola de gestión una vez que el kernel está cargado.

Este parámetro está especificado implícitamente cuando crea el dispositivo de arranque, pero puede borrar este parámetro mientras esté en el menú de inicio.

Sin este parámetro, se mostrarán todos los mensajes de inicio, seguidos de una entrada de comandos. Para iniciar la consola de gestión desde la entrada de comandos, ejecute el comando: **/bin/product**

nousb

Desactiva la carga del subsistema del USB (bus universal en serie).

nousb2

Desactiva la compatibilidad con USB 2.0. No obstante, los dispositivos USB 1.1 trabajan con este parámetro. Este parámetro le permite utilizar algunas unidades USB en el modo USB 1.1 si no funcionan en el modo USB 2.0.

nodma

Desactiva el acceso directo a memoria (DMA) para todas las unidades del disco duro IDE. Evita que el kernel se congele en algún hardware.

nofw

Desactiva la compatibilidad con la interfaz de FireWire (IEEE1394).

nopcmcia

Desactiva la detección del hardware PCMCIA.

nomouse

Desactiva la compatibilidad con el ratón.

module_name=desactivado

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

pci=bios

Obliga al uso de PCI BIOS en vez de acceder directamente al dispositivo del hardware. Es conveniente que utilice este parámetro si el equipo tiene un puente PCI no estándar de host.

pci=nobios

Desactiva el uso de PCI BIOS; solo se pueden utilizar métodos de acceso directo al hardware. Es conveniente que utilice este parámetro cuando el dispositivo de arranque no puede iniciarse, lo que puede deberse a la BIOS.

pci=biosirq

Utiliza las alertas PCI BIOS para obtener la tabla de rutas de interrupción. Es conveniente que utilice este parámetro si el kernel no puede asignar solicitudes de interrupción (IRQ) o descubrir enlaces secundarios de PCI en la placa madre.

Estas llamadas pueden no funcionar correctamente en algunos equipos. Pero puede ser la única manera de obtener la tabla de rutas de interrupción.

9.1.2 Configuraciones de red

Mientras crea el dispositivo de arranque, tiene la opción de preconfigurar las conexiones de red que usará el agente de arranque. Se pueden preconfigurar los siguientes parámetros:

- Dirección IP
- Máscara de subred
- Puertas de enlace
- Servidor DNS
- Servidor WINS.

Una vez que se inicia el agente de arranque en un equipo, se aplica la configuración en la tarjeta de interfaz de red (NIC) del equipo. Si no se preconfiguran las configuraciones, el agente usa la

configuración automática del servidor DHCP. También tiene la capacidad de establecer manualmente la configuración de red cuando se ejecuta el agente de arranque en el equipo.

Preconfiguración de múltiples conexiones de red

Puede preestablecer la configuración TCP/IP en hasta 10 tarjetas de interfaz de red. Para asegurar que cada NIC tendrá asignada la configuración adecuada, cree el dispositivo en el servidor en donde se personalizan los dispositivos. Cuando seleccione la NIC existente en la ventana del asistente, se selecciona su configuración para guardarla en el dispositivo. También se guarda la dirección MAC de cada NIC en los dispositivos.

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

Una vez que el dispositivo de arranque se ejecute en el servidor, recupera la lista de NIC disponibles. Esta lista está ordenada por las ranuras que ocupan las NIC: las más cercanas al procesador están en la parte superior.

El agente de arranque asigna la configuración apropiada a cada NIC conocida y las identifica por sus direcciones MAC. Después de que se configuran las NIC con direcciones MAC conocidas, se asigna la configuración que realizó para NIC no existentes a las NIC restantes, comenzando por la NIC no asignada superior.

Puede personalizar los dispositivos de arranque para cualquier equipo, y no sólo para el equipo en donde se crea el dispositivo. Para hacerlo, configure las NIC de acuerdo con el orden de ranuras de la unidad del equipo: NIC1 ocupa la ranura más cercana al procesador, NIC2 es la siguiente ranuras de la unidad y así sucesivamente. Cuando el agente de arranque se ejecuta en el equipo, no encontrará NIC con direcciones MAC conocidas y configurará las NIC en el mismo orden que usted.

Ejemplo

El agente de arranque podría usar uno de los adaptadores de red para la comunicación con la consola de gestión por medio de la red productiva. Se podría establecer la configuración automática para esta conexión. Se pueden transferir los datos que se pueden dividir para su recuperación por la segunda NIC, incluida en la red de copia de seguridad por medio de la configuración TCP/IP.

9.1.3 Puerto de red

Cuando crea un dispositivo de arranque, tiene la opción de preconfigurar el puerto de red que el agente de arranque escuchará para la conexión entrante desde la utilidad **acrocnd**. Puede elegir entre:

- el puerto predeterminado
- el puerto usado actualmente
- el puerto nuevo (introduzca el número de puerto)

Si no se preconfiguró el puerto, el agente usa el puerto 9876.

9.1.4 Controladores para Universal Restore

Cuando crea dispositivos de arranque, tiene la opción de añadir controladores de Windows al dispositivo. Universal Restore utilizará los controladores para arrancar el sistema operativo Windows migrado a un hardware diferente.

Entonces podrá configurar Universal Restore:

- para buscar los controladores en los dispositivos que mejor se ajustan al hardware de destino
- para obtener los controladores de almacenamiento masivo que especifica desde el dispositivo. Esto debe hacerse cuando el hardware de destino tiene el controlador para almacenamiento masivo (como adaptador SCSI, RAID, o Fiber Channel) para el disco duro.

Los controladores serán ubicados en la carpeta de controladores visibles en el dispositivo de arranque. No se cargan los controladores en la memoria RAM del equipo de destino, por lo que el dispositivo debe estar insertado o conectado por medio de la operación de Universal Restore.

Puede agregar controladores a un dispositivo de arranque cuando crea un dispositivo extraíble o su ISO o medio extraíble, como una unidad flash. Los controladores no se pueden cargar en WDS/RIS.

Se pueden agregar los controladores a la lista sólo en grupos, al agregar los archivos INF o carpetas que contienen dichos archivos. La selección de controladores individuales desde los archivos INF no es posible, pero Media Builder muestra el contenido del archivo para su información.

Para agregar unidades:

1. Haga clic en **Añadir** y navegue hasta el archivo INF o la carpeta que contiene los archivos INF.
2. Seleccione el archivo INF o la carpeta.
3. Haga clic en **Aceptar**.

Se pueden eliminar los controladores de la lista sólo en grupos, al eliminar los archivos INF.

Para eliminar los controladores:

1. Seleccione el archivo INF.
2. Haga clic en **Quitar**.

9.2 Dispositivos de arranque basados en WinPE

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

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

Bootable Media Builder es compatible con las distribuciones de WinPE que están basadas en cualquiera de los siguientes kernels:

- Windows Vista (PE 2.0)
- Windows Vista SP1 y Windows Server 2008 (PE 2.1)
- Windows 7 (PE 3.0) con o sin el complemento para Windows 7 SP1 (PE 3.1)
- Windows 8 (PE 4.0)
- Windows 8.1 (PE 5.0)
- Windows 10 (PE para Windows 10)

Bootable Media Builder es compatible con las distribuciones de 32 bits y 64 bits de WinPE. Las distribuciones de 32 bits de WinPE también funcionan en hardware de 64 bits. Sin embargo, necesita una distribución de 64 bits para arrancar un equipo que utiliza la interfaz extensible del firmware unificada (UEFI).

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

9.2.1 Preparación: WinPE 2.x y 3.x

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

Para preparar un equipo con AIK

1. Descargue e instale Windows Automated Installation Kit.
Automated Installation Kit (AIK) para Windows Vista (PE 2.0):
<http://www.microsoft.com/Downloads/details.aspx?familyid=C7D4BC6D-15F3-4284-9123-679830D629F2&displaylang=es>
Automated Installation Kit (AIK) para Windows Vista SP1 y Windows Server 2008 (PE 2.1):
<http://www.microsoft.com/downloads/details.aspx?FamilyID=94bb6e34-d890-4932-81a5-5b50c657de08&DisplayLang=es>
Automated Installation Kit (AIK) para Windows 7 (PE 3.0):
<http://www.microsoft.com/DOWNLOADS/details.aspx?familyid=696DD665-9F76-4177-A811-39C26D3B3B34&displaylang=es>
Complemento de Automated Installation Kit (AIK) para Windows 7 SP1 (PE 3.1):
<http://www.microsoft.com/es-es/download/details.aspx?id=5188>
Puede encontrar los requisitos del sistema para la instalación en los siguientes enlaces.
2. [Opcional] Grabe el WAIK en un DVD o cópielo en una unidad de memoria flash.
3. Instale Microsoft .NET Framework desde este kit (NETFXx86 o NETFXx64, según su hardware).
4. Instale el analizador de Microsoft Core XML (MSXML) 5.0 o 6.0 de este kit.
5. Instale Windows AIK de este kit.
6. Instale Bootable Media Builder en el mismo equipo.

