Acronis®
COMPUTE WITH CONFIDENCE
WWW.ACRONIS.ES

Acronis® Backup & Recovery ™ 10 Server para Linux

Update 5

Guía del usuario

Contenido

1 Introducción de Acronis® Backup & Recovery™ 10

1.1 Generalidades de Acronis Backup & Recovery 10

Basado en la imagen de disco y las tecnologías de restauración completa patentadas de Acronis, Acronis Backup & Recovery 10 es el sucesor de Acronis True Image Echo como la solución de recuperación de catástrofes de la próxima generación.

Acronis Backup & Recovery 10 Server for Linux hereda los beneficios de la familia de productos de Acronis True Image Echo:

- Copia de seguridad de un disco o volumen entero, incluyendo el sistema operativo, todas las aplicaciones y datos.
- Recuperación completa de cualquier hardware.
- Copia de seguridad y recuperación de archivos y carpetas.

Acronis Backup & Recovery 10 Server for Linux ofrece nuevos beneficios que ayudan a las organizaciones a cumplir con los objetivos de tiempo de recuperación desafiantes mientras reducen tanto el coste de capital como el coste de mantenimiento del software.

- **Aprovechamiento de la infraestructura de TI existente**

  Totalmente compatible y fácil de actualizar desde Acronis True Image Echo.
- **Protección de datos altamente automatizada**

  Planificación completa de la protección de datos (copia de seguridad, retención y validación de copias de seguridad) dentro de una política de copias de seguridad.

  Esquemas de copia de seguridad Torres de Hanói y Abuelo-Padre-Hijo incorporados con parámetros adaptables.

  Se puede escoger entre una variedad de eventos y condiciones para dar inicio a una copia de seguridad.
- **Interfaz gráfica de usuario rediseñada**

  Tablero de control para una rápida toma de decisiones operativas.

  Generalidades de todas las operaciones configuradas y ejecutándose, con codificación por color para operaciones correctas y con fallos.
- **Servicios adicionales de dispositivos de inicio**

  Las utilidades de línea de comandos de Linux y Acronis están disponibles en los dispositivos de inicio para crear la estructura de volúmenes lógica antes de comenzar la recuperación.

1.2 Cómo empezar

Gestión directa

1. Instale Acronis Backup & Recovery 10 Management Console y Acronis Backup & Recovery 10 Agente.
2. Inicio de la consola.

Linux

Inicie la sesión como raíz o como un usuario normal y después cambie de usuario según sea necesario. Inicie la consola con el commando:

```
/usr/sbin/acronis_console
```

3. Conecte la consola al equipo en el que está instalado el agente.

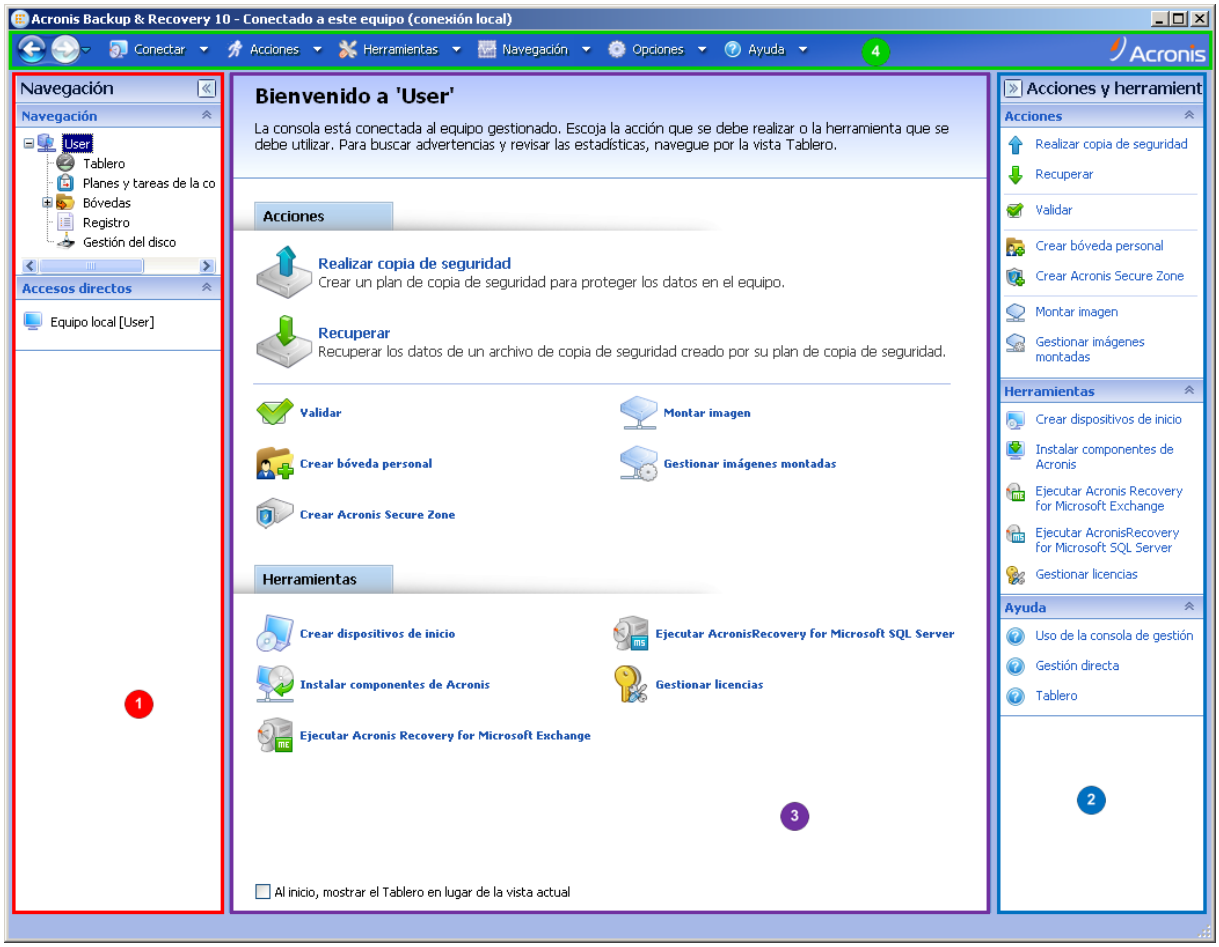
A dónde ir desde aquí

Para saber cuál es el próximo paso consulte "Conceptos básicos (pág. 17)".

Para comprender los elementos de la GUI consulte "Uso de la consola de gestión (pág. 7)".

1.2.1 Uso de la consola de gestión

En cuanto se conecta la consola a un equipo gestionado (pág. 190) o a un servidor de gestión (pág. 194), los elementos correspondientes aparecen en el espacio de trabajo de la consola (en el menú, en el área principal con la pantalla de **Bienvenida**, el panel de **Navegación**, el panel de **Acciones y herramientas**) permitiéndole llevar a cabo operaciones específicas del agente o del servidor.



Acronis Backup & Recovery 10 Management Console: Pantalla de Bienvenida

Elementos clave del espacio de trabajo de la consola

	Nombre	Descripción
1	Panel de **Navegación**	Contiene el árbol de **Navegación** y la barra de **Accesos directos** y le permite navegar por las diferentes vistas (consulte la sección Panel de navegación (pág. 8)).
2	Panel **Acciones y herramientas**	Contiene barras con un conjunto de acciones que pueden llevarse a cabo y herramientas (consulte la sección Panel acciones y herramientas (pág. 9)).
3	Área **principal**	El espacio de trabajo principal, donde puede crear, editar y gestionar planes, políticas y tareas de copia de seguridad y llevar a cabo otras operaciones. Muestra las diferentes vistas y páginas de acción (pág. 11) de acuerdo con los elementos seleccionados en el menú, el árbol de **Navegación** o el panel **Acciones y herramientas**.
4	Barra de **menú**	Aparece en la parte superior de la ventana del programa y le permite llevar a cabo todas las operaciones disponibles en ambos paneles. Los elementos del menú cambian de forma dinámica.

Es necesario tener una resolución de 1024x768 o mayor para trabajar de forma cómoda con la consola de gestión.

Panel de "Navegación"

El panel de navegación incluye el árbol de **Navegación** y la barra de **Accesos directos**.

Árbol de navegación

El árbol de **Navegación** le permite navegar por las vistas de los programas. Las vistas dependen de si la consola está conectada a un equipo gestionado o al servidor de gestión.

Vistas para un equipo gestionado

Cuando la consola está conectada a un equipo gestionado, las siguientes vistas están disponibles en el árbol de navegación.

- **[Nombre del equipo]**. Raíz del árbol, también llamada vista **Bienvenida**. Muestra el nombre del equipo al cual está conectada la consola en ese momento. Utilice esta vista para tener un acceso rápido a las operaciones principales, disponibles en el equipo gestionado.
  - **Tablero de control**. Utilice esta vista para calcular rápidamente si los datos están protegidos correctamente en el equipo gestionado.
  - **Planes y tareas de la copia de seguridad**. Utilice esta vista para gestionar planes y tareas de la copia de seguridad en el equipo gestionado: ejecutar, editar, detener y eliminar planes y tareas, ver sus estados y estatus, supervisar planes.
  - **Bóvedas**. Utilice esta vista para gestionar bóvedas personales y los archivos comprimidos almacenados en ellas, añadir nuevas bóvedas, renombrar y eliminar las ya existentes, validar bóvedas, explorar el contenido de las copias de seguridad, montar copias de seguridad como unidades virtuales, etc.
  - **Registro**. Utilice esta vista para examinar la información sobre operaciones llevadas a cabo por el programa en el equipo gestionado.

Barra de accesos directos

La barra de **Accesos directos** aparece debajo del árbol de navegación. La misma le brinda un método fácil y conveniente para conectarse con los equipos solicitados añadiéndolos a los accesos rápidos.

Para añadir un acceso rápido a un equipo

1. Conecte la consola a un equipo gestionado.
2. En el árbol de navegación, haga clic con el botón derecho en el nombre del equipo (un elemento raíz del árbol de navegación) y después seleccione **Crear acceso directo**.

   Si la consola y el agente se instalan en el mismo equipo, el acceso directo a este equipo se añadirá a la barra de accesos directos automáticamente como **Equipo local [Nombre del equipo]**.

Panel "Acciones y herramientas"

El panel **Acciones y herramientas** le permite trabajar fácil y eficazmente con Acronis Backup & Recovery 10. Las barras del panel proporcionan un acceso rápido a las operaciones y herramientas de los programas. Todos los elementos de la barra de **Acciones y herramientas** están duplicados en el menú del programa.

Barras

Acciones de "[nombre del elemento]"

Contiene un conjunto de acciones que pueden llevarse a cabo sobre los elementos seleccionados en cualquiera de las vistas de navegación. Al hacer clic en la acción se abre la página de acción (pág. 12) correspondiente. Los elementos de las diferentes vistas de navegación tienen su propio conjunto de acciones. El nombre de la barra cambia de acuerdo con el elemento que se selecciona. Por ejemplo, si selecciona el plan de copia de seguridad denominado *Copia de seguridad del sistema* en la vista **Planes y tareas de la copia de seguridad**, la barra de acciones se denominará **Acciones de la "copia de seguridad del sistema"** y contendrá el conjunto de acciones típico de los planes de copia de seguridad.

También es posible acceder a todas las acciones a través de los elementos del menú correspondientes. Un elemento del menú aparece en la barra de menú cuando se selecciona un elemento en cualquiera de las vistas de navegación.

Ejemplos de barras de "acciones de 'nombre del elemento'"

Acciones

Contiene una lista de operaciones comunes que se pueden llevar a cabo en un equipo gestionado o en un servidor de gestión. Siempre las mismas para todas las vistas. Al hacer clic en la operación se abre la página de acción correspondiente (consulte la sección Páginas de acción (pág. 12)).

También es posible acceder a todas las acciones a través del menú **Acciones**.

Barra de "Acciones" en un equipo gestionado y en un servidor de gestión

Herramientas

Contiene una lista de las herramientas de Acronis. Siempre la misma en todas las vistas de los programas.

También es posible acceder a todas las herramientas a través del menú **Herramientas**.

Barra de "Herramientas"

Ayuda

Contiene una lista de los temas de ayuda. Diferentes vistas y páginas de acción de Acronis Backup & Recovery 10 proporcionadas con listas de temas de ayuda específicos.

Operaciones con paneles

Cómo expandir/minimizar paneles

De manera predeterminada, el panel de **Navegación** aparece expandido y el de **Acciones y herramientas** minimizado. Es posible que tenga que minimizar el panel para liberar un poco de espacio de trabajo adicional. Para esto, haga clic en la flecha tipo ( , para el panel de **Navegación**;  , para el panel **Acciones y herramientas**). El panel se minimizará y la flecha tipo cambiará su dirección. Haga clic en la flecha tipo nuevamente para expandir el panel.

Cómo cambiar los bordes de los paneles

1. Posicione el ratón sobre el borde del panel.
2. Cuando el puntero se transforme en una flecha de dos puntas, arrástrelo para mover el borde.

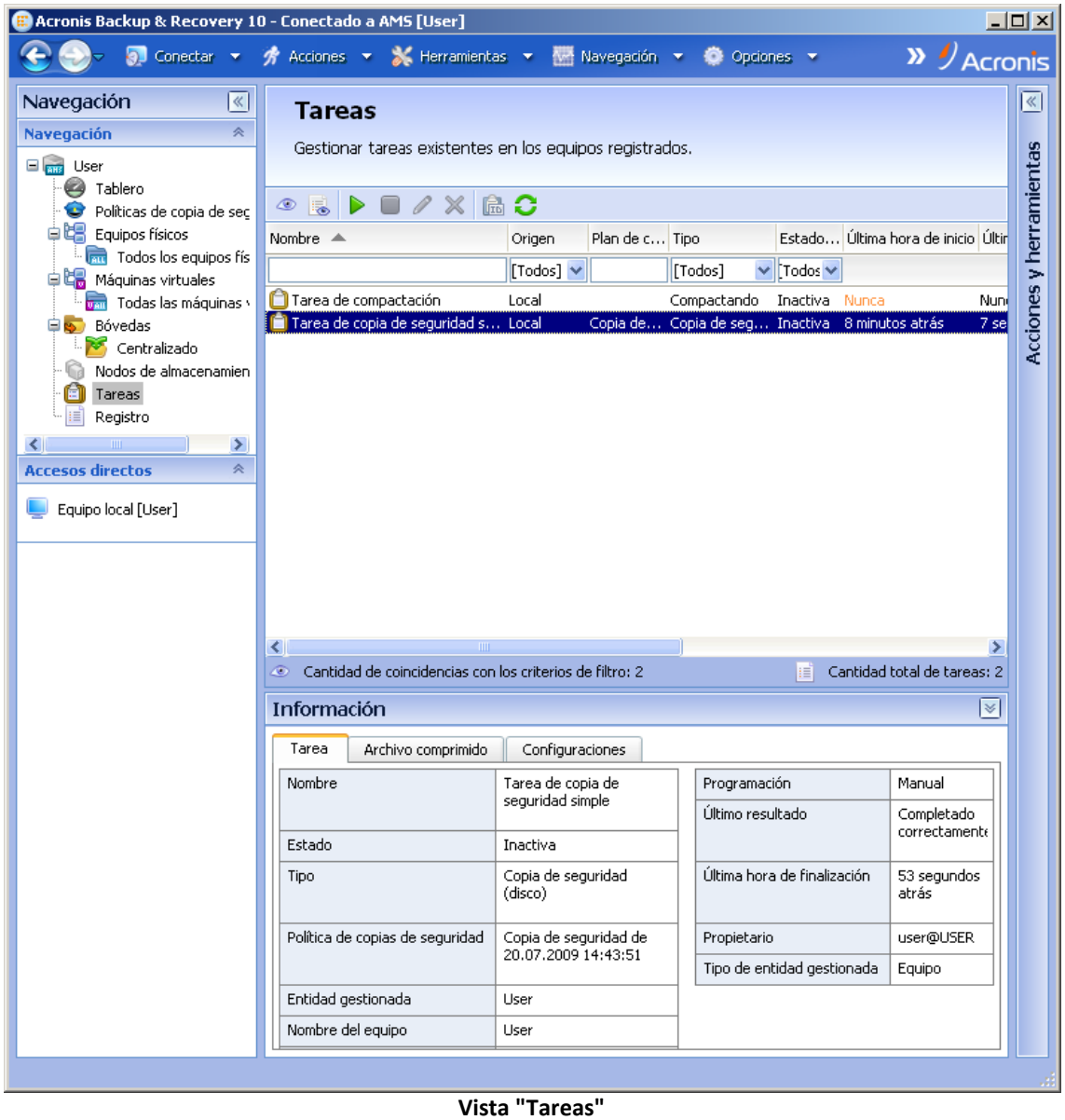
La consola de gestión "recuerda" cómo se configura los bordes de los paneles. La próxima vez que ejecute la consola de gestión, todos los bordes de los paneles estarán en la misma posición que se había configurado previamente.