Es recomendable que se familiarice con la documentación de ayuda suministrada con Windows AIK. Para tener acceso a la documentación, seleccione **Microsoft Windows AIK -> Documentación** desde el menú de inicio.

9.2.2 Preparación: WinPE 4.0 y posterior

Para poder crear o modificar las imágenes de PE 4 o posterior, instale Bootable Media Builder en un equipo que tenga instalado Windows Assessment and Deployment Kit (ADK). Si no tiene un equipo con ADK, prepárelo de la siguiente manera:

Para preparar un equipo con ADK

1. Descargue el programa de instalación de Assessment and Deployment Kit.
Assessment and Deployment Kit (ADK) para Windows 8 (PE 4.0):
<http://www.microsoft.com/es-es/download/details.aspx?id=30652>.
Assessment and Deployment Kit (ADK) para Windows 8.1 (PE 5.0):
<http://www.microsoft.com/es-ES/download/details.aspx?id=39982>.
Assessment and Deployment Kit (ADK) para Windows 10 (PE para Windows 10):
<https://msdn.microsoft.com/es-es/windows/hardware/dn913721%28v=vs.8.5%29.aspx>.
Puede encontrar los requisitos del sistema para la instalación en los enlaces anteriores.
2. Instale Assessment and Deployment Kit en el equipo.
3. Instale Bootable Media Builder en el mismo equipo.

9.2.3 Incorporación del complemento de Acronis a WinPE

Para incorporar el complemento de Acronis a WinPE:

1. Inicie Bootable Media Builder.
2. Especifique las claves de licencia. Las claves de licencia no se asignarán ni volverán a asignarse. Determinan la funcionalidad que se habilitará para el dispositivo creado. Sin las claves de licencia, solo podrá crear medios para recuperación.
3. Seleccione **Tipo de dispositivo de arranque: Windows PE** o **Tipo de dispositivo de arranque: Windows PE (64 bits)**. Se necesita un dispositivo de 64 bits para arrancar un equipo que utiliza la interfaz extensible del firmware unificada (UEFI).

Si ha seleccionado **Tipo de dispositivo de arranque: Windows PE**, primero realice lo siguiente:

 - Haga clic en **Descargar complemento para WinPE (32 bits)**.
 - Guarde el complemento en **%PROGRAM_FILES%\Acronis\BootableComponents\WinPE32**.

Si tiene previsto recuperar un sistema operativo en un hardware diferente o en un equipo virtual y desea asegurar la capacidad de arranque del sistema, seleccione la casilla de verificación **Incluir la herramienta Universal Restore...**
4. Seleccione **Crear WinPE automáticamente**.

El software ejecuta la secuencia de comandos apropiada y continúa en la siguiente ventana.
5. Seleccione si desea habilitar o deshabilitar la conexión remota a un equipo que se arranca desde el medio. Si se habilita, introduzca un nombre de usuario y una contraseña para que se puedan especificar en una línea de comando si la utilidad **acrocmd** se ejecuta en un equipo distinto. Si deja estas casillas vacías, la conexión remota se deshabilitará.
6. Especifique las configuraciones de red (pág. 99) de los adaptadores de red del equipo o elija la configuración automática DHCP.
7. [Opcional] Especifique los controladores de Windows que se deben añadir a Windows PE.

Cuando haya iniciado su equipo en Windows PE, los controladores le ayudarán a acceder al dispositivo donde está ubicada la copia de seguridad. Añada los controladores de 32 bits si utiliza una distribución de 32 bits de WinPE o controladores de 64 bits si utiliza una distribución de 64 bits de WinPE.

Además, podrá apuntar a los controladores añadidos al configurar Universal Restore para Windows. Para utilizar Universal Restore, añada los controladores de 32 bits o 64 bits según esté planificando recuperar un sistema operativo de Windows de 32 bits o 64 bits.

Para añadir los controladores:

 - Haga clic en **Añadir** y especifique la ruta al archivo *.inf necesario para el correspondiente controlador SCSI, RAID o SATA, adaptador de red, unidad de cinta u otro dispositivo.
 - Repita este procedimiento para cada controlador que desee incluir en el medio WinPE resultante.
8. Escoja si desea crear una imagen ISO o WIM o cargar el medio en un servidor (WDS o RIS).
9. Especifique la ruta completa al archivo de imagen que se obtendrá incluyendo el nombre del archivo o especifique el servidor y proporcione el nombre de usuario y la contraseña para acceder a él.
10. Compruebe su configuración en la pantalla de resumen y haga clic en **Continuar**.
11. Grabe el .ISO en un CD o DVD con una herramienta de otra empresa o cópielo en una unidad flash.

Una vez que el equipo se inicia en WinPE, el agente se inicia automáticamente.

Para crear una imagen PE (archivo ISO) del archivo WIM resultante:

- Reemplace el archivo boot.wim predeterminado en su carpeta de Windows PE junto al archivo WIM creado recientemente. Para el ejemplo anterior, escriba:

```
copy c:\AcronisMedia.wim c:\winpe_x86\ISO\sources\boot.wim
```

- Use la herramienta **Oscdimg**. Para el ejemplo anterior, escriba:

```
oscdimg -n -bc:\winpe_x86\etfsboot.com c:\winpe_x86\ISO  
c:\winpe_x86\winpe_x86.iso
```

No copie y pegue este ejemplo. Introduzca el comando manualmente o de lo contrario fallará.

Para obtener más información sobre cómo personalizar Windows PE 2.x y 3.x, consulte el manual de usuario de Entorno de preinstalación de Windows (Winpe.chm). La información acerca de la personalización de Windows PE 4.0 y posterior está disponible en la biblioteca Microsoft TechNet.

10 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.

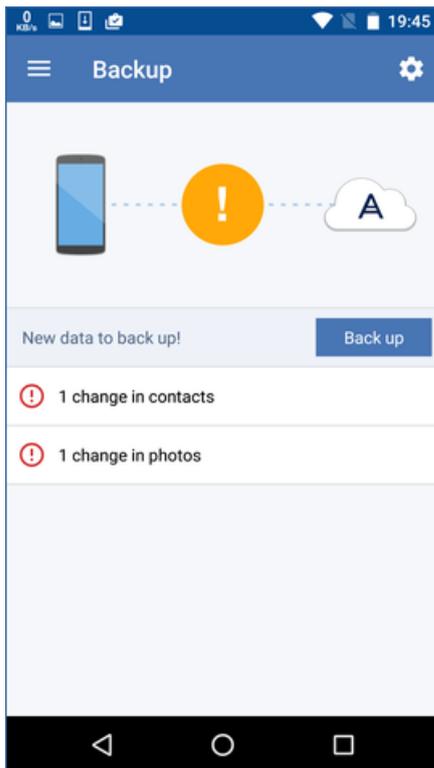
De qué puede realizar una copia de seguridad

- 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 dicha 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 recuperados se guardarán en el almacenamiento interno, independientemente de si los datos originales estaban ubicados en el almacenamiento interno del dispositivo o en la tarjeta SIM.

Instrucciones paso a paso

Para obtener la aplicación de copia de seguridad

1. En un dispositivo móvil, abra un explorador y vaya a <https://backup.acronis.com/>.
2. Inicie sesión con la cuenta Acronis.
3. Haga clic en **Todos los dispositivos > Añadir**.
4. En **Dispositivos móviles**, seleccione el tipo de dispositivo.
Según el tipo de dispositivo, es posible que sea redirigido a App Store o Google Play.
5. [Solo en dispositivos iOS] Haga clic en **Obtener**.
6. Haga clic en **Instalar** para instalar la aplicación de copias de seguridad.

Para iniciar una copia de seguridad de un dispositivo iOS

1. Abra la aplicación de copias de seguridad.
2. Inicie sesión con la cuenta Acronis.
3. Seleccione las categorías de datos de las que desea realizar la copia de seguridad. De manera predeterminada, se seleccionan todas las categorías.
4. Pulse **Crear copia de seguridad ahora**.
5. Permita a la aplicación acceder a sus datos personales. Si deniega el acceso a algunas categorías de datos, estas no se incluirán en la copia de seguridad.

La copia de seguridad comienza.

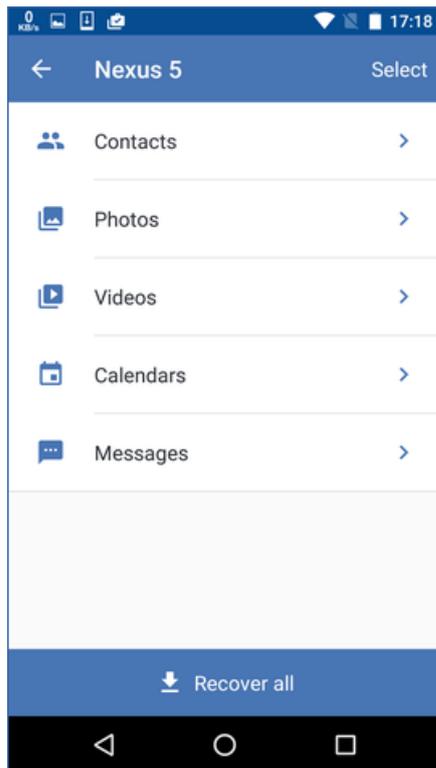
Para iniciar una copia de seguridad de un dispositivo Android

1. Abra la aplicación de copias de seguridad.
2. Inicie sesión con la cuenta Acronis.
3. [Solo en dispositivos Android 6.0 y posterior] Permita a la aplicación acceder a sus datos personales. Si deniega el acceso a algunas categorías de datos, estas no se incluirán en la copia de seguridad.
4. [Opcional] Seleccione las categorías de datos que no desea incluir en la copia de seguridad. Para ello, pulse el icono de engranaje, después el control deslizante de las categorías de datos que desea excluir de la copia de seguridad y, finalmente, la flecha atrás.
5. Pulse **Crear copia de seguridad**.

Para recuperar los datos en un dispositivo móvil

1. Abra la aplicación de copias de seguridad.
2. Deslice el dedo hacia la derecha y, después, pulse **Acceso y recuperación**.
3. Pulse el nombre del dispositivo.
4. Realice uno de los siguientes procedimientos:
 - Para recuperar todos los datos incluidos en la copia de seguridad, pulse **Recuperar todos**. No es necesario realizar más acciones.
 - Para recuperar una o más categorías de datos, pulse **Seleccionar** y después seleccione las casillas de verificación de las categorías elegidas. Pulse **Recuperar**. No es necesario realizar más acciones.

- Para recuperar uno o más elementos que pertenecen a la misma categoría de datos, pulse la categoría de datos concreta. Continúe a los pasos siguientes.



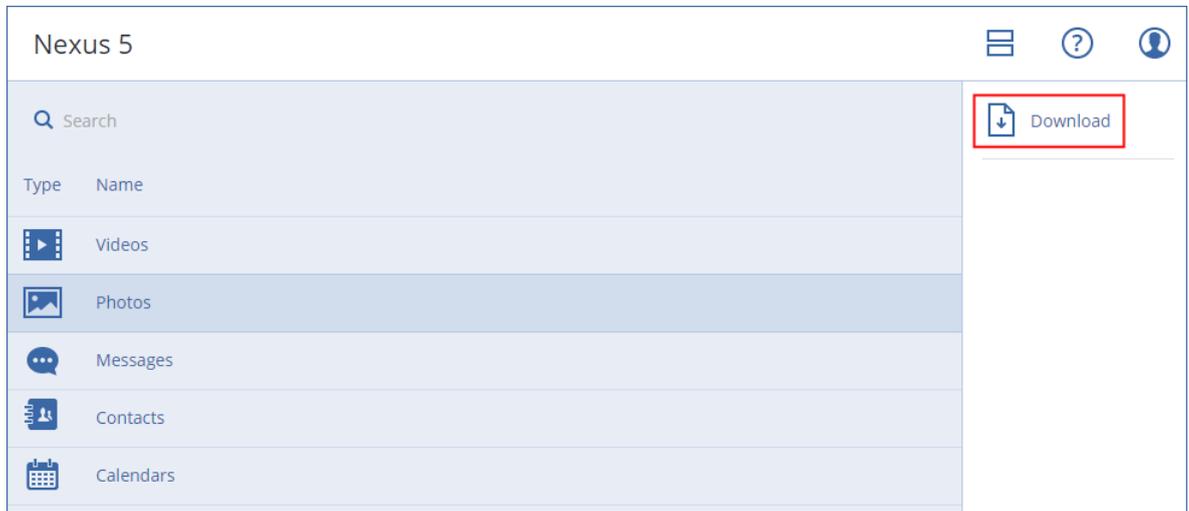
5. Realice uno de los siguientes procedimientos:
 - Para recuperar un único elemento, púlselo.
 - Para recuperar varios elementos, pulse **Seleccionar** y después seleccione las casillas de verificación de los elementos elegidos.



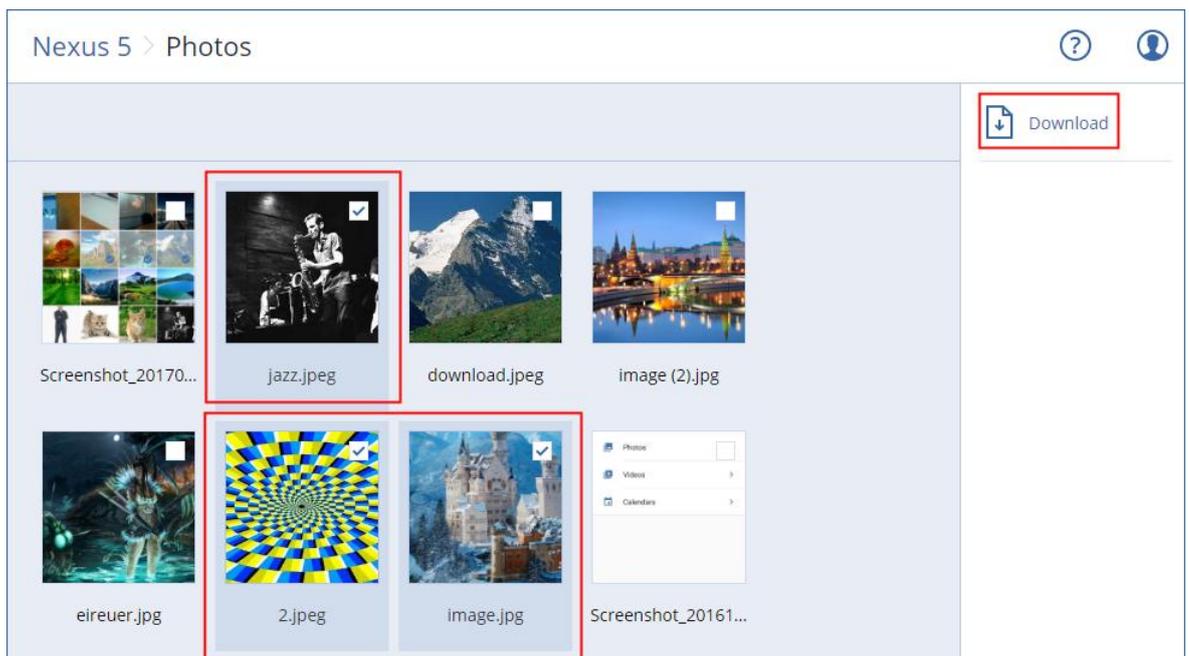
6. Pulse **Recuperar**.

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

1. En un equipo, abra un explorador y vaya a <https://backup.acronis.com/>.
2. Inicie sesión con la cuenta Acronis.
3. En **Todos los dispositivos**, seleccione el nombre de su dispositivo móvil y, a continuación, haga clic en **Recuperación**.
4. Seleccione el punto de recuperación.
5. Realice una de las siguientes operaciones:
 - Para descargar todas las fotografías, todos los vídeos o contactos, seleccione las categorías de datos correspondientes. Haga clic en **Descargar**.



- Para descargar fotografías, vídeos o contactos uno a uno, seleccione el nombre de la categoría de datos correspondiente y, después, seleccione las casillas de verificación de los elementos elegidos. Haga clic en **Descargar**.



- Para ver una vista preliminar de un mensaje de texto, una fotografía o un contacto, seleccione el nombre de la categoría de datos correspondiente y, después, haga clic en el elemento elegido.

Para obtener más información, consulte <https://docs.acronis.com/mobile-backup>. Esta ayuda también está disponible en la aplicación de copia de seguridad (pulse **Configuración** > **Ayuda** en el menú de la aplicación para dispositivos móviles).