Área principal, vistas y páginas de acción

El área principal es un sitio básico en el que trabajará con la consola. Aquí se crean, editan y administran los planes, políticas, tareas de respaldo del sistema y se realizan otras operaciones. El área principal muestra vistas y páginas de acciones diversas de acuerdo con los elementos que selecciona en el menú y, en el árbol de **Navegación**, o en el panel de **Acciones y Herramientas.**

Vistas

Una vista aparece en el área principal al hacer clic en cualquier elemento del árbol de **Navegación** del Panel de navegación (pág. 8).



Vista "Tareas"

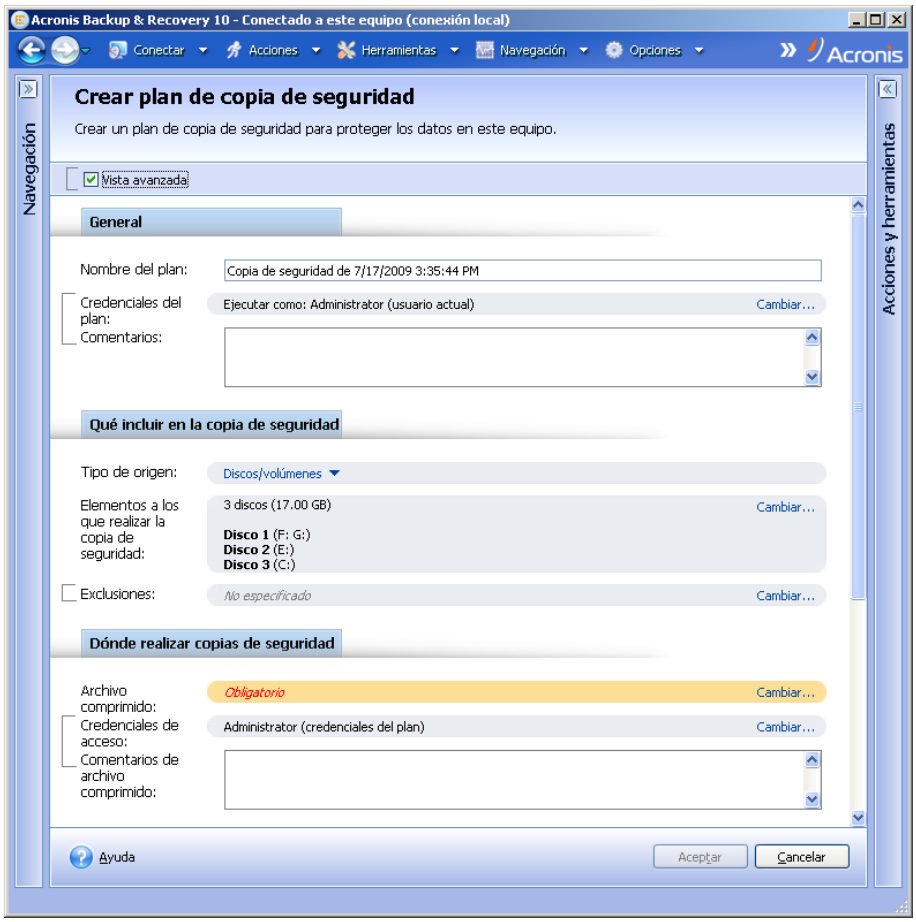
La manera más común de trabajar con las vistas

En general, cada vista contiene una tabla de elementos, una barra de herramientas con botones y el panel **Información**.

- Utilice las capacidades de filtro y organización para buscar el elemento en cuestión dentro de la tabla
- En la tabla, seleccione el elemento deseado
- En el panel **Información** (minimizado de manera predeterminada), vea los detalles del elemento
- Lleve a cabo acciones sobre el elemento seleccionado. Hay varias formas de llevar a cabo la misma acción en diferentes elementos seleccionados:
  - Al hacer clic en los botones de la barra de tareas,
  - Al hacer clic en los elementos de la barra de **Acciones** de **[Nombre del elemento]** (en el panel **Acciones y herramientas**),
  - Al seleccionar los elementos en el menú **Acciones**,
  - Al hacer clic con el botón derecho en el elemento y seleccionar la operación en el menú contextual.

Páginas de acción

En el área principal aparece una página de acción al hacer clic en un elemento de cualquiera de las acciones del menú **Acciones** o de la barra de **Acciones** del panel de **Acciones y herramientas**. La misma contiene los pasos que hay que llevar a cabo para crear e iniciar cualquier tarea, plan de copia de seguridad o política de copias de seguridad.

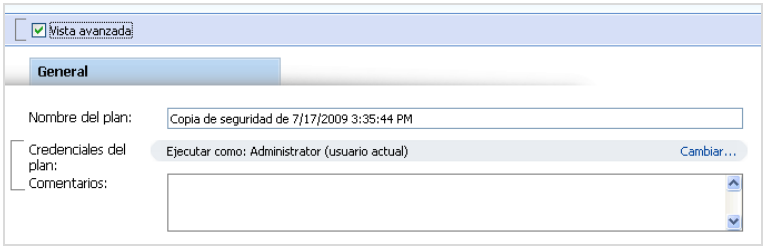


Página de acción: Crear plan de copia de seguridad

Uso de controles y especificación de configuraciones

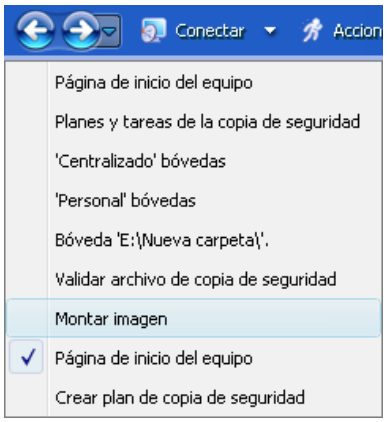
Las páginas de acción ofrecen dos formas de representación: básica y avanzada. La representación básica esconde campos como credenciales, comentarios, etc. Cuando se habilita la representación avanzada, se muestran todos los campos disponibles. Puede intercambiar las vistas seleccionando la casilla de verificación **Vista avanzada** en la parte superior de la página de acción.

La mayoría de las configuraciones se configuran haciendo clic en los enlaces **Cambiar…** que se encuentran a la derecha. Otros se seleccionan en la lista desplegable o se escriben manualmente en los campos de la página.



Página de acción: Controles

Acronis Backup & Recovery 10 recuerda los cambios que se hacen en las páginas de acción. Por ejemplo, si empezase a crear un plan de copias de seguridad y luego por cualquier motivo cambiase a otra vista sin completar la creación del plan, puede hacer clic en el botón de navegación **Atrás** del menú. O, si ha avanzado algunos pasos, haga clic en la flecha **Abajo** y seleccione de la lista la página en donde empezó la creación del plan. Por lo tanto, puede llevar a cabo los pasos que faltan y completar la creación del plan de copia de seguridad.



Botones de navegación

1.3 Componentes de Acronis Backup & Recovery 10

Esta sección contiene una lista de los componentes de Acronis Backup & Recovery 10 con una descripción breve de su funcionalidad.

Componentes para un equipo gestionado (agentes)

Estas aplicaciones realizan copias de seguridad, recuperación y otras operaciones con los datos de los equipos gestionados con Acronis Backup & Recovery 10. Los agentes deben tener una licencia para llevar a cabo operaciones en cada equipo gestionado. Los agentes tienen múltiples funciones o complementos que permiten una funcionalidad adicional y por lo tanto pueden requerir licencias adicionales.

Consola

La consola proporciona la interfaz gráfica de usuario y la conexión remota con los agentes. No se requieren licencias para el uso de la consola.

Generador de dispositivos de inicio

Con el generador de dispositivos de inicio, puede crear dispositivos de inicio para utilizar los agentes y otras utilidades de rescate en un entorno de rescate. La disponibilidad de los complementos del agente en un entorno de rescate depende de si el complemento está instalado en el equipo en donde el generador de dispositivos está funcionando.

1.3.1 Agente para Linux

Este agente permite la protección de datos de nivel de disco y de nivel de archivos con Linux.

Copia de seguridad del disco

La protección de datos de nivel de disco se basa en la realización de copias de seguridad de un disco o de un sistema de archivos de un volumen en conjunto, junto con toda la información necesaria para que el sistema operativo se inicie, o todos los sectores del disco que utilicen el enfoque sector por sector (modo sin procesar). Una copia de seguridad que contiene una copia de un disco o un volumen en una forma compacta se denomina una copia de seguridad de disco (volumen) o una imagen de disco (volumen). Es posible recuperar discos o volúmenes de forma completa a partir de estas copias de seguridad, así como carpetas o archivos individuales.

Copia de seguridad de archivos

La protección de datos de nivel de archivos se basa en la realización de copias de seguridad de archivos y directorios que se encuentran en el equipo en el que está instalado el agente o en una red compartida a la que se accede utilizando el protocolo smb o nfs. Los archivos se pueden recuperar en su ubicación original o en otro lugar. Es posible recuperar todos los archivos y directorios con los que se realizó la copia de seguridad o seleccionar cuál de ellos recuperar.

1.3.2 Management Console

Acronis Backup & Recovery 10 Management Console es una herramienta administrativa para el acceso local a Acronis Backup & Recovery 10 Agente para Linux. La conexión remota al agente no es posible

1.3.3 Generador de dispositivos de inicio

El generador de dispositivos de inicio de Acronis es una herramienta dedicada para la creación de dispositivos de inicio (pág. 195). El generador de dispositivos que se instala en Linux crea dispositivos de inicio basados en el núcleo de Linux.

1.4 Sistemas de archivos compatibles

Acronis Backup & Recovery 10 puede realizar copias de seguridad y recuperar los siguientes sistemas de archivos con las siguientes limitaciones:

- FAT16/32
- NTFS

- Ext2/Ext3/Ext4
- ReiserFS3: los archivos específicos no se pueden recuperar de las copias de seguridad del disco ubicadas en Acronis Backup & Recovery 10 Storage Node
- ReiserFS4: recuperación del volumen sin la capacidad de cambiar el tamaño del mismo, los archivos específicos no se pueden recuperar de las copias de seguridad del disco ubicadas en Acronis Backup & Recovery 10 Storage Node
- XFS: recuperación del volumen sin la capacidad de cambiar el tamaño del mismo, los archivos específicos no se pueden recuperar de las copias de seguridad del disco ubicadas en Acronis Backup & Recovery 10 Storage Node
- JFS: los archivos específicos no se pueden recuperar de las copias de seguridad del disco ubicadas en el nodo de almacenamiento Acronis Backup & Recovery 10
- Linux SWAP

Acronis Backup & Recovery 10 puede realizar copias de seguridad y recuperar sistemas de archivos dañados o incompatibles utilizando el enfoque sector por sector.

1.5 Sistemas operativos compatibles

Acronis Backup & Recovery 10 Management Console, Acronis Backup & Recovery 10 Agent para Linux

- Linux con kernel 2.4.18 o posterior (incluyendo kernels de 2.6.x) y glibc 2.3.2 o posterior
- Varias distribuciones Linux de 32 bits y 64 bits, incluyendo:
  - Red Hat Enterprise Linux 4 y 5
  - Red Hat Enterprise Linux 6
  - Ubuntu 9.04 (Jaunty Jackalope), 9.10 (Karmic Koala) y 10.04 (Lucid Lynx)
  - Fedora 11 y 12
  - SUSE Linux Enterprise Server 10 y 11
  - Debian 4 (Lenny) y 5 (Etch)
  - CentOS 5
- El agente para Linux es de hecho un ejecutable de 32 bits. Para la autenticación, el agente utiliza bibliotecas del sistema, versiones de 32 bits que no siempre se instalan de manera predeterminada con las distribuciones de 64 bits. Al utilizar el agente en una distribución basada en RedHat de 64 bits, como RHEL, CentOS o Fedora, o en una distribución SUSE de 64 bits, asegúrese de que los siguientes paquetes de 32 bits estén instalados en el sistema:

  pam.i386

  libselinux.i386

  libsepol.i386

  Estos paquetes deberían estar disponibles en el repositorio de su distribución de Linux.
- Antes de instalar el producto en un sistema que no use el administrador 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
```

1.6 Requisitos del sistema

Los componentes instalados en Linux

Nombre de la edición	Memoria (sobre el SO y las aplicaciones en ejecución)	Espacio de disco necesario durante la instalación o la actualización	Espacio de disco ocupado por los componentes	Adicional
Server for Linux	120 MB	400 MB	240 MB	Resolución de la pantalla de 1024*768 píxeles o mayor
Generador de dispositivo de inicio (Linux)	70 MB	240 MB	140 MB	

Medio de inicio

Tipo de medio	Memoria	Tamaño de imagen ISO	Adicional
Basado en Linux	256 MB	130 MB	

1.7 Soporte técnico

Programa de asistencia y mantenimiento

Si necesita ayuda con su producto de Acronis, vaya a http://www.acronis.es/support/.

Actualizaciones de productos

Puede descargar las últimas actualizaciones para sus productos de software de Acronis registrado desde nuestra página web en cualquier momento después de iniciar sesión en su **Cuenta** (https://www.acronis.es/my/) y registrar el producto. Consulte **Registro de productos de Acronis en el sitio web** (http://kb.acronis.com/content/4834) y **Guía de usuario de la página web de Acronis** (http://kb.acronis.com/content/8128).

2 Comprensión de Acronis Backup & Recovery 10

Esta sección tiene como objetivo brindar una clara comprensión del producto para que se lo pueda usar en varias circunstancias sin las instrucciones "paso a paso".

2.1 Conceptos básicos

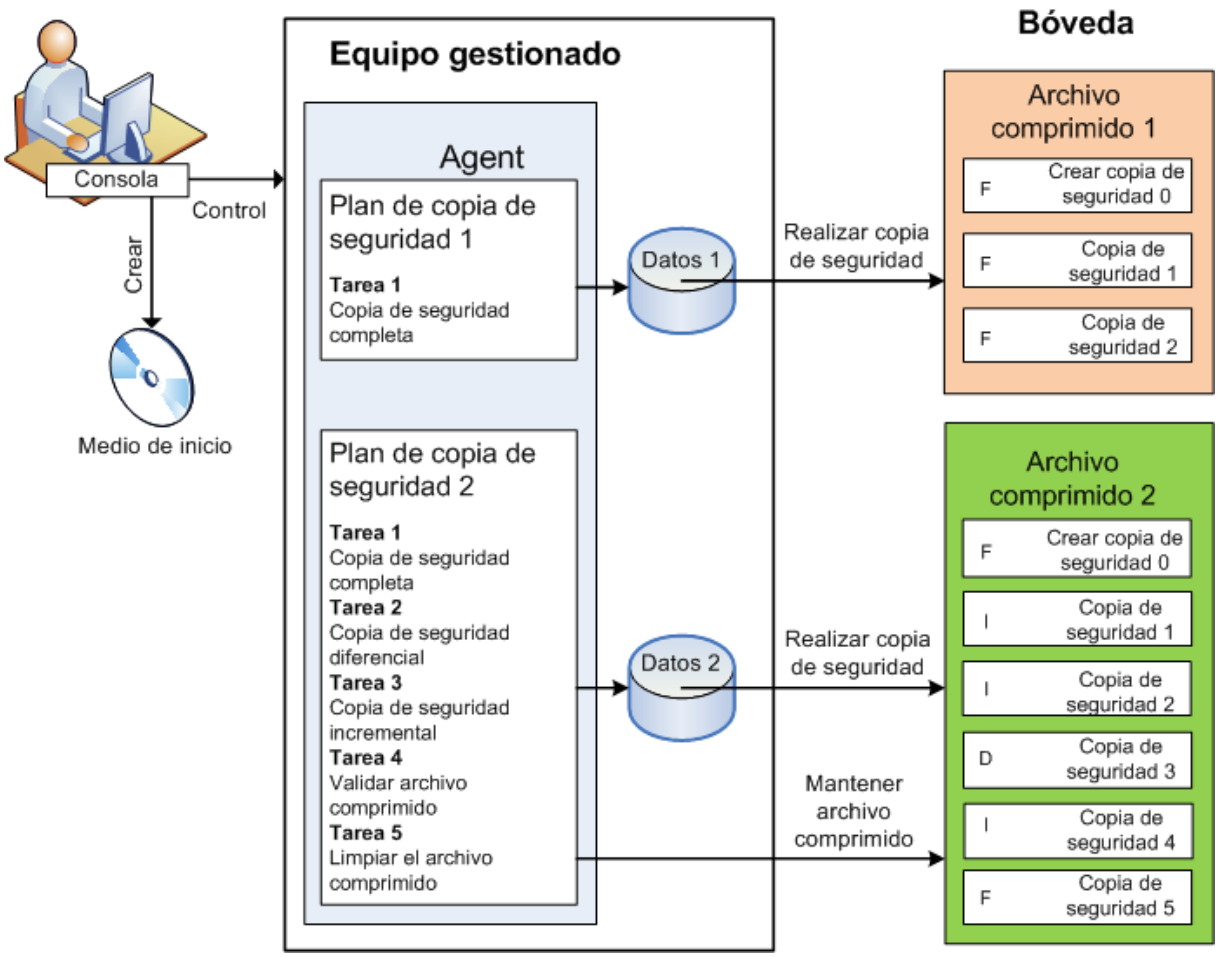
Familiarícese con los conceptos básicos de la interfaz gráfica de usuario y la documentación de Acronis Backup & Recovery 10. Los usuarios avanzados pueden utilizar esta sección como una guía de inicio rápida "paso a paso". Puede encontrar los detalles en la ayuda interactiva.

Copias de seguridad con sistema operativo

1. Para proteger los datos en un equipo, instale el agente (pág. 185) Acronis Backup & Recovery 10 en el equipo que a partir de ese momento será administrado (pág. 190).
2. Para poder administrar este equipo con la Interfaz gráfica de usuario, instale la Consola (pág. 188) de administración de Acronis Backup & Recovery 10 en el equipo desde donde desee operar. Si tiene la versión autónoma del producto, ignore este paso porque en su caso, la consola se instala con el agente.
3. Ejecute la consola. Debe crear un medio de inicio (pág. 195) para poder recuperar el sistema operativo del equipo, si no se puede iniciar el sistema.
4. Conecte la consola al equipo administrado.
5. Cree un plan de copia de seguridad (pág. 196).

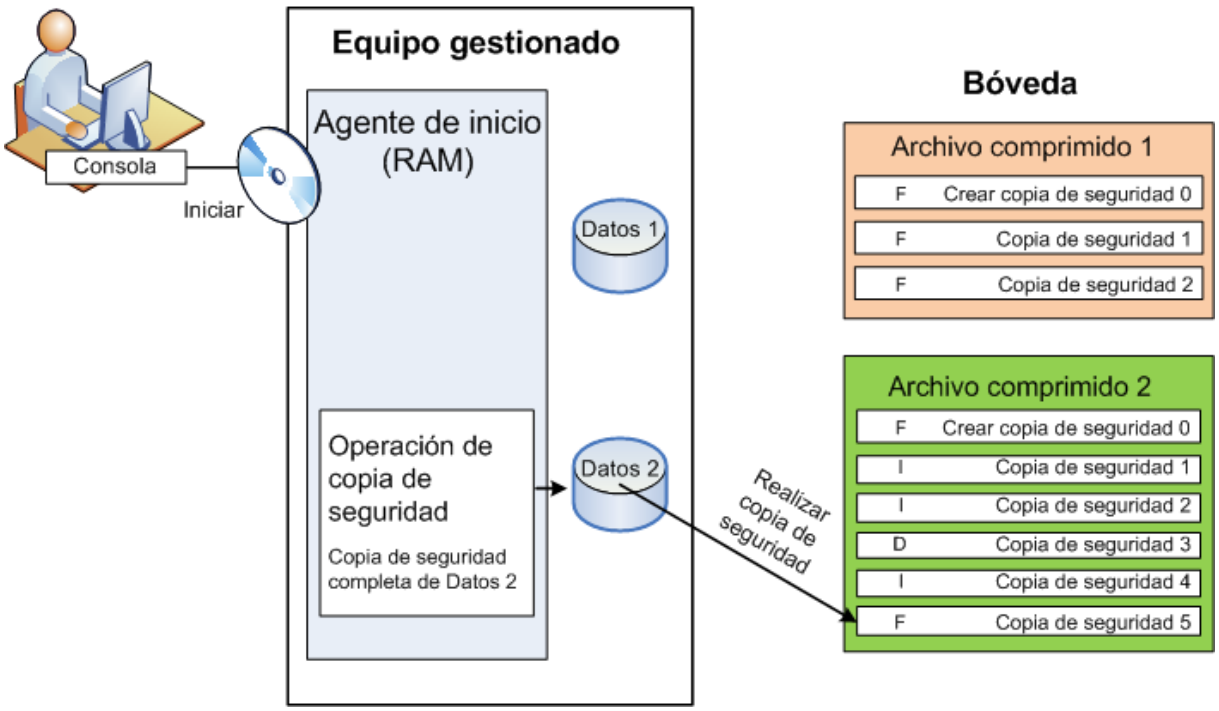
   Para hacerlo, por lo menos, debe especificar los datos a proteger y la ubicación en donde guardar el archivo de copia de seguridad (pág. 186). Esto ayudará a crear un plan de copia de seguridad con una sola tarea (pág. 198) que creará una copia de seguridad (pág. 189) completa de sus datos cada vez que se inicie manualmente la tarea. Un plan complejo de copias de seguridad tiene varias tareas programadas, crean copias completas de seguridad incrementales o diferenciales (pág. 21), realizan operaciones de mantenimiento de archivos como validación (pág. 199) de copias de seguridad o eliminación de copias de seguridad desactualizadas (limpieza (pág. 193) de archivos). Puede personalizar las operaciones de copia de seguridad con varias opciones, como comandos antes y después de copia de seguridad, control del ancho de banda de la red, manejo de errores u opciones de notificación.
6. Use la página de **planes y tareas de la copia de seguridad** para ver la información de sus planes y tareas de copia de seguridad y supervisar su ejecución. Use la página de registro para buscar en el **registro** de las operaciones.
7. La bóveda (pág. 186) es el lugar donde se guardn los archivos de copia de seguridad. Navegue hasta la página de **bóvedas** para ver la información sobre sus bóvedas. Navegue hasta la bóveda específica para ver los archivos y las copias de seguridad y realice operaciones manuales con ellos (montaje, validación, eliminación, visualización de contenidos). También puede seleccionar una copia de seguridad para recuperar sus datos.

El siguiente diagrama ilustra las nociones que se mostraron anteriormente.. Para obtenermás información, consulte el Glosario.



Realice la copia de seguridad con dispositivos de arranque

Puede iniciar el equipo con un medio de inicio, configurar la operación de copias de seguridad de la misma manera que en un plan simple de copia de seguridad y ejecutar la operación. Esto lo ayudará a extraer archivos y los volúmenes lógicos de un sistema que no inicia, a tomar una imagen del sistema fuera de línea o a realizar copias de seguridad sector por sector en un sistema de archivos incompatible.



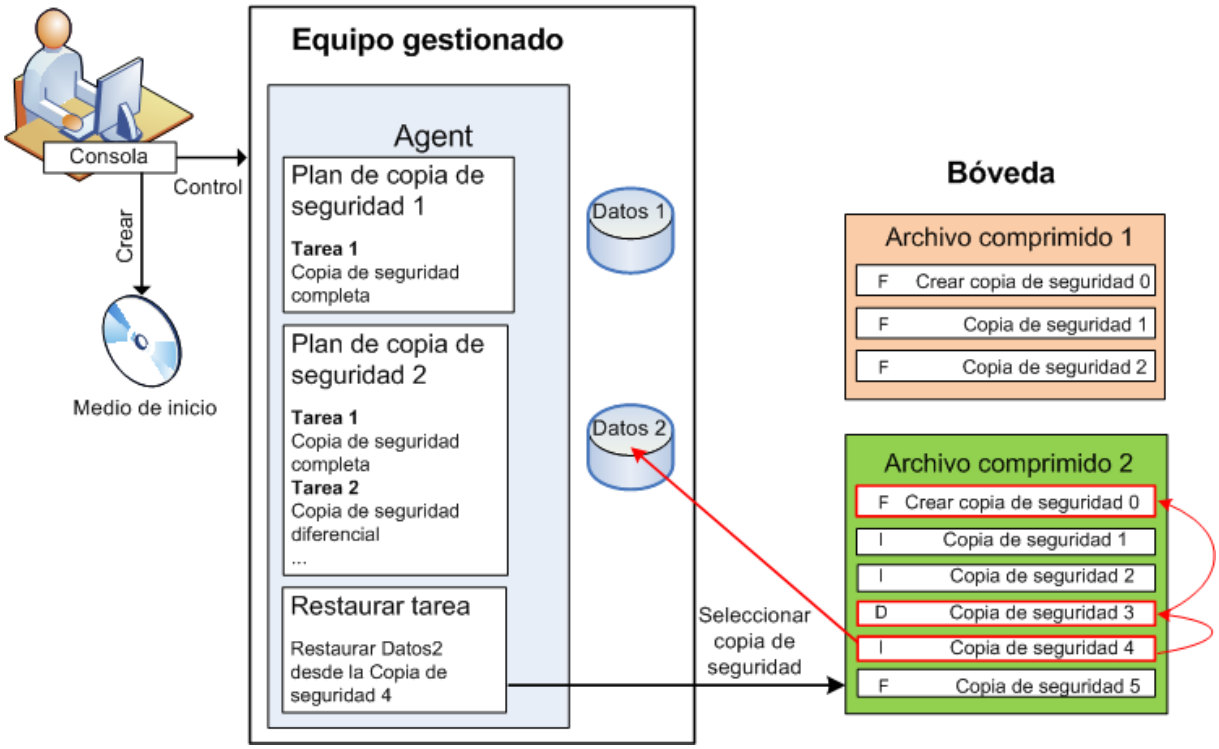
Recuperación con sistema operativo

En cuanto a la recuperación de datos, puede crear una tarea de recuperación en el equipo administrado. Puede especificar la bóveda y seleccionar el archivo y después seleccionar la copia de seguridad en cuanto a la fecha y hora de la creación de la copia de seguridad, o más precisamente, la hora cuando se comenzó la creación. En la mayoría de los casos, se revertirán los datos hasta ese momento.

Ejemplos de excepciones a esta regla:
La recuperación de una base de datos desde una copia de seguridad que contiene un registro de transacción (una sola copia de seguridad proporciona puntos múltiples de recuperación y así puede realizar selecciones adicionales).
La recuperación de varios archivos desde un archivo de copia de seguridad sin instantánea (se revertirá cada archivo al momento en que se copió a la copia de seguridad).

También puede especificar el destino desde donde recuperar los datos. Puede personalizar la operación de recuperación por medio de opciones de recuperación, como los comandos antes y después de recuperación, manejo de errores o las opciones de notificación.

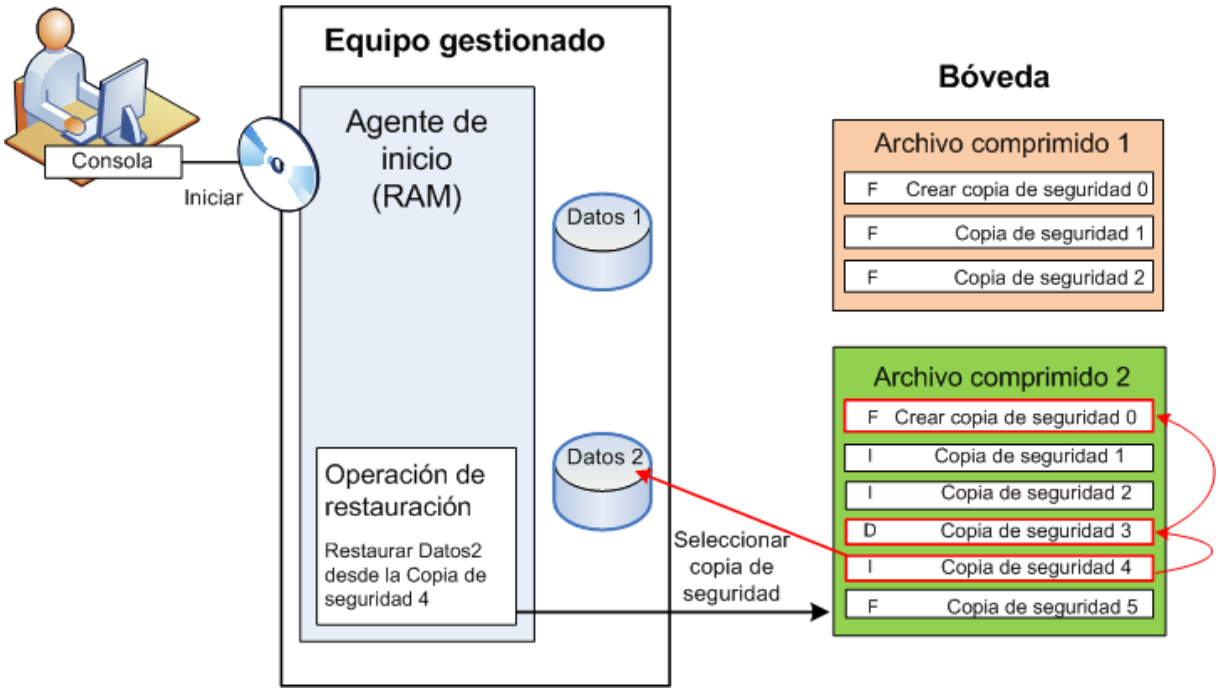
El siguiente diagrama ilustra la recuperación de datos bajo el sistema operativo (en línea). No se puede realizar una copia de seguridad en el equipo mientras se realiza la operación de recuperación. Si fuera necesario, puede conectar la consola a otro equipo y configurar la operación de recuperación en ese equipo. Esta capacidad (recuperación paralela remota) apareció por primera vez en Acronis Backup & Recovery 10; los productos anteriores de Acronis no lo proporcionan.



Recuperación por medio de dispositivos de arranque

La recuperación a partir de un volumen bloqueado por el sistema operativo, como el volumen en donde reside el sistema, requiere de un reinicio en el entorno de arranque que es parte del agente. Después de completar la recuperación, el sistema operativo recuperado se conecta en línea automáticamente.

Si falla el inicio del equipo o si necesita recuperar los datos desde cero, puede iniciar el equipo que tiene los dispositivos de arranque y puede configurar la operación de recuperación del mismo modo como tarea de recuperación. El siguiente diagrama ilustra la recuperación por medio de los dispositivos de arranque.



2.2 Copias de seguridad completas, incrementales y diferenciales

Acronis Backup & Recovery 10 proporciona la capacidad para usar los esquemas de la copia de seguridad populares, como abuelo-padre-hijo y Torres de Hanói, y también para crear esquemas de copia de seguridad personalizados. Todos los esquemas de copia de seguridad están basados en métodos de copia de seguridad diferenciales, incrementales o completos. El término "esquema" denota el algoritmo para aplicar estos métodos para el algoritmo de limpieza del archivo.

Los métodos de comparación entre sí no parecen tener mucho sentido porque los métodos funcionan como un equipo en un esquema de copias de seguridad. Cada método debería tener un rol específico de acuerdo con sus ventajas. Un esquema de copia de seguridad competente podrá sacar provecho de las ventajas de todos los métodos de copias de seguridad y atenúa la influencia de deficiencias de todos los métodos. Por ejemplo, una copia de seguridad diferencial semanal facilita la limpieza del archivo porque se puede borrar fácilmente junto con el conjunto semanal de la copia de seguridad incremental de la que depende.

La realización de la copia de seguridad con los métodos de respaldo completo, incre (pág. 189)mental o diferencial genera una copia de seguridad del tipo correspondiente.

Copia de seguridad completa

Una copia de seguridad completa almacena todos los datos seleccionados para la copia de seguridad. Una copia de seguridad completa está por debajo del nivel de archivo y forma la base para una copia de seguridad incremental y diferencial. Un archivo puede contener múltiples copias de seguridad completas o sólo copias de seguridad completas. Una copia de seguridad es autosuficiente: no

necesita acceso a ninguna otra copia de seguridad para recuperar los datos desde otra copia de seguridad completa.

Se acepta ampliamente que una copia de seguridad es lo más lento pero es lo más rápido de restaurar. Con las tecnologías de Acronis, la recuperación de una copia de seguridad incremental no puede ser más lenta que la recuperación desde una copia completa.

Una copia de seguridad completa es muy útil cuando:

- se debe restaurar el sistema a su estado inicial,
- este estado inicial no cambia con frecuencia, entonces no necesita una copia de seguridad regular.

Ejemplo: Un cibercafé o un laboratorio de una escuela o universidad en donde el administrador debe deshacer los cambios realizados con frecuencia por los estudiantes o invitados y rara vez actualiza la copia de seguridad de referencia (de hecho, lo hacesolamente después de instalar las actualizaciones de software). En este caso, el tiempo de la copia de seguridad no es importante y el tiempo de recuperación será mínimo cuando recupere los sistemas desde la copia de seguridad completa. El administrador puede tener varias copias de la copia de seguridad completa para mayor confiabilidad.

Copia de seguridad incremental

Una copia de seguridad incremental almacena todos los cambios desde la **última copia de seguridad**. Necesita tener acceso a otras copias de seguridad desde el mismo archivo para recuperar los datos con una copia de seguridad incremental.

Una copia de seguridad incremental es muy útil cuando:

- tiene la necesidad de volver a uno de los múltiples estados guardados,
- los cambios de los datos tienden a ser pequeños cuando se lo compara con el tamaño total de los datos.

Se acepta ampliamente que las copias de seguridad incrementales son menos confiables que los completos porque si un "eslabón de la cadena" está dañado, no se puede usar los demás. Sin embargo, guardar varias copias de seguridad múltiples no es una opción cuando necesita múltiples versiones anteriores de sus datos, porque la confiabilidad de un archivo extra grande es más dudoso.

Ejemplo: La realización de una copia de seguridad del registro de transacciones de la base de datos.

Copia de seguridad diferencial

Una copia de seguridad diferencial almacena todos los cambios desde la **última copia de seguridad completa**. Necesita tener acceso a una copia de seguridad completa correspondiente para recuperar los datos desde una copia de seguridad diferencial. Una copia de seguridad diferencial es muy útil cuando:

- usted está interesado en guardar sólo el estado de datos más reciente,
- los cambios de los datos tienden a ser pequeños cuando se lo compara con el tamaño total de los datos.

La conclusión típica es: "Una copia de seguridad diferencial lleva más tiempo para realizar y son más rápidas de recuperar, mientras que las incrementales son las más rápidas de realizar y llevan más para recuperar". De hecho, no hay diferencia física entre la copia de seguridad incremental agregada a la copia de seguridad completa y una copia de seguridad diferencial agregada a la misma copia de seguridad completa en un mismo momento. La diferencia antes mencionada, implica la creación de una copia de seguridad después, o en vez de, crear múltiples copias de seguridad incremental.

Una copia de seguridad incremental o diferencial creada después de la defragmentación de disco podría ser considerablemente más grande de lo normal porque el programa de defragmentación cambia las ubicaciones de los archivos en el disco y las copias de seguridad reflejan estos cambios. Se recomienda crear nuevamente una copia de seguridad completa después de la desfragmentación del disco.

La siguiente tabla resume las ventajas y desventajas de cada tipo de seguridad como aparecen ser de dominio público. En la vida real, estos parámetros dependen de varios factores, como la cantidad, velocidad y patrón de los cambios de los datos, la naturaleza de los datos, las especificaciones de los dispositivos, las opciones que se establecen para la copia de seguridad y recuperación, entre otras. La práctica es la mejor guía para seleccionar el esquema óptimo para la copia de seguridad.

Parámetro	Copia de seguridad completa	Copia de seguridad diferencial	Copia de seguridad incremental
Espacio de almacenamiento	Máximo	Mediano	Mínimo
Hora de creación	Máximo	Mediano	Mínimo
Tiempo de recuperación	Mínimo	Mediano	Máximo

2.3 Privilegios de usuario en un equipo administrado

Cuando se administra un equipo donde se ejecuta Linux, el usuario tiene u obtiene los privilegios de raíz y entonces puede:

- Realizar la copia de seguridad y la recuperación de cualquier dato o todo el equipo, con todo el control del agente de Acronis Backup & Recovery 10 y las operaciones y archivos de registro en el equipo.
- Administrar los planes y tareas de la copia de seguridad local que son propiedad de cualquier usuario registrado en el sistema operativo.

Para evitar el registro de la rutina en el sistema como raíz, el superusuario se puede registrar con las credenciales de usuario normales y entonces cambiar de usuario como lo necesite.

2.4 Propietarios y credenciales

Esta sección explica el concepto de propietario y el significado de las credenciales del plan (o tarea) de la copia de seguridad.

Propietario del plan (tarea)

El propietario del plan local de la copia de seguridad es del último usuario que modificó o creó la tarea.

El propietario del plan centralizado de la copia de seguridad es el administrador del management server que creó o fue el último en modificar la política centralizada que generó el plan.

La tareas que pertenecen a un plan de copia de seguridad, tanto local como centralizado, son del propietario del plan de la copia de seguridad.

Las tareas no pertenecen al plan de copia de seguridad, como sucede con las tareas de recuperación, sino que son propiedad del último usuario que modificó o creó la tarea.