11 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. 114) Bases de datos como archivos (pág. 114) | Todo el equipo (pág. 74) Bases de datos a una instancia activa de SQL Server (pág. 114) Bases de datos como archivos (pág. 114) | Todo el equipo (pág. 74) |
| Microsoft Exchange Server | Bases de datos a un servidor activo de Exchange (pág. 117) Bases de datos como archivos (pág. 117) Recuperación granular en un servidor activo de Exchange (pág. 119) | Todo el equipo (pág. 74) Bases de datos a un servidor activo de Exchange (pág. 117) Bases de datos como archivos (pág. 117) Recuperación granular en un servidor activo de Exchange (pág. 119) | Todo el equipo (pág. 74) |
| Servidores de bases de datos de Microsoft SharePoint | Bases de datos a una instancia activa de SQL Server (pág. 114) Bases de datos como archivos (pág. 114) Recuperación granular mediante SharePoint Explorer | Todo el equipo (pág. 74) Bases de datos a una instancia activa de SQL Server (pág. 114) Bases de datos como archivos (pág. 114) Recuperación granular mediante SharePoint Explorer | Todo el equipo (pág. 74) |
| Servidor web front-end de Microsoft SharePoint | - | - | Todo el equipo (pág. 74) |
| Servicios de dominio de Active Directory | - | Todo el equipo (pág. 74) | - |

11.1 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.
- SQL Server Browser Service y el protocolo TCP/IP estén habilitados. Para obtener instrucciones sobre cómo iniciar SQL Server Browser Service, consulte: <https://msdn.microsoft.com/es-es/library/ms189093.aspx>. Puede habilitar el protocolo TCP/IP al utilizar un procedimiento similar.
- El escritor de SQL para VSS esté activado.

En Microsoft Exchange Server, asegúrese de que:

- Se haya iniciado el servicio del almacén de información de Microsoft Exchange.
- Windows PowerShell esté instalado. En Exchange 2010 o posterior, la versión de Windows PowerShell debe ser, como mínimo, 2.0.
- Microsoft .NET Framework esté instalado.

En Exchange 2007, la versión de Microsoft .NET Framework debe ser, como mínimo, 2.0.

En Exchange 2010 o posterior, la versión de Microsoft .NET Framework debe ser, como mínimo, 3.5.

- El escritor de Exchange para VSS está activado.

En un controlador de dominio, asegúrese de que:

- El escritor de Active Directory para VSS esté activado.

Al crear un plan de copias de seguridad, asegúrese de que:

- En los equipos físicos, la opción de copia de seguridad Volume Shadow Copy Service (VSS) (pág. 71) esté habilitada.
- En los equipos virtuales, la opción de copia de seguridad Volume Shadow Copy Service (VSS) para equipos virtuales (pág. 72) 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-60/index.jsp?topic=%2Fcom.vmware.vddk.pg.doc%2FvddkBackupVadp.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.

11.2 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. 110).

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. 42).

11.2.1 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. 63).

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.

11.2.2 Seleccionar datos de Exchange Server

La siguiente tabla resume los datos de Microsoft Exchange Server que puede seleccionar para realizar la copia de seguridad y los permisos de usuario mínimos requeridos para realizar la copia de seguridad de los datos.

| Versión de Exchange | Elementos de los datos | Permisos de usuario |
|---------------------|--------------------------|---|
| 2007 | Grupos de almacenamiento | Asociación en el grupo de funciones Administradores de la organización de Exchange . |
| 2010/2013/2016 | Bases de datos | Asociación en el grupo de funciones Gestión de organización . |

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 Agent for 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**.

11.3 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. 63). Los registros de transacción de Exchange solo se truncan en los equipos virtuales. Puede habilitar la opción de copia de seguridad completa de VSS (pág. 71) 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. 110) y "Derechos de usuario necesarios" (pág. 114) se recogen otros requisitos.

11.3.1 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.

11.4 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 recuperar bases de datos en un equipo que no tiene instalado el Agente para SQL o si necesita extraer datos para búsquedas y minería de datos, control o procesos futuros 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. 116).

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. 116).

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. 93).

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 otro equipo u otra instancia de SQL Server 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**.

11.4.1 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.

11.4.2 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**.

11.5 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 | Asociación en el grupo de funciones Gestión de organización . |

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. 118).

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. 93).

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**.

11.5.1 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](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](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](http://technet.microsoft.com/es-es/library/aa998871(v=EXCHG.80).aspx)

11.6 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.

11.6.1 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. 93).

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, facilite las credenciales de una cuenta que pertenezca al grupo de roles **Gestión de la organización**.
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**.

11.6.2 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. 93).

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.

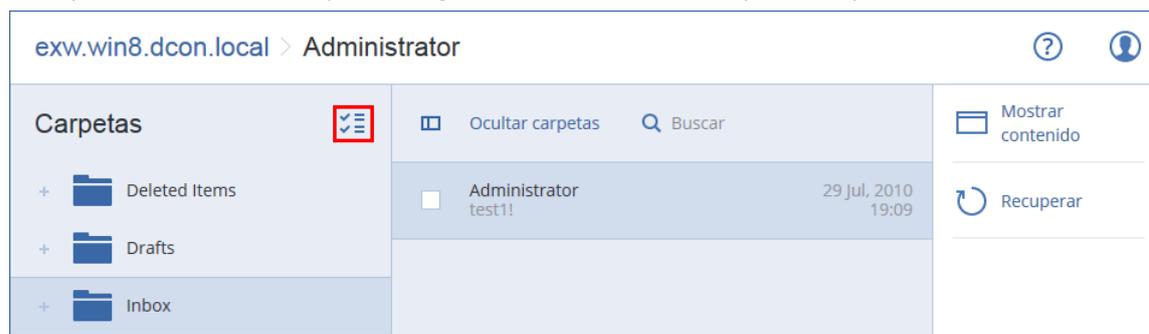
Tiene a su disposición las siguientes opciones de búsqueda. No se pueden usar caracteres comodín.

- 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**.

- 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, facilite las credenciales de una cuenta que pertenezca al grupo de roles **Gestión de la organización**.

- 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.

- Haga clic en **Iniciar recuperación**.

- Confirme su decisión.

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

12 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?

Para realizar copias de seguridad y recuperar buzones de correo de Office 365, debe tener el rol de administrador global en Microsoft Office 365.

Instale el Agente para Office 365 en un equipo que ejecute Windows y esté conectado a Internet. Solo puede haber un Agente para Office 365 en una organización. En el caso de las implementaciones en la cloud, el agente debe estar registrado en la cuenta de administrador del nivel más alto (administrador de cliente).

- En el caso de las implementaciones en la cloud, indique las credenciales del administrador de cliente durante la instalación del agente y al iniciar sesión en la interfaz web.
- Indique las credenciales del administrador global de Office 365 en la página **Microsoft Office 365** de la interfaz web.

El agente iniciará sesión en Office 365 usando esta cuenta. Para permitir que el agente acceda al contenido de los buzones de correo, se asignará el rol de gestión **ApplicationImpersonation** a esta cuenta.

¿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.

12.1 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. 42).

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**.

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

12.2.1 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. 93) 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**.

12.2.2 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. 93) 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.

13 Operaciones avanzadas con equipos virtuales

13.1 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.

13.1.1 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. 93).
2. Haga clic en **Ejecutar como VM**.

El software selecciona automáticamente el servidor y otros parámetros necesarios.

| |
|--|
| <p>EQUIPO DE DESTINO ABR11MMS_temp en 10.250.151.182</p> |
| <p>ALMACÉN DE DATOS datastore-share-iscsi-bender</p> |
| <p>CONFIGURACIÓN DE VM Memoria: 1.00 GB Adaptadores de red: 0</p> |
| <p>ESTADO DE ENERGÍA Activado ▼</p> |
| <p>EJECUTAR AHORA</p> |

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.

13.1.2 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.

13.1.3 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.

13.2 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. 131) 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. 129)

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. 130)

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.

13.2.1 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. 131).
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:

13.2.2 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.

13.2.3 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. 130)
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. 130)
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. 131)
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.

13.2.3.1 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.

13.2.3.2 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**.

13.2.3.3 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. 132).
7. Haga clic en **Iniciar recuperación**.
8. Confirme su decisión.

13.2.4 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. 58).

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. 59).

Comandos previos/posteriores

Esta opción se parece a la opción de copia de seguridad "Comandos previos/posteriores" (pág. 66).

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. 72).

13.2.5 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. 88).

Rendimiento

Esta opción se parece a la opción de recuperación "Rendimiento" (pág. 90).

Comandos pre/post

Esta opción se parece a la opción de recuperación "Comandos pre/post" (pág. 90).

Gestión de energía de VM

Esta opción se parece a la opción de recuperación "Gestión de energía de VM" (pág. 92).

13.2.6 Recopilación de una réplica inicial

Para acelerar la replicación en una ubicación remota y ahorrar ancho de banda en la red, puede realizar recopilación de réplicas.

Importante Para realizar la recopilación de réplicas, Agente para VMware (dispositivo virtual) debe ejecutarse en el ESXi de destino.

Para recopilar una réplica inicial

1. Realice uno de los siguientes procedimientos:
 - Si el equipo virtual original puede desconectarse, hágalo y luego vaya directamente al paso 4.
 - Si el equipo virtual original no se puede desconectar, continúe en el paso siguiente.
2. Cree un plan de replicación (pág. 128).