Administración de un plan (tarea) que es propiedad de otro usuario

Si un usuario tiene derechos de Administrador en un equipo, puede modificar las tareas y los planes de copia de seguridad locales que cualquier usuario registró en el sistema operativo.

Cuando un usuario abre un plan o tarea para edición, que es propiedad de otro usuario, se borran todas las contraseñas de la tarea. Esto evita el truco "modificar la configuración, dejar la contraseña". El programa muestra una advertencia cada vez que intenta editar un plan (tarea) que fue modificada por otro usuario. Al ver la advertencia, tiene dos opciones:

- Hacer clic en **Cancelar** y cree su propio plan o tarea. La tarea original permanecerá intacta.
- Continuar con la edición. Deberá ingresar todas las credenciales requeridas para la ejecución del plan o tarea.

Propietario del archivo

El propietario del archivo es el usuario que guardó el archivo en su destino. Para más exactitud, es el usuario cuya cuenta se especificó cuando se creó el plan de copia de seguridad en el paso **Dónde realizar copias de seguridad**. Por defecto, su usan las credenciales del plan.

Las credenciales del plan y las de las tareas.

Es cualquier tarea que se ejecute en un equipo por arte de un usuario. Cuando crea un plan o una tarea, tiene la opción de especificar claramente una cuenta en la que se ejecutará dicho plan o la tarea. Su opción depende de si el plan o la tarea se utilizan para un inicio manual o para la ejecución programada.

Inicio manual

Puede evitar el paso sobre **credenciales de planes (tareas)**. Cada vez que comienza la tarea, la tarea se ejecutará con las credenciales con las que ingresó actualmente. Cualquier persona que tenga privilegios administrativos en el equipo también puede iniciar la tarea. Se ejecutará la tarea con las credenciales de las personas.

La tarea siempre ejecutará con las mismas credenciales, independientemente del usuario que inició la tarea, si especifica las credenciales de las tareas explícitamente. Para hacerlo, en la página de creación del plan (tarea) debe:

1. Seleccionar la casilla de verificación **Vista avanzada**.
2. Seleccionar: **Cambio general -> Credenciales del plan (tarea)**.
3. Ingrese las credenciales con las que se ejecutará el plan (tarea).

Inicio programado o postergado.

Las credenciales del plan (tarea) son obligatorias. Si evita el paso de las credenciales, se le pedirá las credenciales después de terminar la creación del plan (tarea).

¿Por qué el programa obliga a especificar las credenciales?

Se debe ejecutar una tarea programada o postergada de todos modos, independientemente de si el usuario está conectado o no (por ejemplo, el sistema en la ventana de "Bienvenida" de Windows) o si hay otro usuario conectado además del propietario de la tarea. Basta que el equipo esté encendido (es decir, no en modo espera o hibernación) a la hora que se programó la tarea. Esa es la razón por lo que el programador de Acronis necesita que las credenciales especificadas explícitamente para que pueda cargar la tarea.

2.5 Esquema GFS de copia de seguridad

Esta sección cubre la implementación del esquema de copia de seguridad del tipo "abuelo-padre-hijo" (GFS) en Acronis Backup & Recovery 10.

Con este esquema de copia de seguridad no puede realizar copias de seguridad más de una vez por día. El esquema le permite marcar los ciclos diarios, semanales y mensuales en su programa diario de copia de seguridad y especificar los períodos de retención para las copias de seguridad diarias, semanales y mensuales. A las copias de seguridad se las llama "hijos", a las semanales "padres" y a las copias de seguridad de más larga vida se las llama "abuelos".

GFS como esquema de rotación de cintas

Al principio, se creó a GFS como un esquema de rotación de cintas. Los esquemas de rotación de cintas, como tales, no están automatizados. Sólo determinan:

- la cantidad de cintas que se necesitan para permitir la recuperación con la resolución deseada (el intervalo de tiempo entre los puntos de recuperación) y el período de restauración;
- qué cintas se deben sobrescribir con la siguiente copia de seguridad.

El esquema de rotación de cintas le permite arreglárselas con la cantidad mínima de cartuchos en vez de estar sepultado en cintas usadas. Hay muchas fuentes en Internet que describen las variedades de los esquemas GFS de cintas. Tiene la libertad para usar cualquiera de las variables al hacer las copias de seguridad con un dispositivo de cinta conectado a nivel local.

GFS de Acronis

Con Acronis Backup & Recovery 10, puede establecer fácilmente un plan de copia de seguridad que realizará regularmente copias de seguridad de los datos y realizará una limpieza del archivo comprimido resultante de acuerdo con el esquema GFS.

Cree el plan de copia de seguridad como siempre. Para el destino de la copia de seguridad, seleccione un dispositivo de almacenamiento en que se pueda realizar la limpieza, como un dispositivo de almacenamiento basado en HDD o un sistema robotizado de cintas. (Como no se puede usar el espacio liberado en la cinta después de la limpieza, hasta que la cinta esté libre, tenga en cuenta ciertas consideraciones adicionales cuando use el esquema GFS en un sistema robotizado.)

La siguiente es una explicación de las configuración que es específica para el esquema de GFS de copias de seguridad.

Las configuraciones relacionadas a GFS del plan de copia de seguridad

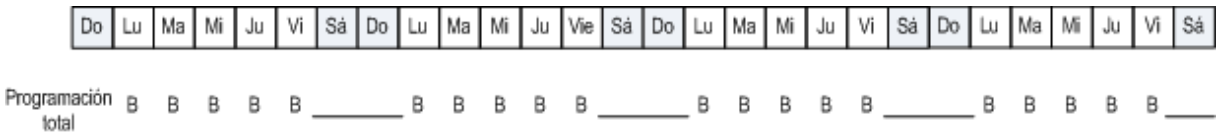
Comienzo de la copia de seguridad en:

Copia de seguridad en:

Este paso crea el total del programa de la copia de seguridad, es decir, define todos los días en los que se necesita la copia de seguridad.

Asumiremos que se selecciona la copia de seguridad a las 20:00 en los días laborales. Aquí está el programa completo que definió.

“B” significa “Copia de seguridad”.



Programa completo.
Programa: Días laborales a las 20:00.

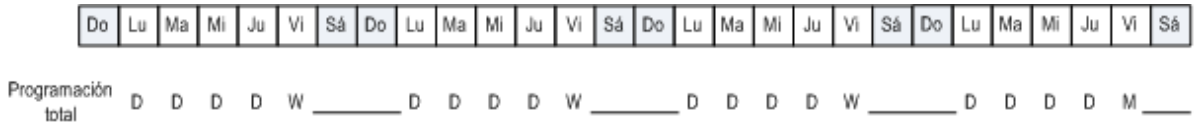
Semanalmente/mensualmente

Este paso crea los ciclos diario, semanales y mensuales del programa.

Seleccione un día de la semana de los que seleccionó en el paso anterior. Cada 1era, 2da y 3era copia de seguridad realizada en este día de la semana, será considerado como una copia de seguridad semanal. La 4ª copia de seguridad realizada en este día de la semana se considerará como una copia de seguridad semanal. Las copias de seguridad realizadas en otros días se considerarán como copias de seguridad diarios.

Asumiremos que se selecciona "Viernes" para las copias de seguridad semanales. Aquí se tiene el total del programa marcado de acuerdo a la selección.

“D” significa que a la copia de seguridad se la considera diaria. “W” significa que a la copia de seguridad se la considera semanal. “M” significa que a la copia de seguridad se la considera mensual.

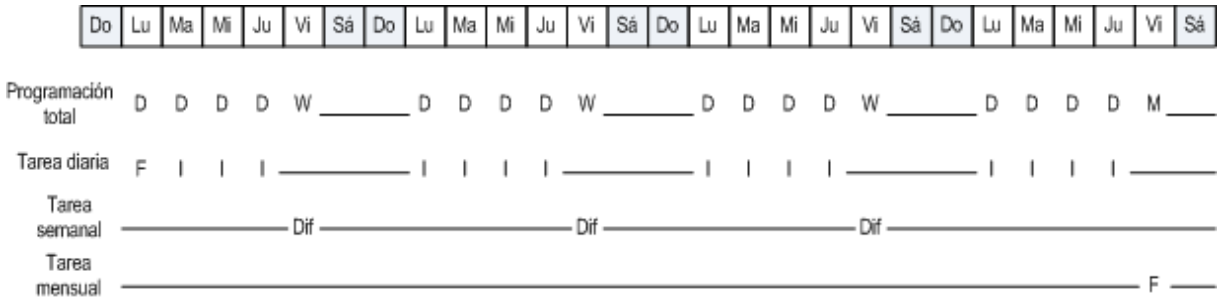


El programa marcado de acuerdo al esquema GFS.
Programa: Días laborales 20:00.
Semanal/mensual: Viernes

Acronis utiliza las copias de seguridad incrementales y diferenciales que ayudan a ahorrar espacio de almacenamiento y optimiza la limpieza que necesita la consolidación. En cuanto a métodos de copias de seguridad, la copia de seguridad semanal es diferencial (Dif.), la copia de seguridad mensual es completa (F) y las copias de seguridad diarias son incrementales (I). La primera copia de seguridad siempre es completa.

El parámetro semanal/mensual divide el esquema total en programas diarios, semanales y mensuales.

Asumiremos que se selecciona "Viernes" para las copias de seguridad semanales. Aquí está el programa real de las tareas de copias de seguridad que se realizarán.



Las áreas de copias de seguridad realizadas de acuerdo con esquema GFS de Acronis Backup & Recovery 10.
Programa: Días laborales 20:00.
Semanal/mensual: Viernes

Mantener copias de seguridad: Diariamente

Este paso define la regla de retención para copias de seguridad diarias. La tarea de limpieza se ejecutará después de cada copia de seguridad diaria y se eliminarán las copias de seguridad que sean anteriores a la fecha indicada.

Mantener copias de seguridad: Semanalmente

Este paso define la regla de retención para copias de seguridad semanales. La tarea de limpieza se ejecutará después de cada copia de seguridad semanal y se eliminarán las copias de seguridad que sean anteriores a la fecha indicada. El período de retención de las copias de seguridad semanales no puede ser menor al período de retención de las copias de seguridad diarias. Por lo general, son varias veces más largas.

Mantener copias de seguridad: Mensualmente

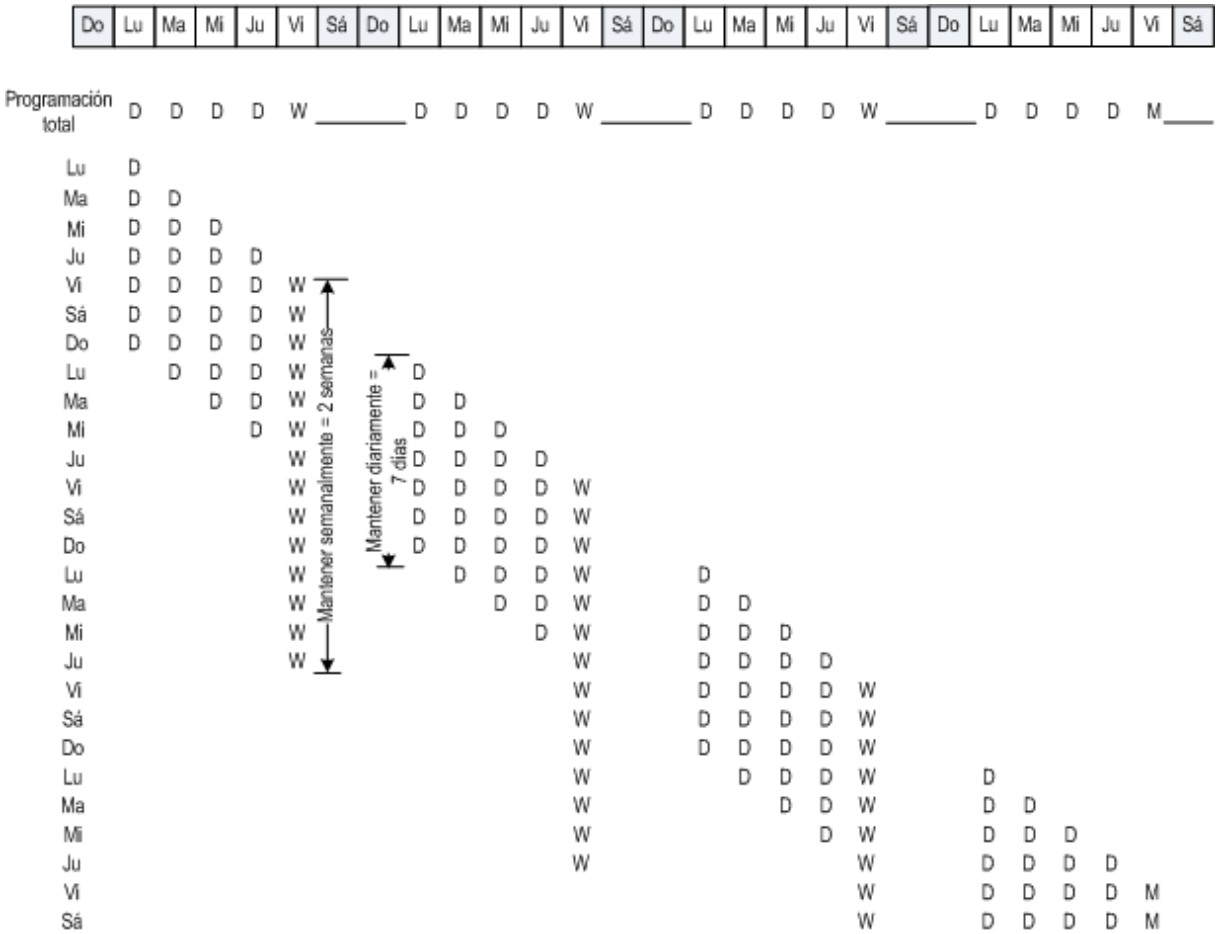
Este paso define la regla de retención para copias de seguridad mensuales. La tarea de limpieza se ejecutará después de cada copia de seguridad mensual y se eliminarán las copias de seguridad que sean anteriores a la fecha indicada. El período de retención de las copias de seguridad mensuales no puede ser menor al período de retención de las copias de seguridad semanales. Por lo general, son varias veces más largas. Es posible mantener las copias de seguridad mensuales infinitamente.

Archivo comprimido resultante: Ideal

Asumiremos que se mantienen las copias de seguridad diarias durante siete días, las semanales durante 2 semanas y las mensuales durante 6 meses. Así se quedaría el archivo después de que se inicie el plan de copia de seguridad si todas las copias de seguridad son completas y entonces se las podrían eliminar tan pronto como lo requiera el programa.

La columna izquierda muestra los días de la semana. Por cada día de la semana, el contenido del archivo después de la copia de seguridad y se muestra la limpieza posterior.

“D” significa que a la copia de seguridad se la considera diaria. “W” significa que a la copia de seguridad se la considera semanal. “M” significa que a la copia de seguridad se la considera mensual.



Un archivo ideal creado de acuerdo al esquema GFS.
Programa: Días laborales 20:00.
Semanal/mensual: Viernes
Mantener las copias de seguridad diarias: 7 días
Mantener las copias de seguridad semanales: 2 semanas
Mantener las copias de seguridad mensuales: 6 meses

Al comenzar desde la tercera semana, se eliminará regularmente las copias de seguridad semanales. Después de seis meses, se comenzarán a eliminar las copias de seguridad mensuales. El diagrama para las copias de seguridad semanal y mensual se parecerán a la escala de tiempo.

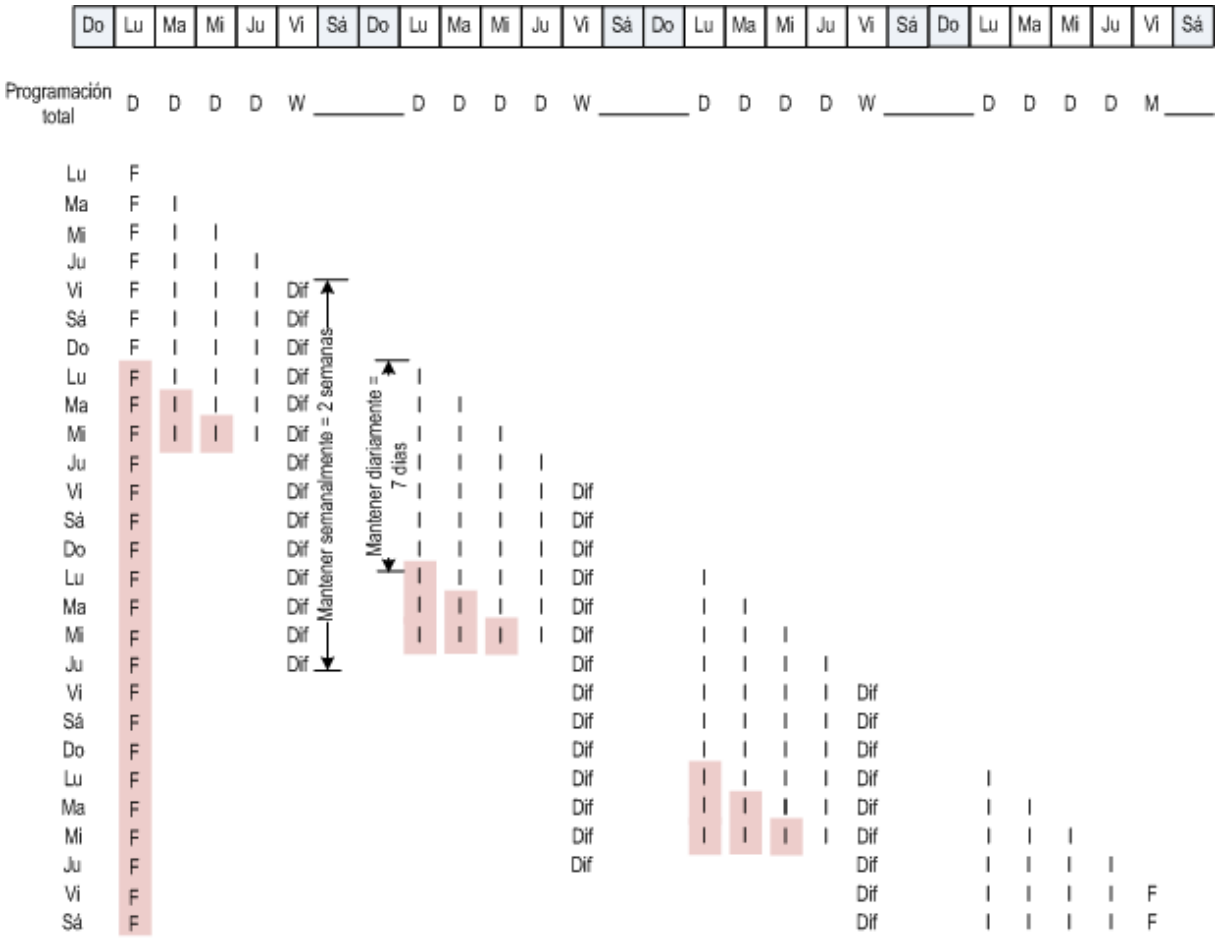
Archivo comprimido resultante: Real

En realidad, el contenido del archivo será un poco diferente al programa ideal.

Cuando se use los métodos de copias de seguridad incrementales y diferenciales, no podrá eliminar las copias de seguridad tan pronto como lo requiera el esquema si las copias de seguridad posteriores se basan en esa copia. Una consolidación regular no es aceptable porque requiere de muchos recursos del sistema. El programa debe esperar hasta que el esquema requiera de la eliminación de todas las copias de seguridad dependientes y entonces allí podrá eliminar la cadena completa.

Aquí se muestra como se verá el primer mes de su plan de copias de seguridad en la vida real. “F” significa copia de seguridad completa. “Dif.” significa copia de seguridad diferencial. “I” significa copia de seguridad incremental.

Las copias de seguridad que sobreviven a su vida útil nominal debido a dependencias, están marcadas con rosa. La copia de seguridad completa inicial será eliminada tan pronto como se eliminen todas las copias de seguridad incrementales y diferenciales basadas en esa copia de seguridad.



Un archivo creado de acuerdo al esquema GFS de Acronis Backup & Recovery 10.
Programa: Días laborales 20:00.
Semanal/mensual: Viernes
Mantener las copias de seguridad diarias: 7 días
Mantener las copias de seguridad semanales: 2 semanas
Mantener las copias de seguridad mensuales: 6 meses

2.6 Esquema de copias de seguridad Torres de Hanói

La necesidad de copias de seguridad frecuentes siempre entra en conflicto con el costo de mantenerlas por un período largo. El esquema de copias de seguridad Torres de Hanói (ToH) es unarreglo útil.

Generalidades de Torres de Hanói

El esquema de la Torres de Hanói se basa en un juego matemático del mismo nombre. En el juego hay varios aros guardados de acuerdo con su tamaño, los más grandes en el fondo, en una de las tres estacas. El objetivo es mover los aros a la tercera estaca. Sólo puede mover un aro a la vez y está prohibido ubicar un aro más grande arriba de otro más pequeño. La solución es cambiar el primer aro en cada movimiento (mueve 1, 3, 5, 7, 9, 11...), el segundo aro a intervalos de cuatro movimientos (mueve 2, 6, 10...), el tercer aro en intervalos de ocho movimientos (mueve 4, 12...), y así.

Por ejemplo, si hay cinco aros con la etiqueta A, B, C, D, y E en el juego, la solución es la siguiente cadena de movimientos:

Aro \ Mover	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
1	A		A		A		A		A		A		A		A		A		A		A		A		A		A		A		A
2		B				B				B				B				B				B				B				B	
3				C								C								C								C			
4								D																D							
5																E															

El esquema de la Torres de Hanói para copias de seguridad se basa en los mismos patrones. Funciona con **Sessions** en vez de **Movimientos** y **niveles de Copia de seguridad** en vez de **Aros.** Por lo general, un patrón de esquema de nivel-N, contiene las sesiones (N-th potencia de dos).

Entonces, el esquema de la Torres de Hanói para copias de seguridad de cinco niveles, consiste en 16 sesiones (mueve de 1 a 16 en la ilustración anterior).

La tabla muestra el patrón para el esquema de copia de seguridad. El patrón consiste en 16 sesiones.

Nivel de copia de seguridad \ Sesión	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	A		A		A		A		A		A		A		A	
2		B				B				B				B		
3				C								C				
4								D								
5																E

El esquema de la Torres de Hanói para copias de seguridad mantiene sólo una copia de seguridad por nivel. Se debe eliminar todas las copias de seguridad desactualizadas. Entonces el esquema permite el almacenamiento eficiente de datos: la mayoría de copias de seguridad se acumula hacia el tiempo presente. Si se tienen 4 copias de seguridad, puede recuperar los datos desde hoy, ayer o hace media semana atrás, o una semana atrás. Para el esquema de cinco niveles, también puede recuperar los datos respaldados hasta dos semanas atrás. Cada copia de seguridad adicional duplica el período máximo de restauración de sus datos.

Torres de Hanói por Acronis

Por lo general, el esquema de la Torres de Hanói para copias de seguridad es muy complejo como para calcular mentalmente el siguiente medio a usar. Pero Acronis Backup & Recovery 10 proporciona la automatización del uso de esquemas Puede establecer el esquema de copias de seguridad mientras crea el plan de copia de seguridad.

Implementación de Acronis para las siguientes características:

- hasta 16 niveles de copias de seguridad
- las copias de seguridad incrementales en el primer nivel (A): para ganar tiempo y ahorrar almacenamiento para las operaciones más frecuentes de copias de seguridad; pero la recuperación de datos de dichas copias de seguridad lleva más tiempo porque requiere acceso a tres copias de seguridad

- las copias de seguridad completas del último nivel (E para el patrón de cinco niveles): las copias de seguridad más raras en el esquema, lleva más tiempo y ocupa más espacio en el almacenamiento
- las copias de seguridad diferenciales en todos los niveles intermedios (B, C y D para el patrón de cinco niveles)
- la configuración comienza con una copia de seguridad debido a que la primera copia de seguridad no puede ser incremental
- el esquema obliga a cada nivel de copia de seguridad a mantener sólo la copia de seguridad más reciente, se debe eliminar otras copias de seguridad del nivel; sin embargo, se pospone la eliminación de la copia de seguridad en los casos donde la copia de seguridad es la base para otra incremental o diferencial
- se mantiene una copia de seguridad anterior en un nivel hasta que se haya creado copia de seguridad satisfactoriamente en el nivel.

La tabla muestra el patrón para el esquema de copia de seguridad. El patrón consiste en 16 sesiones.

Nivel de copia de seguridad \ Sesión	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1 (Incremental)		A		A		A		A		A		A		A		A
2 (Diiferencial)			B				B				B				B	
3 (Diiferencial)					C								C			
4 (Diiferencial)									D							
5 (Completo)	E															

Como resultado de usar copias de seguridad incrementales y diferenciales, es posible que haya una copia de seguridad cuya eliminación se posponga porque es la base para otras copias de seguridad. La tabla siguiente indica el caso cuando se pospone en la sesión 17 la eliminación de una copia de seguridad completa en la sesión 1 hasta la sesión 25 porque la copia de seguridad diferencial (D) creada en la sesión 9 todavía es actual. En la tabla, las celdas con copias de seguridad eliminadas están desactivadas.

Nivel de copia de seguridad \ Sesión	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
1 (Incremental)		A		A		A		A		A		A		A		A		A		A		A		A	
2 (Diferencial)			B				B				B				B				B				B		
3 (Diferencial)					C								C								C				
4 (Diferencial)									D																D
5 (Completo)	E																E								

La copia de seguridad diferencial (D), creada en la sesión 9, será eliminada en la sesión 25 después de que se complete la creación de una nueva copia de seguridad diferencial. De esta manera, un archivo de copia de seguridad creado con el esquema de Torres de Hanói por Acronis puede incluir hasta dos copias adicionales de seguridad de acuerdo a la implementación clásica del esquema.

Para obtener más información sobre el uso de la Torres de Hanói con bibliotecas de cintas, consulte Uso del esquema de rotación de cintas con Torres de Hanói.

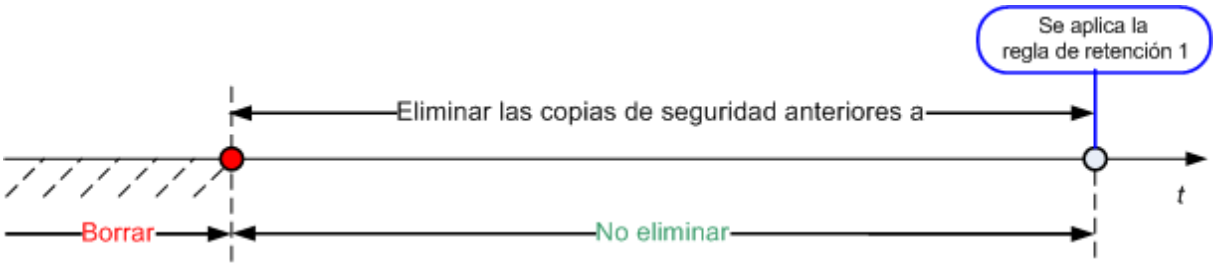
2.7 Reglas de retención

Las copias de seguridad realizadas por un plan de copias de seguridad crean un archivo comprimido. Las dos reglas de retención que se describen en esta sección le permiten limitar el tamaño del archivo comprimido y establecer su vida útil (período de retención) de las copias de seguridad.

Las reglas de retención son eficaces si el archivo comprimido tiene más de una copia de seguridad. Esto significa que se guardará la última copia de seguridad del archivo comprimido aunque se detecte una violación a una regla de retención. No intente borrar la única copia de seguridad de la que dispone al aplicar las reglas de retención *antes* de realizar la copia de seguridad. No funcionará. Utilice la configuración alternativa **Limpiar archivo comprimido** > **Cuando no haya espacio suficiente al realizar la copia de seguridad** (pág. 134) si acepta el riesgo de perder la última copia de seguridad.

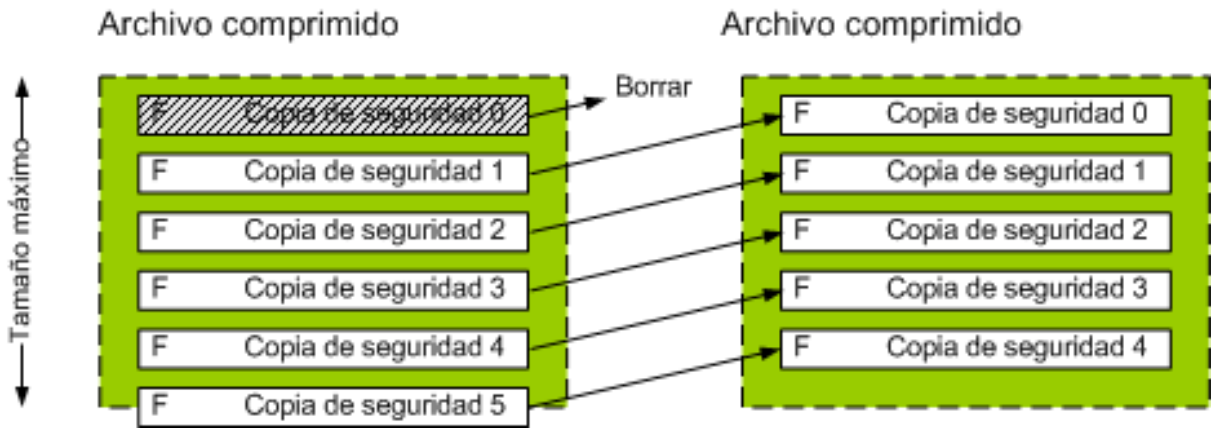
1. Eliminar las copias de seguridad anteriores a:

Es un intervalo de tiempo que se calcula desde el momento que se aplicaron las reglas de retención. Cada vez que se aplica una regla de retención, el programa calcula la fecha y hora en el pasado que corresponde a ese intervalo y elimina todas las copias de seguridad anteriores a ese momento. No se eliminará ninguna de las copias de seguridad creadas después de ese momento.



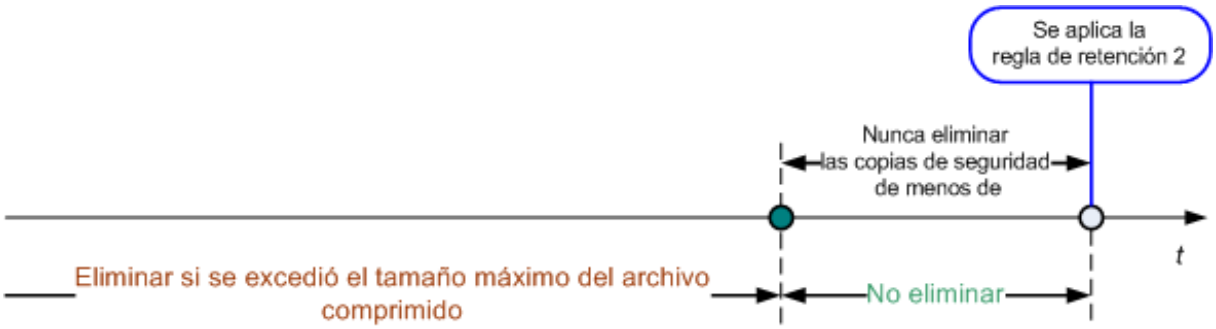
2. Mantener el tamaño del archivo comprimido en:

Este es el tamaño máximo del archivo comprimido: cada vez que se aplica una regla de retención, el programa compara el tamaño actual del archivo comprimido con el valor que estableció y elimina las copias de seguridad más viejas para mantener el tamaño del archivo comprimido dentro de ese valor. El siguiente diagrama muestra el contenido del archivo comprimido antes y después de la eliminación.



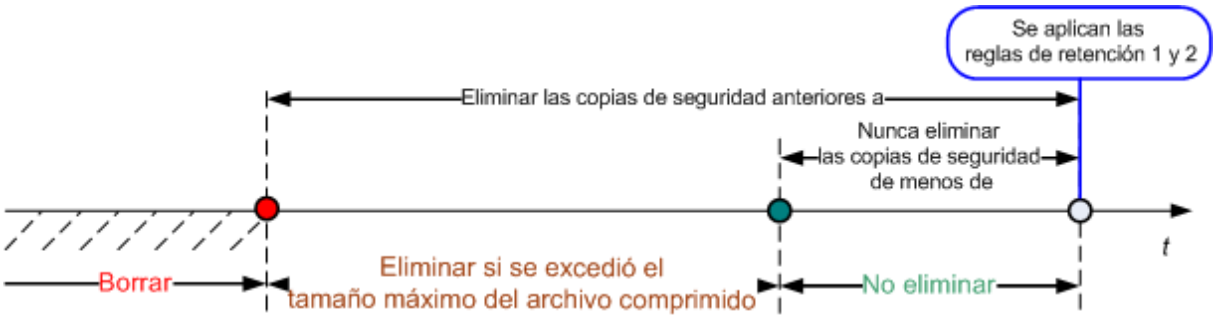
Existe el riesgo de que se eliminen todas las copias de seguridad menos una si se estableció de manera incorrecta el tamaño del archivo comprimido (demasiado pequeño) o una copia de seguridad resulta ser demasiado grande. Seleccione la casilla de verificación **No eliminar las copias de**

seguridad de menos de y especifique el tiempo máximo que se deben retener las copias de seguridad para evitar que se eliminen las copias de seguridad recientes. El siguiente diagrama ilustra la regla resultante.



Combinación de reglas 1 y 2.

Puede limitar la vida útil de ambas copias de seguridad y el tamaño del archivo comprimido. El siguiente diagrama ilustra la regla resultante.



Ejemplo

Eliminar las copias de seguridad con más de: 3 meses.

Mantener el tamaño del archivo comprimido en: 200 GB

No eliminar las copias de seguridad menores a: 10 días.

- Cada vez que se aplica una regla de retención, el programa eliminará las copias de seguridad creadas que tengan más de 3 meses (o concretamente, 90 días).
- Si después de la eliminación, el tamaño del archivo es más de 200 GB y la última copia de seguridad tiene más de 10 días, el programa eliminará la copia de seguridad.
- Después, si es necesario, se eliminará la siguiente copia de seguridad hasta que el tamaño del archivo comprimido alcance el límite prestablecido o la copia de seguridad más antigua tenga 10 días.

Eliminación de las dependencias de las copias de seguridad

Ambas reglas de retención presumen la eliminación de algunas copias de seguridad y la retención de otras. ¿Que sucede si un archivo contiene copias de seguridad incrementales y diferenciales que dependen de la otra y de la completa en la que se basan? No se puede eliminar una copia de seguridad completa desactualizada y mantener a sus "secundarias" incrementales.

Cuando la eliminación de la copia de seguridad afecta a otras copias de seguridad, se aplica una de las siguientes reglas:

- **Se retiene la copia de seguridad hasta que se puedan eliminar las dependientes**

  Se mantendrá la copia de seguridad desactualizada hasta que se actualicen todas las copias de seguridad dependientes. Entonces, se eliminará toda la cadena durante una limpieza regular. Este modo ayuda a evitar una potencial consolidación que requiera mucho tiempo pero que requiera de espacio adicional para almacenar las copias de seguridad cuya eliminación se postergó. El tamaño del archivo comprimido y su antigüedad pueden superar los valores especificados.

- **Consolidar la copia de seguridad**

  El programa consolidará la copia de seguridad que está sujeta a eliminación en la siguiente copia de seguridad dependiente. Por ejemplo, las reglas de retención requieren la eliminación de una copia de seguridad completa pero retienen la siguiente incremental. Las copias de seguridad se combinarán en una sola copia de seguridad completa que tendrá la fecha de la copia de seguridad incremental. Cuando se elimina una copia de seguridad incremental o diferencial de la mitad de la cadena, el tipo de copia de seguridad resultante será incremental.

  Este modo asegura que después de cada limpieza, el tamaño del archivo y su antigüedad estarán dentro de los límites especificados. Sin embargo, la consolidación puede tomar mucho tiempo y muchos recursos del sistema. Y necesitará espacio adicional en la bóveda para los archivos temporales creados durante la consolidación.

  Lo que necesita saber sobre consolidación

  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.

  Las copias de seguridad resultantes de la consolidación siempre usarán la compresión máxima. Esto significa que todas las copias de seguridad en un archivo comprimido usarán la compresión máxima como resultado de una limpieza repetida con consolidación.

Las mejores prácticas

Mantenga el equilibrio entre la capacidad del dispositivo de almacenamiento, los parámetros restrictivos que establece y la frecuencia de limpieza. Las reglas de retención lógica asumen que la capacidad del dispositivo de almacenamiento es mucho mayor al de una copia de seguridad promedio y que el tamaño máximo del archivo comprimido no se acerca a la capacidad física de almacenamiento, pero deja una reserva razonable. Debido a esto, si se excede el tamaño del archivo comprimido entre las ejecuciones de las tareas de limpieza, no será un problema para el proceso comercial. Cuanto menor sea la cantidad de ejecuciones de limpieza, mayor será el espacio necesario para almacenar las copias de seguridad que ya pasaron su vida útil.

La página Bóvedas (pág. 77) le proporciona información sobre espacio libre disponible en cada bóveda. Compruebe esta página periódicamente. Si el espacio libre (que en definitiva es el espacio libre en el dispositivo de almacenamiento) se acerca a cero, es posible que deba aumentar las restricciones o los archivos en la bóveda.

2.8 Realización de copias de seguridad de volúmenes LVM y de dispositivos MD (Linux)

Esta sección explica cómo se hacen copias de seguridad y se recuperan volúmenes, gestionado por Linux Logical Volume Manager (LVM), conocido como volúmenes lógicos; y dispositivos de múltiples discos (MD), conocido como Software RAID deLinux .

2.8.1 Realización de copias de seguridad de volúmenes lógicos

Acronis Backup & Recovery 10 Agent para Linux puede tener acceso, realizar las copias de seguridad y recuperar dichos volúmenes cuando se ejecuta en Linux con kernel 2.6.x o un dispositivo de inicio basado en Linux.

Interfaz gráfica de usuario de copia de seguridad

En la Acronis Backup & Recovery 10 interfaz gráfica de usuario, los volúmenes lógicos aparecen bajo **volúmenes GPT y dinámicos** al final de la lista de los volúmenes disponibles para la copia de seguridad.

Para realizar copias de seguridad de todos los discos disponibles, especifique todos los volúmenes lógicos además de los volúmenes básicos que no pertenecen a éstos. Esta es la selección predeterminada cuando abre la página **Creación de plan de copia de seguridad**.

Los volúmenes básicos incluidos en los volúmenes lógicos se muestran en la lista con la columna **Sistema de archivo** en **ninguno**. Si selecciona dichos volúmenes, el programa les hará la copia de seguridad sector por sector. Por lo general, esto no es necesario.

Restaurar

Al recuperar volúmenes lógicos tiene dos opciones:

- **Recuperar únicamente los contenidos del volumen**. No se cambiará el tipo u otras propiedades del volumen de destino.

  Esta opción está disponible tanto en el sistema operativo como en dispositivos de inicio.

  Esta opción es muy útil en los casos siguientes:

  - Cuando se han perdido algunos datos en el volumen y no se ha reemplazado ningún disco duro.
  - Cuando se recupera volumen lógico sobre un disco básico (MBR) o volumen. En este caso puede cambiar el tamaño del volumen resultante.

    Un sistema, recuperado desde una copia de seguridad de un volumen lógico en un disco MBR básico, no puede iniciar porque su núcleo intenta montar el sistema de archivos raíz en el volumen lógico. Para iniciar el sistema, cambie la configuración del cargador y /etc/fstab para que LVM no se utilice y reactive su cargador de inicio (pág. 151).

  - Al recuperar un volumen básico o lógico a un volumen lógico creado previamente. Este es el caso al crear la estructura de volúmenes lógicos de forma manual utilizando la utilidad **lvm**.
- **Recuperación tanto de la estructura de volúmenes lógicos como de sus contenidos**.

  Este es el caso con la recuperación desde cero o en un equipo con diferente estructura de volumen. La estructura de volúmenes lógicos puede crearse de forma automática en el momento de la recuperación en caso de haber sido guardada en la copia de seguridad (pág. 36).

  Esta opción sólo está disponible cuando se trabaja desde dispositivos de inicio.

Para obtener instrucciones más detalladas sobre como recuperar volúmenes lógicos, consulte Recuperación de dispositivos MD y volúmenes lógicos (pág. 180).

Enlace útil:

- http://tldp.org/HOWTO/LVM-HOWTO/.

2.8.2 Realización de copias de seguridad de dispositivos MD

Los dispositivos MD combinan varios volúmenes MD y crean dispositivos de bloques sólidos (/dev/md0, /dev/md1, ..., /dev/md31). La información acerca de los dispositivos MD está almacenada en /etc/raidtab o en áreas dedicadas de dichos volúmenes.

Puede realizar copias de seguridad de dispositivos MD (montados) activos de la misma manera que con los volúmenes lógicos. Los dispositivos MD aparecen al final de la lista de volúmenes disponibles para la copia de seguridad.

La copia de seguridad de volúmenes incluidos en dispositivos MD no tiene ningún sentido cuando un dispositivo MD está montado, de la misma forma que no será posible recuperarlos.

Al recuperar dispositivos MD bajo dispositivos de inicio, la estructura de los dispositivos MD puede crearse de forma automática en caso de haber sidoguardados en la copia de seguridad (pág. 36). Para obtener información detallada acerca de la recuperación de dispositivos MD cuando se trabaja desde dispositivos de inicio, vaya a Recuperación de dispositivos MD y volúmenes lógicos (pág. 180).

Para obtener información acerca del montaje de dispositivos MD al realizar la recuperación en Linux, vaya a Montaje de dispositivos MD para recuperación (Linux) (pág. 149).

2.8.3 Guardar la información de la estructura de volumen

Para que la estructura de dispositivos MD y de volúmenes lógicos se cree de forma automática en el momento de la recuperación, necesita guardar la información de la estructura de volumen de cualquiera de las siguientes formas:

- Al crear un plan de copia de seguridad para la copia de seguridad del nivel de disco, vaya a **Opciones de copia de seguridad > Configuraciones avanzadas** y seleccione la casilla de verificación **Guardar RAID software y metadatos de la LVM junto con las copias de seguridad**. (Se selecciona de forma predeterminada.)
- Antes de realizar la primera copia de seguridad del disco en una máquina de origen, ejecute el siguiente comando:

```
trueimagecmd --dumpraidinfo
```

Cualquiera de esas operaciones guarda la estructura de volumen lógico del equipo en el directorio /etc/Acronis. Asegúrese de seleccionar el volumen con este directorio para la copia de seguridad.

2.8.4 Selección de volúmenes lógicos y dispositivos MD en línea de comando

Supongamos que el sistema tiene cuatro discos físicos: Disco 1, disco 2, disco 3 y disco 4.

- Se configura un volumen RAID-1 en dos volúmenes básicos: sdb1, sdd1
- Se configura un volumen lógico en dos volúmenes básicos: sdb2, sdd2
- El disco 1 incluye Acronis Secure Zone, al cual normalmente no se le hace copia de seguridad.

Se puede obtener una lista de volúmenes con los siguientes comandos:

```
trueimagecmd --list

Num  Partition            Flags       Start      Size       Type
---- ------------------- ----------- ---------- ---------- -----------
Disk 1 (sda):
1-1  sda1                 Pri,Act     63         208813     Ext2
1-2  sda2                 Pri         417690     12289725   ReiserFS
1-3  sda3                 Pri         24997140   1052257    Linux Swap
     Unallocated                      27101655   2698920    Unallocated
1-4  Acronis Secure Zone  Pri         32499495   522112     FAT32
     Unallocated                      33543720   5356       Unallocated
Disk 2 (sdb):
2-1  sdb1                 Pri         62         124969     Ext2
2-2  sdb2                 Pri         250001     125000     None
     Unallocated                      500001     8138607    Unallocated
Disk 3 (sdc):
     Table                            0                     Table
     Unallocated                      1          1048575    Unallocated
Disk 4 (sdd):
4-1  sdd1                 Pri         62         124969     Ext2
4-2  sdd2                 Pri         250001     125000     None
     Unallocated                      500001     798575     Unallocated
Dynamic & GPT Volumes:
DYN1  VolGroup00-LogVol00                        245760     Ext3
                          Disk: 3     250385     245760
                          Disk: 5     250385     245760
DYN2  md0                                        124864     Ext2
                          Disk: 5     62         249728
                          Disk: 3     62         249728
```

El volumen lógico, DYN1, ocupa volúmenes básicos 2-2 y 4-2. El volumen RAID-1, DYN2, ocupa un volumen básico 2-1 y 4-1.

Para realizar la copia de seguridad del volumen DYN1, ejecute el siguiente comando (aquí, el nombre de la copia de seguridad se presupone que es /home/backup.tib):

```
trueimagecmd --partition:dyn1 --filename:/home/backup.tib --create
```

Para realizar la copia de seguridad del volumen RAID-1, DYN2, ejecute el siguiente comando:

```
trueimagecmd --partition:dyn2 --filename:/home/backup.tib --create
```

Para realizar copias de seguridad de los tres volúmenes de discos duros, seleccione los volúmenes 1-1, 1-2, 1-3, DYN1 y DYN2:

```
trueimagecmd   --partition:1-1,1-2,1-3,dyn1,dyn2   --filename:/home/backup.tib   --
create
```

Si selecciona Disco 3, volumen 2-1 o volumen 2-2, el programa creará una copia de seguridad sin procesar (sector por sector).

2.9 Copia de seguridad de conjuntos de RAID de hardware (Linux)

Los conjuntos de RAID de hardware en Linux combinan diversas unidades físicas para crear un solo disco que puede particionarse. El archivo especial relacionado con un conjunto de RAID de hardware

se ubica, por lo general, en /dev/ataraid. Puede realizar copias de seguridad de conjuntos de RAID de hardware de la misma manera que los disco duros comunes.

Los disco físicos que son parte del conjunto de RAID de hardware se pueden enumerar junto a otros discos si tienen una tabla de partición dañada o ninguna tabla de partición en absoluto. La copia de seguridad de dichos discos no tiene mucho sentido porque no será posible recuperarlos.

2.10 Soporte de cintas

Acronis Backup & Recovery 10 es compatible con bibliotecas de cintas, cargadores automáticos, SCSI y unidades de cinta USB como dispositivos de almacenamiento. Un dispositivo de cinta se puede conectar a nivel local a un equipo administrado (en este caso, el agente Acronis Backup & Recovery 10 escribe y lee las cintas) o se puede acceder desde el nodo de almacenamiento de Acronis Backup & Recovery 10. Los nodos de almacenamiento aseguran el funcionamiento completamente automático de Bibliotecas de cintas y cargadores automáticos.

Los archivos de copia de seguridad creados con varias maneras de acceder a la cinta tienen diferentes formatos. Un agente no puede leer una cinta escrita con un nodo de almacenamiento.

Los medios basados en Linux y PE permiten la copia de seguridad y recuperación con acceso local y acceso por el nodo de almacenamiento. Se puede recuperar las copias de seguridad creadas con dispositivos de arranque con el agente de Acronis Backup & Recovery 10 que se ejecuta en el sistema operativo.

2.10.1 Tabla de compatibilidad de cintas

La siguiente tabla resume la legibilidad de las cintas escritas por Acronis True Image Echo y la familia de productos Acronis True Image 9.1 en Acronis Copia de seguridad de & Recovery 10. La tabla también ilustra la compatibilidad de las cintas escritas de varios componentes de Acronis Copia de seguridad de & Recovery 10.

			...es legible en un dispositivo de cinta conectado en un equipo con...			
			Medio de inicio de ABR10	Agente de Windows ABR10	Agente de Linux ABR10	Nodo de almacenamiento ABR10
Cinta escrita en un dispositivo de cinta conectado a nivel local (unidad de cinta o biblioteca de cintas) por...	Medio de inicio	ATIE 9.1	+	+	+	+
		ATIE 9.5	+	+	+	+
		ATIE 9.7	+	+	+	+
		ABR10	+	+	+	+
	Agente para Windows	ATIE 9.1	+	+	+	+
		ATIE 9.5	-	-	-	+
		ATIE 9.7	-	-	-	+
		ABR10	+	+	+	+
	Agente para Linux	ATIE 9.1	+	+	+	+

		ATIE 9.5	+	+	+	+
		ATIE 9.7	+	+	+	+
		ABR10	+	+	+	+
Cinta escrita en un dispositivo de cinta por...	Servidor de copia de seguridad	ATIE 9.1	+	+	+	+
		ATIE 9.5	-	-	-	+
		ATIE 9.7	-	-	-	+
	Nodo de almacenamiento	ABR10	-	-	-	+

2.10.2 Uso de una sola unidad de cinta

Una unidad de cinta que está conectada a nivel local a un equipo administrado y se puede usar con los planes de copias de seguridad locales, como dispositivo de almacenamiento. La funcionalidad de un cargador automático conectado a nivel local o la biblioteca de cintas está limitada a la unidad de cinta. Esto significa que el programa sólo puede funcionar con la cinta que se encuentra montada y debe montar las cintas manualmente.

Creación de una copia de seguridad en un dispositivo de cinta conectado a nivel local

Cuando se crea un plan de copia de seguridad, puede seleccionar el dispositivo de cinta conectado a nivel local como el destino para la copia de seguridad. No se necesita el nombre del archivo cuando se crea una copia de seguridad en una cinta.

Un archivo puede abarcar múltiples cintas pero puede contener sólo una copia de seguridad completa y un número ilimitado de copias de seguridad incremental. Cada vez que se cree una copia de seguridad completa, comience con una nueva cinta y cree un nuevo archivo. Una vez que la cinta esté llena, aparecerá una ventana de diálogo donde se solicita la colocación de una nueva cinta.

El contenido de cintas que no están en blanco, se sobrescribirán cuando se lo pida. Tiene la opción de desactivar los comandos, consulte Configuraciones adicionales (pág. 66).

Solución alternativa

En caso de que desee conservar más de un archivo comprimido en la cinta, por ejemplo, si desea realizar copias de seguridad del volumen C y el D por separado, seleccione el modo de copia de seguridad incremental en lugar de copia de seguridad completa cuando cree la primera copia de seguridad para el segundo disco. En otras situaciones, la copia de seguridad incremental se utiliza para añadir cambios al archivo creado anteriormente.

Es posible que experimente pausas breves que son necesarias para rebobinar la cinta. Una cinta de baja calidad o vieja así como un cabezal magnético sucio pueden provocar pausas que pueden durar hasta varios minutos.

Limitaciones

1. Copias de seguridad completas dentro de un archivo no son compatibles.
2. Los archivos individuales no se pueden recuperar desde la copia de seguridad del disco.
3. Las copias de seguridad no se pueden eliminar de una cinta manualmente o automáticamente durante la limpieza. Las reglas de retención y los esquemas de copia de seguridad que usan

limpieza automática (GPS, Torres de Hanói) están deshabilitados en la interfaz GUI cuando se realice una copia de seguridad a una cinta conectada a nivel local.

4. La bóveda personal no se puede crear en los dispositivos de cinta.
5. Debido a que la presencia de un sistema operativo no se puede detectar en la copia de seguridad en una cinta, se propone a Acronis Universal Restore (pág. 198) en la recuperación de cada disco o volumen, incluso cuando se recupera en un volumen de Linux o sin sistema de Windows.
6. Acronis Active Restore (pág. 185) no está disponible cuando se recupera desde una cinta.

Creación de una recuperación en un dispositivo de cinta conectado a nivel local

Antes de crear una tarea de recuperación, inserte o monte la cinta con la copia de seguridad que necesita recuperar. Cuando cree una tarea de recuperación, seleccione el dispositivo de cinta de la lista de ubicaciones disponibles y después seleccione la copia de seguridad. Después de comenzar una recuperación, se le pedirá otras cintas si se necesita otras cintas para la recuperación.

2.11 Compatibilidad con SNMP

Objetos SNMP

Acronis Backup & Recovery 10 proporciona los siguientes objetos del Protocolo simple de administración de red (SNMP) para las aplicaciones de gestión SNMP:

- Tipo de evento

  Identificador de objeto (OID): 1.3.6.1.4.1.24769.100.200.1.0

  Sintaxis: OctetString

  El valor puede ser "Información", "Advertencia", 'Error" y "Desconocido". "Desconocido" se envía únicamente en el mensaje de prueba.
- Descripción del texto del evento

  Identificador de objeto (OID): 1.3.6.1.4.1.24769.100.200.2.0

  Sintaxis: OctetString

  El valor contiene la descripción del texto del evento (tiene el mismo aspecto que los mensaje publicados por Acronis Backup & Recovery 10 en su registro).

Ejemplo de valores varbind:

1.3.6.1.4.1.24769.100.200.1.0:Information

1.3.6.1.4.1.24769.100.200.2.0:I0064000B

Operaciones compatibles

Acronis Backup & Recovery 10 **es compatible únicamente con operaciones TRAP**. no es posible gestionar Acronis Backup & Recovery 10 usando solicitudes GET- y SET. Esto significa que necesita utilizar un receptor SNMP Trap para recibir mensajes TRAP.

Acerca de la base de información de gestión (MIB)

El archivo MIB **acronis-abr.mib** se encuentra ubicado en el directorio de instalación Acronis Backup & Recovery 10. De forma predeterminada: %ProgramFiles%\Acronis\BackupAndRecovery en Windows y /usr/lib/Acronis/BackupAndRecovery en Linux.

Este archivo puede ser leído por un explorador MIB o por un simple editor de texto como el Notepad.

Acerca del mensaje de prueba

Cuando configure notificaciones SNMP, puede enviar un mensaje de prueba para comprobar si sus configuraciones son correctas.

Los parámetros del mensaje de prueba son como se describe a continuación:

- Tipo de evento

  OID: 1.3.6.1.4.1.24769.100.200.1.0

  Valor: "Desconocido"
- Descripción del texto del evento

  OID: 1.3.6.1.4.1.24769.100.200.2.0

  Valor: "?00000000"

2.12 Tecnologías propias de Acronis

En esta sección se describen las tecnologías propias heredadas de los productos de la familia de Acronis Backup & Recovery 10 de Acronis True Image Echo y Acronis True Image 9.1.

2.12.1 Acronis Secure Zone

Acronis Secure Zone es una partición segura que permite mantener archivos comprimidos de copia de seguridad en el espacio de disco de un equipo gestionado y, por lo tanto, recuperar un disco del mismo disco en el que reside la copia de seguridad.

Algunas aplicaciones de Windows, como las herramientas de gestión de disco de Acronis, pueden acceder a la zona.

Si el disco tuviera una falla física, se perderían la zona y los archivos ubicados allí. Esa es la razón por la que Acronis Secure Zone no debe ser la única ubicación donde se almacene una copia de seguridad. En entornos empresariales, se puede pensar en Acronis 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.

Ventajas

Acronis Secure Zone

- Permite la recuperación de un disco en el mismo disco en donde reside la copia de seguridad del disco.
- Ofrece un método rentable y útil para la protección de datos por funcionamiento defectuoso del software, ataque de virus, error del operador.
- Como es un almacenamiento interno de archivos, elimina la necesidad de separar los medio o conexión de red para realizar la copia de seguridad o recuperar los datos. Esto es muy útil para los usuarios móviles.
- Puede funcionar como destino primario cuando se use copia de seguridad de doble destino (pág. 64).

Limitaciones

- La zona no se puede organizar en un disco dinámico o un disco que use el estilo de partición GPT.

Administración de Acronis Secure Zone

Acronis Secure Zone se considera una bóveda (pág. 186) personal. Una vez que se crea en un equipo gestionado, la zona está presente siempre en la lista de **Bóvedas personales**. Los planes de copias de seguridad centralizados (pág. 196) pueden utilizar tanto Acronis Secure Zone como planes locales (pág. 197).

Si ha utilizado Acronis Secure Zone anteriormente, tenga en cuenta que se ha producido un cambio radical en su funcionamiento. La zona ya no realiza limpiezas automáticas, es decir, ya no elimina archivos comprimidos antiguos. Use esquemas de copia de seguridad con limpieza automática para realizar copias de seguridad en la zona, o elimine las copias de seguridad desactualizadas manualmente con la funcionalidad de administración de archivos.

Con el nuevo comportamiento de Acronis Secure Zone, puede conseguir:

- la lista de archivos ubicados en la zona y la copia de seguridad en cada archivo
- examen del contenido de la copia de seguridad
- el montaje de la copia de seguridad del disco para copiar los archivos de la copia de seguridad a un disco físico
- eliminar de manera segura los archivos comprimidos y las copias de seguridad de los archivos comprimidos.

Para obtener más información sobre funciones disponibles en Acronis Secure Zone, consulte la sección Bóvedas personales (pág. 78).

Actualización desde Acronis True Image Echo

Cuando se actualiza desde Acronis True Image Echo a Acronis Backup & Recovery 10, Acronis Secure Zone mantendrá los archivos comprimidos creados con Echo. La zona aparecerá en la lista de bóveda personal y los archivos antiguos estarán disponibles para recuperación.

2.12.2 Acronis Startup Recovery Manager

Se puede modificar el agente de inicio (pág. 186) del disco del sistema y se puede configurar para arrancar en el momento de inicio, cuando se pulse F11. Esto elimina la necesidad de los medios de recuperación o conexión de red para iniciar la utilidad de rescate de inicio. La característica tiene el nombre comercial "Acronis Startup Recovery Manager".

Acronis Startup Recovery Manager es muy útil para los usuarios móviles. En caso de fallo, el usuario reinicia el equipo, pulsa F11 cuando aparezca el aviso "Press F11 for Acronis Startup Recovery Manager..." y realiza recuperación de datos en la misma manera que con un medio de inicio común. El usuario también puede realizar copias de seguridad con Acronis Startup Recovery Manager, mientras está en movimiento.

En equipos con el cargador de inicio GRUB instalado, el usuario selecciona Acronis Startup Recovery Manager del menú de inicio en lugar de pulsar F11.

La activación y desactivación de Acronis Startup Recovery Manager

La operación que permite el uso de Acronis Startup Recovery Manager se denomina "activación". Para activar Acronis Startup Recovery Manager, seleccione **Acciones > Activar Acronis Startup Recovery Manager** en el menú del programa.

Puede activar o desactivar Acronis Startup Recovery Manager en cualquier momento desde el menú **Herramientas**. La desactivación deshabilitará el mensaje de tiempo de inicio "Pulse F11 para Acronis

Startup Recovery Manager…" (o elimina la entrada correspondiente del menú de inicio GRUB correspondiente). Esto significa que necesitará dispositivos de arranque en caso que se deba iniciar el sistema.

Limitación

Después de activar Acronis Startup Recovery Manager es necesario reactivar cargadores de terceros.

Actualización de Acronis True Image Echo

Después de la actualización de Acronis True Image Echo a Acronis Backup & Recovery 10, Acronis Startup Recovery Manager aparece como desactivado independientemente de su estado antes de la actualización. Puede activar Acronis Startup Recovery Manager nuevamente en cualquier momento.

3 Opciones

Esta sección cubre las opciones de Acronis Backup & Recovery 10 que se puede configurar utilizando la interfaz gráfica de usuario (GUI). El contenido de esta sección es aplicable a las ediciones avanzadas y autónomas de Acronis Backup & Recovery 10.

3.1 Opciones de Consola

Las opciones de consola definen la manera en la que se representa la información en la Interfaz Gráfica de Usuario de Acronis Backup & Recovery 10.

Para acceder a las opciones de la Consola, seleccione **Opciones> Consola** desde el menú superior.

3.1.1 Página de inicio

Esta opción define si se desea mostrar la ventana de **Bienvenida** o el **Tablero** después de que la consola se conecte al equipo gestionado o Management server.

El valor predeterminado: La ventana de **Bienvenida**.

Para realizar una selección, marque o desmarque la casilla de verificación para **mostrar el Tablero después de que la consola se conecte al equipo**.

Esta opción también se puede establecer en la ventana de **Bienvenida**. Si selecciona la casilla de verificación **Al inicio, se verá el Tablero en vez de la vista actual** en la ventana de **Bienvenida,** dicha configuración se actualizará según corresponda.

3.1.2 Mensajes emergentes

Sobre las tareas que necesitan interacción

Esta opción es eficaz cuando la consola está conectada a un equipo gestionado o Management server.

La opción define si se debe mostrar la ventana emergente cuando hay una o más tareas que requieran de la interacción del usuario. Esta ventana le permite especificar su decisión para confirmar el reinicio o para volver a intentarlo después de liberar espacio de disco, o en todas las tareas en el mismo lugar. Hasta que una tarea necesite de interacción, puede abrir esta ventana en cualquier momento desde el **Tablero** del equipo gestionado. También podría revisar los estados de ejecución de tareas en la vista de**Tareas** y especificar su decisión sobre cada tarea en el panel de **Información**.

El valor predeterminado: **Habilitado.**

Para realizar una selección, seleccione o anule su selección en la casilla de verificación en la **ventana emergente "Tareas que necesitan Interacción"**.

Sobre los resultados de la ejecución de tareas

La opción sólo es eficaz cuando la consola está conectada a un equipo gestionado.

La opción define si se muestran los mensajes emergentes sobre los resultados de la ejecución de tareas: finalización exitosa, falla o éxito con advertencias. Cuando se deshabilita la visualización de mensajes emergentes, puede revisar los estados de ejecución de tareas y los resultados en la vista de **Tareas**.

El valor predeterminado: **Habilitado** para todos los resultados.

Para una realizar una configuración por cada resultado individualmente (finalización exitosa, falla o éxito con advertencias) selecciones o anule su selección en la casilla de verificación respectiva.

3.1.3 Alertas según el momento

Última copia de seguridad

Esta opción es eficaz cuando la consola está conectada a un equipo gestionado (pág. 190) o Management server (pág. 194).

La opción define si se informa en caso de que no se realice la copia de seguridad en algún equipo durante cierto tiempo. Puede ingresar el período de tiempo que cree es importante para su empresa.

El valor predeterminado: Informa si se completó la última copia de seguridad en un equipo con hasta **5 días** de anterioridad.

Se muestra la alerta en la sección **Alertas** del **Tablero**. Cuando la consola se conecta al Management server, la configuración también controlará el esquema de colores de los valores de la columna de la **Última Copia de seguridad** para cada equipo. .

Última conexión

Esta opción es eficaz cuando la consola se conecta al Management server o al equipo registrado (pág. 190).

Esta opción define si se informa si no se establece la conexión entre el equipo registrado y el Management server durante un período de tiempo, y así indica que es posible que el equipo no pueda ser gestionado centralmente (por ejemplo: en el caso de fallas de la conexión de red para ese equipo). Puede establecer el período de tiempo que crea importante.