Al crear el plan, en **Equipo de destino**, seleccione **Réplica nueva** y el ESXi que aloja el equipo original.
3. Ejecute el plan una vez.

Se crea una réplica en el ESXi original.
4. Exporte los archivos del equipo virtual (o de la réplica) a un disco duro externo.
 - a. Conecte el disco duro externo al equipo donde se ejecuta vSphere Client.
 - b. Conecte vSphere Client al vCenter\ESXi original.
 - c. Seleccione la réplica recién creada en el inventario.
 - d. Haga clic en **Archivo > Exportar > Exportar plantilla de OVF**.
 - e. En **Directorio**, especifique la carpeta del disco duro externo.
 - f. Haga clic en **Aceptar**.
5. Transfiera el disco duro a la ubicación remota.
6. Importe la réplica al ESXi de destino.

- a. Conecte el disco duro externo al equipo donde se ejecuta vSphere Client.
 - b. Conecte vSphere Client al vCenter\ESXi de destino.
 - c. Haga clic en **Archivo > Implementar plantilla de OVF**.
 - d. En **Implementar desde un archivo o URL**, especifique la plantilla que exportó en el paso 4.
 - e. Complete el procedimiento de importación.
7. Edite el plan de replicación que creó en el paso 2. En **Equipo de destino**, seleccione **Réplica existente** y, a continuación, seleccione la réplica importada.

Como resultado, el software continuará actualizando la réplica. Todas las replicaciones serán incrementales.

13.3 Gestión de entornos de virtualización

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

13.4 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 físico | + | + | + |
| Equipo virtual VMware ESXi | + | + | + |
| Equipo virtual Hyper-V | + | + | + |

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

- Physical-to-virtual (P2V) - "Equipo físico a virtual" (pág. 75)
- Virtual-to-virtual (V2V) - "Equipo virtual" (pág. 77)
- Virtual-to-physical (V2P) - "Equipo virtual" (pág. 77) o "Recuperación de discos usando dispositivos de arranque" (pág. 78)

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:

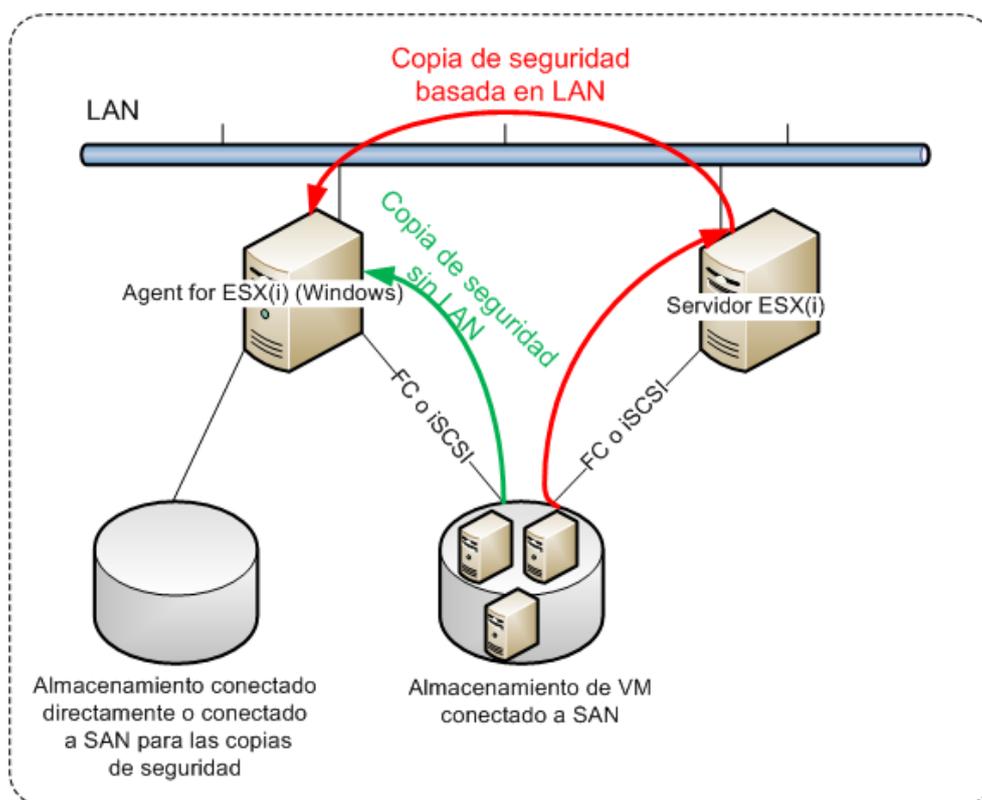
- Elegir discos o volúmenes independientes para la recuperación.
- Asignar de forma manual los discos de la copia de seguridad a los discos del equipo de destino.
- Volver a crear los volúmenes lógicos (LVM) o software RAID de Linux en el equipo de destino.
- Proporcionar los controladores del hardware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

13.5 Agent para VMware: copia de seguridad sin LAN

Si sus servidores ESXi de producción están tan cargados que no es recomendable la ejecución de los dispositivos virtuales, considere instalar Agente para VMware (Windows) en un equipo físico fuera de la infraestructura de ESXi.

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

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



Para permitir que el agente acceda al almacén de datos directamente

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

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 evitar la inicialización de LUN, estableceremos la **directiva SAN** en **Compartidos sin conexión** antes de conectar el LUN.

Para configurar la directiva SAN

1. Inicie sesión como administrador, ejecute símbolo del sistema, escriba **diskpart** y, a continuación, presione **Intro**.
2. Escriba **san policy=offlineshared** y, a continuación, presione **Intro**.
3. Para comprobar que los ajustes se hayan aplicado correctamente, escriba **san** y, a continuación, presione **Intro**. Asegúrese de que se muestra la **Directiva SAN: Compartidos sin conexión**.
4. Reinicie el equipo.

Para configurar un iniciador iSCSI

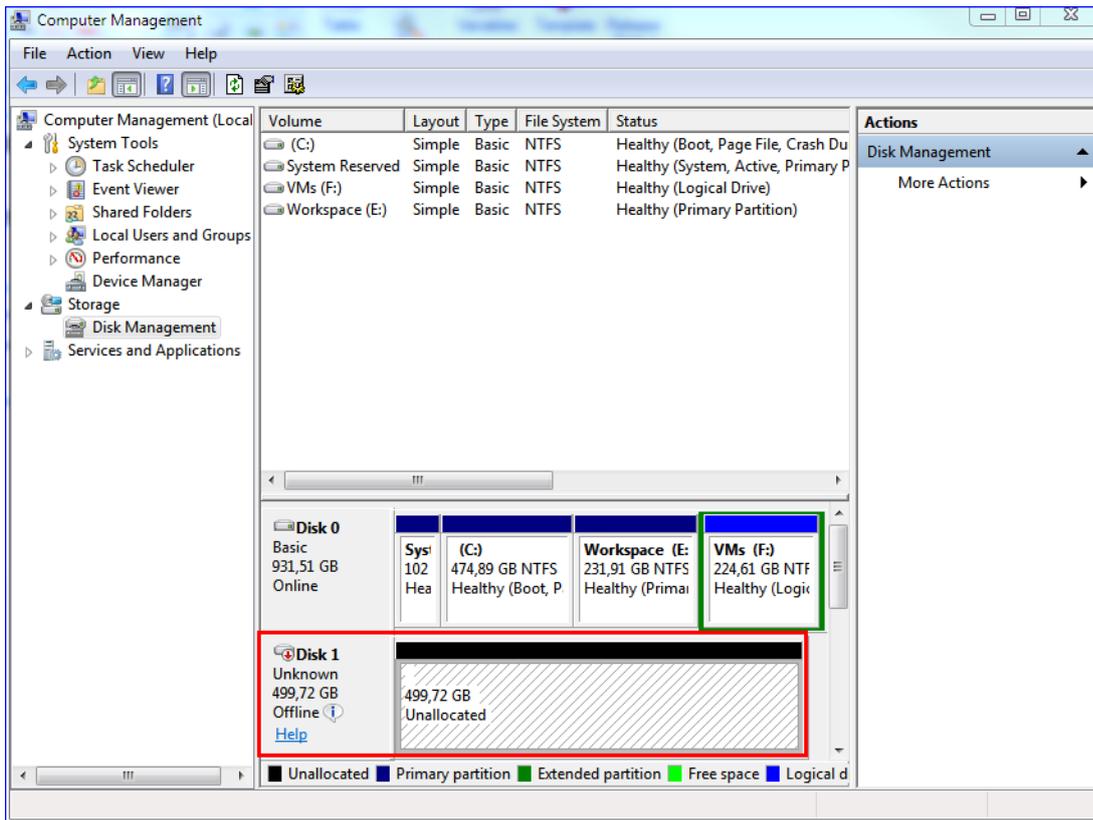
1. Vaya al **Panel de control > Herramientas administrativas > Iniciador de iSCSI**.

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.



13.6 Agente para VMware: privilegios necesarios

Esta sección describe los privilegios necesarios para realizar operaciones con equipos virtuales ESXi y, además, para la implementación de dispositivos virtuales. Agente para VMware (dispositivo virtual) solo está disponible para su implementación en una instalación.

Para realizar las operaciones en todos los servidores host y clústeres gestionados por un servidor vCenter Server, el Agente para VMware necesita los privilegios en el servidor vCenter Server. Si desea que el agente trabaje solo en un servidor host ESXi específico, asigne al agente los mismos privilegios en el servidor.

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. 133).

| Objeto | Privilegio | Operación | | | | |
|--|--|---|---|---|---|--|
| | | Copia de seguridad de un equipo virtual | Recuperación en un nuevo equipo virtual | Recuperación en un equipo virtual existente | Ejecutar VM desde la copia de seguridad | Implementación de un dispositivo virtual |
| Operaciones criptográficas (primeros pasos con vSphere 6.5) | Agregar disco | + | | | | |
| | Acceso directo | + | | | | |
| Almacén de datos | Asignar espacio | | + | + | + | + |
| | Examinar almacén de datos | | | | + | + |
| | Configurar los almacenes de datos | + | + | + | + | + |
| | Operaciones con archivos de bajo nivel | | | | + | + |
| Global | Licencias | + | + | + | + | |
| | Deshabilitar métodos | + | + | + | | |
| | Habilitar métodos | + | + | + | | |
| Servidor > Configuración | Configuración de autoarranque de VM | | | | | + |
| | Configuración de partición de almacenamiento | | | | + | |
| Servidor > Inventario | Modificar clúster | | | | | + |
| Servidor > Operaciones locales | Crear VM | | | | + | + |
| | Eliminar VM | | | | + | + |
| | Reconfigurar VM | | | | + | + |
| Red | Asignar red | | + | + | + | + |
| Recurso | Asignar equipo virtual a pool de recursos | | + | + | + | + |
| vApp | Importar | | | | | + |
| Equipo virtual > Configuración | Añadir disco existente | + | + | | + | |

| | | Operación | | | | |
|---|--|---|---|---|---|--|
| Objeto | Privilegio | Copia de seguridad de un equipo virtual | Recuperación en un nuevo equipo virtual | Recuperación en un equipo virtual existente | Ejecutar VM desde la copia de seguridad | Implementación de un dispositivo virtual |
| | Añadir disco nuevo | | + | + | + | + |
| | Añadir o quitar dispositivo | | + | | + | + |
| | Avanzado | + | + | + | | + |
| | Cambiar recuento de CPU | | + | | | |
| | Seguimiento de cambios de disco | + | | + | | |
| | Disco arrendado | + | | + | | |
| | Memoria | | + | | | |
| | Quitar disco | + | + | + | + | |
| | Cambiar nombre | | + | | | |
| | Establecer anotación | | | | + | |
| | Configuración | | + | + | | |
| Equipo virtual > Operaciones de huésped | Ejecución de programa de operación de huésped | +** | | | | + |
| | Consultas de operación de huésped | +** | | | | + |
| Equipo virtual > Interacción | Adquirir vale de control de huésped (en vSphere 4.1 y 5.0) | | | | + | + |
| | Configurar dispositivo de CD | | + | + | | |
| | Interacción de consola | | | | | + |
| | Gestión del sistema operativo huésped por VIX API (en vSphere 5.1 y versiones posteriores) | | | | + | + |
| | Apagar | | | + | + | + |
| | Encender | | + | + | + | + |
| Equipo virtual > Inventario | Crear desde existente | | + | + | + | |

| | | Operación | | | | |
|------------------------------------|---|---|---|---|---|--|
| Objeto | Privilegio | Copia de seguridad de un equipo virtual | Recuperación en un nuevo equipo virtual | Recuperación en un equipo virtual existente | Ejecutar VM desde la copia de seguridad | Implementación de un dispositivo virtual |
| | Crear nuevo | | + | + | + | + |
| | Mover | | | | | + |
| | Registrar | | | | + | |
| | Quitar | | + | + | + | + |
| | Anular el registro | | | | + | |
| Equipo virtual > Aprovisionamiento | Permitir acceso a disco | | + | + | + | |
| | Permitir acceso a disco de solo lectura | + | | + | | |
| | Permitir descarga de equipo virtual | + | + | + | + | |
| Equipo virtual > Estado | Crear instantánea | + | | + | + | + |
| | Eliminar instantánea | + | | + | + | + |

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

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

13.7 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 en un equipo físico. No obstante, el equipo se cuenta como virtual al definir las cuotas del número de equipos en una implementación en la nube.

La diferencia con respecto a un equipo físico es que los equipos virtuales Windows Azure y Amazon EC2 no se pueden iniciar desde dispositivos de arranque. Si necesita realizar una recuperación a un equipo virtual nuevo Windows Azure o Amazon EC2, siga el procedimiento siguiente.

Para recuperar un equipo como un equipo virtual Windows Azure o Amazon EC2

1. Cree un equipo virtual nuevo desde una imagen/plantilla en Windows Azure o Amazon EC2. El equipo nuevo debe tener la misma configuración de disco que el equipo que desea recuperar.
2. Instale Agente para Windows o Agente para Linux en el equipo nuevo.
3. Recupere el equipo incluido en la copia de seguridad tal y como se ha descrito en "Equipo físico" (pág. 74). Al configurar la recuperación, seleccione el equipo nuevo como el equipo de destino.

Requisitos de red

Los agentes instalados en los equipos incluidos en la copia de seguridad deben poder comunicarse con el servidor de gestión a través de la red.

Implementación en una instalación

- Si tanto los agentes como el servidor de gestión están instalados en la nube de Azure/EC2, todos los equipos ya estarán ubicados en la misma red. No se necesitan realizar acciones adicionales.
- Si el servidor de gestión está ubicado fuera de la nube de Azure/EC2, los equipos en la nube no tendrán acceso de red a la red local donde está instalado el servidor de gestión. Para permitir que los agentes instalados en esos equipos puedan comunicarse con el servidor de gestión, se debe crear una conexión de red privada virtual (VPN) entre la red local (en instalaciones) y la red de nube (Azure/EC2). Para obtener instrucciones acerca de cómo crear la conexión VPN, consulte los artículos siguientes:

Amazon EC2:

http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_VPN.html#vpn-create-cgw

Windows Azure:

<https://azure.microsoft.com/es-es/documentation/articles/vpn-gateway-site-to-site-create>

Implementación en la nube

En una implementación en la nube, el servidor de gestión se ubica en uno de los centros de datos de Acronis y, por tanto, los agentes pueden acceder a él. No se necesitan realizar acciones adicionales.

14 Configuración del servidor de gestión

Esta configuración solo está disponible para implementaciones en una instalación.

Para acceder a esta configuración, haga clic en **Configuración > Configuración del sistema**.

Para obtener información acerca de cómo gestionar licencias de Acronis Backup, consulte "Gestión de licencias" (pág. 31).

14.1 Servidor de correo electrónico

Puede especificar un servidor de correo electrónico que se utilizará para enviar notificaciones por correo electrónico desde el servidor de gestión.

Para especificar el servidor de correo electrónico

1. Haga clic en **Configuración > Configuración del sistema > Servidor de correo electrónico**.
2. En **Servicio de correo electrónico**, seleccione una de las siguientes opciones:
 - **Personalizado**
 - **Gmail**
Debe activar la opción de configuración **Aplicaciones menos seguras** en la cuenta de Gmail. Para obtener más información, consulte <https://support.google.com/accounts/answer/6010255>.
 - **Yahoo Mail**
 - **Outlook.com**
3. [Solo en el caso de un servicio de correo electrónico personalizado] Especifique los ajustes siguientes:
 - En el campo **Servidor SMTP**, escriba el nombre del servidor de correo saliente (SMTP).
 - En **Puerto SMTP**, indique el puerto del servidor de correo saliente. El puerto predeterminado es el 25.

- Seleccione si desea utilizar el cifrado TLS o SSL. Seleccione **Ninguno** para deshabilitar el cifrado.
 - Si el servidor SMTP necesita autenticación, seleccione la casilla de verificación **El servidor SMTP necesita autenticación** y, a continuación, especifique las credenciales de la cuenta que se utilizará para enviar mensajes. Si no está seguro de que el servidor SMTP requiera autenticación, póngase en contacto con su administrador de red o su proveedor de servicios de correo electrónico para obtener ayuda.
 - Algunos proveedores de servicios de Internet exigen la autenticación del servidor de correo entrante antes de permitir enviar cualquier información. Si ese es su caso, active la casilla de verificación **Configurar un servidor de correo entrante (POP)** para habilitar el servidor POP y configurar sus ajustes:
 - En **Servidor POP**, escriba el nombre del servidor POP.
 - En **Puerto POP**, indique el puerto del servidor de correo entrante. El puerto predeterminado es el 110.
 - Especifique las credenciales de acceso del servidor de correo entrante.
4. [Solo para Gmail, Yahoo Mail y Outlook.com] Especifique las credenciales de la cuenta que se utilizará para enviar mensajes.
 5. En **Remitente**, escriba el nombre del remitente. Este nombre aparecerá en el campo **De** en las notificaciones de correo electrónico. Si deja este campo en blanco, los mensajes contendrán la cuenta especificada en el paso 3 o 4.
 6. [Opcional] Haga clic en **Enviar mensaje de correo electrónico de prueba** para comprobar si las notificaciones por correo electrónico funcionan correctamente con la configuración especificada. Introduzca una dirección de correo electrónico a la que enviar el mensaje de prueba.

14.2 Notificaciones por correo electrónico

Puede configurar los ajustes predeterminados que sean habituales para las notificaciones por correo electrónico enviadas desde el servidor de gestión.

Cuando crea un plan de copias de seguridad, puede utilizar la configuración predeterminada o anularla mediante los valores personalizados que se especificarán únicamente para este plan.

Importante *Cambiar los ajustes predeterminados afecta a todos los planes de copias de seguridad que usan estos ajustes.*

Antes de configurar estos ajustes, asegúrese de que se han configurado los ajustes del **Servidor de correo electrónico** (pág. 140).

Para configurar los ajustes predeterminados de notificación por correo electrónico

1. Haga clic en **Configuración > Configuración del sistema > Notificaciones por correo electrónico**.
2. En el campo **Direcciones de correo electrónico de los destinatarios**, escriba la dirección de correo electrónico de destino. Puede introducir varias direcciones separadas por punto y coma.
3. Seleccione los tipos de notificaciones que quiere que se envíen. Los tipos disponibles son los siguientes:
 - **Errores**
 - **Advertencias**
 - **Copias de seguridad correctas**

El asunto de los mensajes de correo electrónico se basa en la plantilla siguiente: **[asunto] [nombre de equipo] [nombre de plan de copias de seguridad]**. La variable **[subject]** (asunto) se reemplazará

por una de las siguientes frases: **Copia de seguridad correcta**, **Copia de seguridad con errores**, **Copia de seguridad correcta con advertencias**.

15 Gestión de grupos y cuentas

La funcionalidad descrita en esta sección solo está disponible en la implementación en la nube para cuentas que tengan privilegios de administración.

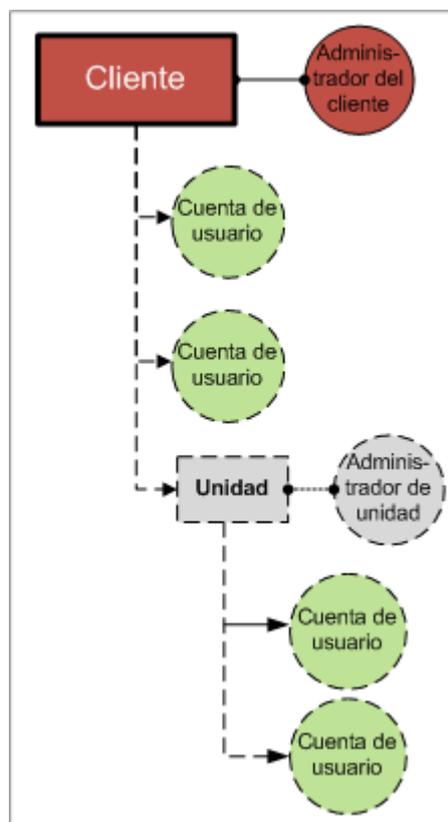
15.1 Cuentas y grupos

Hay dos tipos de cuentas: las **cuentas de administrador** y las **cuentas de usuario**. Tanto el usuario como los administradores pueden gestionar las copias de seguridad de los datos del usuario.

Cada cuenta pertenece a un grupo. Se crea automáticamente el grupo **Cliente** para su organización. De manera opcional, puede crear grupos **Unidad**, que normalmente se corresponden con unidades o departamentos de la organización.

Un administrador puede crear y gestionar grupos, cuentas de administrador y cuentas de usuario en su mismo nivel jerárquico o en cualquier nivel inferior.

En el siguiente diagrama se muestran dos niveles jerárquicos, el grupo Cliente y el grupo Unidad. Los grupos y cuentas opcionales se indican mediante una línea de puntos.



En la siguiente tabla se resumen las operaciones que pueden realizar los administradores y usuarios.

| Operación | Usuarios | Administradores |
|--------------|----------|-----------------|
| Crear grupos | No | Sí |

| | | |
|--|----|----|
| Crear cuentas | No | Sí |
| Descargar e instalar el software de copia de seguridad | Sí | Sí |
| Gestionar copias de seguridad | Sí | Sí |
| Gestionar recuperaciones | Sí | Sí |
| Crear informes acerca del uso del servicio | No | Sí |

15.2 Creación de un grupo

Quizá quiera crear un grupo **Unidad** nuevo dentro de su compañía cuando expanda el servicio de copias de seguridad a una nueva unidad organizativa.

Para crear un grupo

1. Inicie sesión en la consola de copia de seguridad.
2. Haga clic en **Gestionar cuentas**.
3. Seleccione el grupo en el que desea crear el nuevo grupo.
4. En la parte inferior del panel **Grupos**, haga clic en «+».
5. En **Nombre**, especifique un nombre para el nuevo grupo.
6. [Opcional] En **Identificador**, escriba una cadena que actuará como identificador del grupo. Este identificador aparecerá en los informes mensuales, junto con los datos de uso del grupo. Puede usar este identificador para referirse a este grupo en otro software, como por ejemplo en sus sistemas de facturación y control.

El identificador puede constar de un máximo de 256 caracteres Unicode (por ejemplo, números y letras del alfabeto latino). Se puede utilizar la misma cadena en otros grupos.

7. En **Idioma predeterminado**, seleccione el idioma predeterminado de las notificaciones, los informes y el software de copia de seguridad que se usará en este grupo.
8. [Opcional] En **Ubicaciones de copias de seguridad**, seleccione las ubicaciones de copia de seguridad para este grupo y sus grupos secundarios. Los valores disponibles son los siguientes:
 - **Local y nube**
 - **Solo nube**
9. [Opcional] Deshabilite el conmutador **Actualización automática de agentes**. Si lo hace, los agentes que estén registrados con estas cuentas en este grupo y sus grupos secundarios no se actualizarán automáticamente cuando se publique una versión nueva.
10. [Opcional] En **Información de contacto**, especifique la información de contacto del grupo.
11. Haga clic en **Crear**.

El grupo recién creado aparece en el árbol de **Grupos**.

Si quiere especificar la información de facturación de un grupo, seleccione el grupo en la lista **Grupos**, haga clic en **Propiedades**, y complete la sección de la información de facturación.

15.3 Creación de una cuenta

En una unidad debe existir al menos una cuenta (ya sea de administrador o de usuario).

Para crear una cuenta

1. Inicie sesión en la consola de copia de seguridad.
2. Haga clic en **Gestionar cuentas**.
3. Seleccione el grupo en el que quiere crear la cuenta.
4. Haga clic en la pestaña **Cuentas**.
5. Haga clic en **Agregar cuenta**.
6. Especifique la siguiente información de contacto para la cuenta.
 - **Usuario**

***Importante:** Debe haber únicamente un usuario en cada cuenta. Puede crear múltiples usuarios con la misma dirección de correo electrónico.*

 - **Correo electrónico**
 - [Opcional] **Nombre**
 - [Opcional] **Apellido**
7. Si desea que esta cuenta sea una cuenta de administrador, habilite el conmutador de **privilegios de administrador**.
8. [Opcional] Deshabilite el conmutador **Actualización automática de agentes**. Si lo hace, los agentes que estén registrados con esta cuenta no se actualizarán automáticamente cuando se publique una versión nueva.
9. [Opcional] Especifique la cuota de almacenamiento y el número máximo de equipos, dispositivos y buzones de correo de los que el usuario puede realizar copias de seguridad.
 - **Estaciones de trabajo físicas**
 - **Servidores físicos**
 - **Windows Server Essentials**
 - **Servidores virtuales**
 - **Dispositivos móviles**
 - **Buzones de correo de Office 365**
 - **Cuota de almacenamiento**

Estas cuotas son de advertencia. Si se sobrepasa cualquiera de estos valores, se enviará una notificación por correo electrónico a la dirección de correo electrónico que se especifica en el paso 6. No se aplican restricciones al uso del servicio de copias de seguridad.
10. [Opcional] Especifique los 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, las copias de seguridad producirán error.

***Importante:** Si define tanto la cuota como su uso por encima del límite en cero, el usuario no verá la funcionalidad correspondiente.*

11. [Opcional] En **Ubicaciones de copias de seguridad**, seleccione las ubicaciones de copia de seguridad para esta cuenta. Los valores disponibles son los siguientes:
 - **Local y cloud**
 - **Solo cloud**
12. [Opcional] Cambie el nivel de **Notificaciones de copias de seguridad**. Puede escoger uno de los niveles siguientes:
 - **Apagado:** sin notificaciones
 - **Menos:** notificaciones sobre fallos de la copia de seguridad (predeterminado)

- **Más:** notificaciones sobre fallos de la copia de seguridad y advertencias
- **Todas:** notificaciones sobre fallos de la copia de seguridad, advertencias y copias de seguridad realizadas con éxito

Todas las notificaciones se envían a la dirección de correo electrónico especificada.

13. [Opcional] Deshabilite **Notificaciones de uso**. Si lleva a cabo esta opción, no se enviarán las notificaciones por haber sobrepasado las cuotas a la dirección de correo electrónico especificada.

14. Haga clic en **Agregar**.

Como resultado:

- Aparecerá una nueva cuenta en la pestaña **Cuentas**.
- Se le enviará un mensaje con el enlace de activación a la dirección de correo electrónico especificada.

15.4 Creación de un informe acerca del uso del servicio

Los informes de uso proporcionan datos históricos sobre la utilización del servicio de copias de seguridad.

Solo los administradores pueden crear estos informes.

Parámetros del informe

El informe incluye los siguientes datos sobre una unidad y sus cuentas:

- Tamaño de las copias de seguridad por grupo, por cuenta y por tipo de equipo.
- Cantidad de equipos protegidos por grupo, por cuenta y por tipo de equipo.
- Precio por grupo, por cuenta y por tipo de equipo.
- El tamaño total de las copias de seguridad.
- La cantidad total de equipos protegidos.
- Precio total.

Ámbito del informe

Puede seleccionar el ámbito del informe entre los valores siguientes:

- **Clientes y socios directos**
El informe solo incluye los valores de los parámetros de los informes relacionados con los grupos secundarios inmediatos de su grupo.
- **Todos los socios y clientes**
El informe incluye los valores de los parámetros de los informes relacionados con todos los grupos secundarios de su grupo.
- **Todos los clientes y socios (incluyendo los detalles de cuenta)**
El informe incluye los valores de los parámetros de los informes relacionados con todos los grupos secundarios de su grupo y con todas las cuentas de usuario que hay en los grupos.

Habilitar o deshabilitar informes de uso planificados

Un informe planificado contiene los datos de uso del sistema durante el último mes completo. Los informes se generan a las 23:59:59 (hora UTC) del primer día del mes y se envían el segundo día del mes a todos los administradores del grupo.

1. En la consola de gestión de cuentas, haga clic en **Informes**.

2. Seleccione la pestaña **Programado**.
3. Habilite o deshabilite los informes de uso planificados haciendo clic en el conmutador.
4. En **Nivel de detalle**, seleccione el ámbito del informe, como se ha descrito anteriormente.

Generación de un informe de uso personalizado

Este tipo de informe no puede planificarse, se genera a petición. El informe se enviará a su dirección de correo electrónico.

1. En la consola de gestión de cuentas, haga clic en **Informes**.
2. Seleccione la pestaña **Personalizado**.
3. En **Período**, seleccione el informe del periodo:
 - **Mes actual**
 - **Mes anterior**
 - **Personalizado**
4. Si quiere especificar un período de informe personalizado, seleccione las fechas de inicio y fin. De lo contrario, omita este paso.
5. En **Tipo**, seleccione el tipo del informe:
 - **Informe resumido**: El informe incluye los valores totales de los parámetros de los informes en relación con el período especificado, incluido el valor del precio total.
 - **Estadísticas diarias**: El informe incluye los valores de los parámetros de los informes para cada día del período especificado sin incluir los valores de los precios.
6. En **Nivel de detalle**, seleccione el ámbito del informe, como se ha descrito anteriormente.
7. Para generar el informe, haga clic en **Generar y enviar**.

15.5 Limitación del acceso a la interfaz web

Si quiere limitar el acceso a la interfaz web, especifique una lista de direcciones IP desde las que los miembros de un grupo pueden iniciar sesión.

Esta restricción *no* se aplica a los miembros de los grupos secundarios.

Para limitar el acceso a la interfaz web

1. Inicie sesión en la consola de gestión de cuentas.
2. Seleccione un grupo cuyo acceso desee limitar.
3. Haga clic en **Ajustes > Seguridad**.
4. Seleccione la casilla de verificación **Habilitar control de inicio de sesión**.
5. En **Direcciones IP permitidas**, indique las direcciones IP que quiere permitir.
Puede escribir cualquiera de los parámetros siguientes separados por punto y coma.
 - Direcciones IP, como 192.0.2.0
 - Rangos de IP, como 192.0.2.0-192.0.2.255
 - Subredes, como 192.0.2.0/24
6. Haga clic en **Guardar**.

16 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.

Declaración de copyright

Copyright © Acronis International GmbH, 2002-2017. Todos los derechos reservados.

“Acronis” y “Acronis Secure Zone” son marcas comerciales registradas de Acronis International GmbH.

“Acronis Compute with Confidence”, “Acronis Startup Recovery Manager”, “Acronis Active Restore”, “Acronis Instant Restore” y el logotipo de Acronis son marcas comerciales de Acronis International GmbH.

Linux es una marca registrada de Linus Torvalds.

VMware y VMware Ready son marcas comerciales o marcas registradas de VMware, Inc. en Estados Unidos o en otras jurisdicciones.

Windows y MS-DOS son marcas registradas de Microsoft Corporation.

Todas las otras marcas comerciales y derechos de autor mencionados son propiedad de sus respectivos propietarios.

La distribución de las versiones sustancialmente modificadas del presente documento está prohibida sin el permiso explícito del titular del derecho de autor.

La distribución de este trabajo o trabajo derivado en cualquier forma de libro estándar (papel) para fines comerciales está prohibida excepto que se obtenga permiso previo del titular del derecho de autor.

LA DOCUMENTACIÓN SE PROPORCIONA «TAL COMO SE ENCUENTRA» Y SE EXCLUYEN TODAS LAS CONDICIONES EXPLÍCITAS O IMPLÍCITAS, DECLARACIONES Y GARANTÍAS, INCLUIDA CUALQUIER GARANTÍA IMPLÍCITA DE COMERCIABILIDAD, IDONEIDAD CON UN PROPÓSITO ESPECÍFICO O NO VIOLACIÓN DE DERECHOS DE TERCEROS, SALVO EN LA MEDIDA EN QUE DICHAS EXCLUSIONES TENGAN VALIDEZ LEGAL.

Es posible que se suministre código de terceros junto con el software o servicio. Los términos de la licencia de terceros se detallan en el archivo license.txt ubicado en el directorio raíz de instalación. La última lista actualizada del código de terceros y los términos de la licencia asociada que se utiliza con el software y/o servicio está siempre disponible en <http://kb.acronis.com/content/7696>

Tecnologías patentadas de Acronis

Las tecnologías que se usan en este producto están cubiertas y protegidas por uno o más Números de patente de los Estados Unidos: 7,047,380; 7,275,139; 7,281,104; 7,318,135; 7,353,355; 7,366,859; 7,475,282; 7,603,533; 7,636,824; 7,650,473; 7,721,138; 7,779,221; 7,831,789; 7,886,120; 7,895,403; 7,934,064; 7,937,612; 7,949,635; 7,953,948; 7,979,690; 8,005,797; 8,051,044; 8,069,320; 8,073,815; 8,074,035; 8,145,607; 8,180,984; 8,225,133; 8,261,035; 8,296,264; 8,312,259; 8,347,137; 8,484,427; 8,645,748; 8,732,121 y solicitudes de patentes pendientes.

17 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 de copia de seguridad **Personalizado**, 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 **Mensuales, 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 creada el día de la semana seleccionado en la opción **Copia de seguridad semanal** (haga clic en el icono de engranaje y después, en **Opciones de copias de seguridad > Copia de seguridad semanal**).
- Una copia de seguridad diaria es la primera copia de seguridad creada una vez comenzado un día.
- Una copia de seguridad cada hora es la primera copia de seguridad creada una vez comenzado una hora.

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. 149). 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.