El valor predeterminado: Informa si la última conexión del equipo al Management server se realizó con más de **5 días** de anterioridad.

Se muestra la alerta en la sección **Alertas** del **Tablero**. Cuando la consola se conecta al Management server, la configuración también controlará el esquema de colores de los valores de la columna de la **Última conexión** para cada equipo. .

3.1.4 Cantidad de tareas

La opción sólo es eficaz cuando la consola está conectada al Management server.

La opción define la cantidad de tareas que se mostrará a la vez en la vista de **Tareas**. También puede usar los filtros disponibles en la vista de **Tareas** para limitar el número de tareas mostradas.

El valor predeterminado: **400**. Los valores de ajuste son: **20 a 500**.

Para realizar una selección, elija el valor deseado desde el **Número de tareas** en el menú desplegable.

3.1.5 Fuentes

Esta opción es eficaz cuando la consola está conectada a un equipo gestionado o Management server.

La opción define las fuentes que se usarán en la Interfaz Gráfica de Usuario de Acronis Backup & Recovery 10. Las configuraciones de **Menú** afectan a los menús desplegables y contextuales. La configuración de **Aplicación** afecta a los otros elementos de la GUI.

El valor predeterminado: La **fuente por defecto** del sistema para los menús y los elementos de la interfaz de la aplicación.

Para realizar una selección, elija la fuente en el cuadro combinado respectivo y establezca las propiedades de la fuente. Puede obtener una vista previa de la fuente al hacer clic en el botón de la derecha.

3.2 Opciones del equipo

Las opciones del equipo definen el comportamiento general de las agentes de Acronis Backup & Recovery 10 que funcionan en el equipo gestionado, y así se consideran que las opciones son específicas del equipo.

Para acceder a las opciones del equipo, conéctese al equipo gestionado y selecciones **Opciones > Opciones del equipo** desde el menú superior.

3.2.1 Seguimiento de sucesos

Es posible el envío de los sucesos registrados por el agente, que funcionan en un equipo gestionado, para los gestores SNMP especificados. Si no modifica las opciones de seguimiento de sucesos en todos lados menos aquí, su configuración será efectiva para cada plan de copia de seguridad local y cada tarea creada en el equipo.

Puede anular las configuraciones aquí, únicamente para los sucesos que ocurran durante la copia de seguridad o recuperación (Consulte las opciones de copia de seguridad predeterminada y recuperación (pág. 48)) En este caso, las configuraciones serán eficaces para las funciones que no estén relacionadas con la copia de seguridad y la recuperación, como limpieza y validación de archivos comprimidos.

Además podrá anular las configuraciones establecidas en las opciones de copia de seguridad predeterminada y recuperación, cuando se cree un plan de copia de seguridad o tarea de recuperación. Las tareas que obtenga es este caso serán específicas del plan o de la tarea.

Notificaciones SNMP

Esta opción es eficaz tanto para los sistemas operativos de Windows como de Linux.

Esta opción no está disponible cuando se trabaja desde dispositivos de inicio.

Esta opción define si el agente operativo en el equipo gestionado debe enviar los sucesos de registro a los gestores de Simple Network Management Protocol (SNMP). Puede elegir los tipos de sucesos a enviar.

Puede anular las configuraciones aquí, únicamente para los sucesos que ocurran durante la copia de seguridad o recuperación, en las opciones de recuperación y copia de seguridad predeterminada

(pág. 48). En este caso, las configuraciones serán eficaces para las funciones que no estén relacionadas con la copia de seguridad y la recuperación, como limpieza y validación de archivos comprimidos.

Además podrá anular las configuraciones establecidas en las opciones de copia de seguridad predeterminada y recuperación, cuando se cree un plan de copia de seguridad o tarea de recuperación. Las tareas que obtenga es este caso serán específicas del plan o de la tarea.

Para obtener información detallada acerca de cómo utilizar SNMP con Acronis Backup & Recovery 10, vaya a "Asistencia para SNMP (pág. 40)".

El valor predeterminado: **Deshabilitado**.

Configurar el envío de mensajes SNMP

1. Active la casilla de verificación **Enviar mensajes al servidor**.
2. Especifique las opciones apropiadas como se detalla a continuación:
   - **Tipos de eventos para enviar**: elija los tipos de eventos: **Todos los eventos**, **Errores y advertencias**, o **Sólo errores**.
   - **Nombre del servidor/IP:** introduzca el nombre o dirección IP del servidor en el que se ejecuta la aplicación de gestión SNMP y al que se enviarán los mensajes.
   - **Comunidad**: tipo de nombre de la comunidad SNMP a la que pertenecen tanto el servidor que ejecuta la aplicación de gestión SNMP como el equipo emisor. La comunidad típica es "pública".

   Haga clic en **Enviar mensaje de prueba** para verificar si la configuración es correcta.

Para deshabilitar el envío de mensajes SNMP, desactive la casilla de verificación **Enviar mensajes al servidor SNMP**.

Los mensajes se envían a través de UDP.

La siguiente sección tiene información adicional sobre la configuración de los servicios SNMP en el equipo receptor (pág. 47).

La configuración de los servicios SNMP en el equipo receptor.

Windows

Para instalar los servicio SNMP en una máquina en la que se ejecuta Windows:

1. **Inicio > Panel de control > Agregar o quitar programas > Agregar o quitar componentes de Windows.**
2. Seleccione las **Herramientas de Gestión y Supervisión**.
3. Haga clic en **Detalles.**
4. Seleccione la casilla de verificación **Protocolo Simple Network Management**.
5. Haga clic en **Aceptar**.

Es posible que se le pida lmmib2.dll, que se encuentra en el disco de instalación de su sistema operativo.

Linux

Para recibir mensajes SNMP en un equipo en el que se ejecuta Linux, se deberán instalar los paquetes net-snmp (para RHEL y SUSE) o snmpd (para Debian).

A SNMP se lo puede configurar con el comando **snmpconf**. El archivo de configuración predeterminado está ubicado en el directorio: /etc/snmp:

- /etc/snmp/snmpd.conf - archivo de configuración para el agente Net-SNMP SNMP.
- /etc/snmp/snmptrapd.conf - archivo de configuración para el daemon Net-SNMP.

3.2.2 Reglas de limpieza de los registros

Esta opción especifica cómo limpiar el registro del agenteAcronis Backup & Recovery 10.

Esta opción define el tamaño máximo de la carpeta de registro del agente (en un servidor Windows XP/2003, %ALLUSERSPROFILE%\Application Data\Acronis\BackupAndRecovery\MMS\LogEvents).

El valor predeterminado: **Tamaño de registro máximo: 1 GB**. **Durante la limpieza, mantenga el 95% del tamaño de registro máximo**.

Cuando la opción está habilitada, el programa compara el tamaño de registro actual con el tamaño máximo cada 100 entradas del registro. Una vez que se excede el tamaño de registro máximo, el programa elimina las entradas de registro más antiguas. Puede seleccionar las entradas del registro a retener. La configuración predeterminada de 95% conservará la mayoría del registro. Con la configuración mínima de 1%, el registro se borrará casi por completo.

Este parámetro también puede establecerse utilizando Acronis Administrative Template.

3.3 Opciones predeterminadas de copia de seguridad y recuperación

3.3.1 Opciones de copia de seguridad predeterminadas

Cada agente de Acronis tiene sus propias opciones predeterminadas de copia de seguridad. Una vez instalado el agente, las opciones predeterminadas tienen valores predefinidos, que se consideran **preajustes** en la documentación. Cuando crea un plan de copia de seguridad, puede utilizar una opción predeterminada o anular la opción predeterminada mediante el valor personalizado que se especificará únicamente para este plan.

También puede personalizar una opción predeterminada al cambiar su valor a otro diferente al predefinido. El nuevo valor se utilizará de manera predeterminada para todos los planes de copias de seguridad que cree en su equipo en adelante.

Para ver o cambiar las opciones de copia de seguridad predeterminadas, conecte la consola al equipo gestionado y después seleccione **Opciones > Opciones predeterminadas de copia de seguridad y recuperación > Opciones predeterminadas de copia de seguridad** en el menú superior.

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 (Linux, dispositivo de arranque)
- El tipo de datos que se está copiando (disco, archivo)
- El destino de la copia de seguridad (ubicación en redes o disco local)
- El esquema de copia de seguridad (realizar copia de seguridad ahora o utilizando el programador)

La siguiente tabla resume la disponibilidad de las opciones de copia de seguridad.

	Agente de Linux		**Medio de inicio (basado en Linux)**	
	Copia de seguridad del disco	**Copia de seguridad del archivo**	**Copia de seguridad del disco**	**Copia de seguridad del archivo**
Protección del archivo comprimido (pág. 50) (contraseña + cifrado)	+	+	+	+
Exclusión de archivos de origen (pág. 51)	+	+	+	+
Comandos previos o posteriores a la copia de seguridad (pág. 52)	+	+	-	-
Comandos previos o posteriores a la captura de datos (pág. 54)	+	+	-	-
Instantánea de la copia de seguridad a nivel de archivo (pág. 56)	-	+	-	-
Nivel de compresión (pág. 57)	+	+	+	+
Rendimiento de la copia de seguridad:				
Prioridad de la copia de seguridad (pág. 58)	+	+	-	-
Velocidad de escritura del HDD (pág. 58)	Destino: HDD	Destino: HDD	Destino: HDD	Destino: HDD
Velocidad de la conexión de red (pág. 58)	Destino: red compartida	Destino: red compartida	Destino: red compartida	Destino: red compartida
Copias de seguridad incrementales/diferenciales rápidas (pág. 61)	+	-	+	-
División de copias de seguridad (pág. 62)	+	+	+	+
Componentes de medios	Destino: medio extraíble	Destino: medio extraíble	-	-
Manejo de errores (pág. 63):				
No mostrar mensajes ni diálogos durante el procesamiento (modo silencioso)	+	+	+	+
Reintentar si se produce un error	+	+	+	+
Ignorar los sectores defectuosos	+	+	+	+
Doble destino (pág. 64)	Destino: local	Destino: local	-	-
Condiciones de inicio de la tarea (pág. 64)	+	+	-	-
Manejo de fallos de la tarea (pág. 65)	+	+	-	-
Ajustes adicionales (pág. 66):				

Sobrescribir los datos en una cinta sin solicitar la confirmación del usuario	Destino: Cinta	Destino: Cinta	Destino: Cinta	Destino: Cinta
Desmontar dispositivos después de que la copia de seguridad haya finalizado	Destino: medio extraíble	Destino: medio extraíble	Destino: medio extraíble	Destino: medio extraíble
Solicitar el primer medio al realizar la copia de seguridad en un medio extraíble.	Destino: medio extraíble	Destino: medio extraíble	Destino: medio extraíble	Destino: medio extraíble
Reiniciar el equipo automáticamente después de que finalice la copia de seguridad	-	-	+	+
Guarde el RAID por software y los metadatos de la LVM junto con las copias de seguridad	+	-	-	-
Notificaciones:				
Correo electrónico (pág. 59)	+	+	-	-
Win Pop-up (pág. 60)	+	+	-	-
Rastreo de eventos:				
SNMP (pág. 61)	+	+	-	-

Protección del archivo comprimido

Esta opción es eficaz tanto para los sistemas operativos de Windows como de Linux y los medios de inicio..

Esta opción es eficaz tanto para la copia de seguridad a nivel de disco como a nivel de archivo.

El valor predeterminado: **Deshabilitado.**

Para proteger el archivo comprimido de accesos no autorizados

1. Seleccione la casilla de verificación **Establecer la contraseña para el archivo comprimido**.
2. En el campo **Introducir contraseña,** escriba la contraseña.
3. En el campo **Confirmar contraseña**, vuelva a escribir la contraseña.
4. Seleccione una de las siguientes opciones:
   - **No cifrar**: el archivo comprimido estará protegido sólo con la contraseña
   - **AES 128:** se cifrará el archivo comprimido por medio del algoritmo estándar avanzado de cifrado (AES) con una clave de 128 bits
   - **AES 192:** se cifrará el archivo comprimido por medio del algoritmo AES con una clave de 192-bits
   - **AES 256:** se cifrará el archivo comprimido por medio del algoritmo AES con una clave de 256-bits
5. Haga clic en **Aceptar**.

El algoritmo de cifrado AES funciona en el modo Cipher-block chaining (CBC) y utiliza una clave generada de manera aleatoria con un tamaño definido por el usuario de 128, 192 ó 256 bits. Cuanto más grande sea el tamaño de clave, más tiempo se tardará en cifrar el archivo comprimido y más seguros estarán los datos.

Luego, la clave de cifrado se cifra con AES-256 usando un hash SHA-256 de la contraseña como clave. La contraseña no se guarda en ninguna parte del disco o del archivo de copia de seguridad; el hash de la contraseña se usa como para verificación. Con esta seguridad con dos niveles, los datos de copia de seguridad están protegidos contra el acceso no autorizado.

Exclusión de archivos de origen

Esta opción es eficaz tanto para los sistemas operativos de Windows como de Linux y los medios de inicio..

Esta opción es eficaz solo para copias de seguridad a nivel de disco de sistemas de archivos NTFS y FAT. Esta opción es eficaz para copias de seguridad a nivel de archivos de todos los sistemas de archivos compatibles.

La opción define qué archivos y carpetas omitir durante el proceso de copia de seguridad y que, por lo tanto, quedan excluidos de la lista de datos que se incluirán en la copia de seguridad.

El valor predeterminado es: **Excluir los archivos que coincidan con los siguientes criterios *.tmp, *.~, *.bak.**

Para especificar los archivos y carpetas que desea excluir:

Configure alguno de los siguientes parámetros:

- **Excluir todos los archivos y carpetas ocultos**

  Esta opción está vigente sólo para sistemas de archivos compatibles con Windows. Seleccione esta casilla de verificación para omitir archivos y carpetas con el atributo **Oculto**. Si una carpeta está **Oculta**, se excluirán todos sus contenidos, incluso los archivos que no se encuentran **Ocultos**.
- **Excluir todos los archivos y carpetas del sistema**

  Esta opción está vigente sólo 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**.

*Puede ver los atributos del archivo o de la carpeta en las propiedades del archivo/carpeta o mediante el comando **atrib**. Para obtener más información, consulte el Centro de Servicio Técnico y Ayuda de Windows.*

- **Excluir los archivos que coincidan con los siguientes criterios**

  Seleccione esta casilla de verificación para omitir los archivos y las carpetas cuyos nombres en la lista coincidan con alguno de los criterios, llamados máscaras del archivo; utilice los botones **Agregar**, **Editar**, **Eliminar** y **Eliminar todos** para crear la lista de máscaras del archivo.

  Puede utilizar uno o más caracteres comodín * y ? en una máscara de archivo:

  El asterisco (*) sustituye de cero a más caracteres del nombre del archivo; por ejemplo, la máscara de archivo Doc*.txt genera archivos Doc.txt y Document.txt

  El signo de interrogación (?) substituye a un único carácter; por ejemplo, la máscara de archivo Doc?.txt genera archivos Doc1.txt y Docs.txt, pero, por el contrario, no general archivos Doc.txt o Doc11.txt

Para excluir una carpeta especificada por una ruta que contiene la letra de unidad, agregue una barra invertida (\) al nombre de carpeta en el criterio; por ejemplo: C:\Finance\

Ejemplos de exclusión

Criterio	Ejemplo	Descripción
Windows y Linux		
Por nombre	F.log F	Excluye todos los archivos denominados "F.log" Excluye todas las carpetas denominadas "F"
Por máscara (*)	*.log F*	Excluye todos los archivos con la extensión .log Excluye todos los archivos y carpetas cuyos nombres comiencen con "F" (como carpetas F, F1 y archivos F.log, F1.log)
Por máscara (?)	F???.log	Excluye todos los archivos .log cuyos nombres contengan cuatro símbolos y comiencen con "F"
Windows		
Por ruta de archivo	C:\Finance\F.log	Excluye el archivo denominado "F.log" ubicado en la carpeta C:\Finance
Por ruta de carpeta	C:\Finance\F\	Excluye la carpeta C:\Finance\F (asegúrese de especificar la ruta completa, comenzando por la letra de unidad)
Linux		
Por ruta de archivo	/home/user/Finance/F.log	Excluye el archivo denominado "F.log", ubicado en la carpeta /home/user/Finance
Por ruta de carpeta	/home/user/Finance/	Excluye la carpeta /home/user/Finance

Los ajustes anteriores no afectan a los archivos o carpetas seleccionados expresamente para la copia de seguridad. Por ejemplo, supongamos que seleccionó la carpeta MiCarpeta y el archivo MiArchivo.tmp fuera de esa carpeta, y seleccionó la opción de omitir todos los archivos .tmp. En este caso, todos los archivos .tmp de la carpeta MiCarpeta serán omitidos durante el proceso de copia de seguridad, pero no se omitirá el archivo MiArchivo.tmp.

Comandos pre / post

Esta opción es eficaz tanto para los sistemas operativos de Windows como de Linux y los medios de inicio basados en PE..

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 pre-Copia de seguridad	Copia de seguridad	Comando de post-copia de seguridad

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

- eliminación de archivos temporales antes de comenzar la copia de seguridad
- configuración de un producto antivirus de terceros antes de comenzar la copia de seguridad
- copia de un archivo comprimido a otra ubicación después de que termine la copia de seguridad.

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

Para especificar comandos pre/post

1. Puede habilitar la ejecución de comandos pre/post al marcar las siguientes opciones:
   - **Ejecutar antes de la copia de seguridad**
   - **Ejecutar después de la copia de seguridad**
2. Realice uno de los siguientes:
   - Haga clic en **Editar** para especificar un nuevo comando o un archivo por lotes
   - Seleccione el comando existente o el archivo por lotes de la lista desplegable
3. Haga clic en **Aceptar**.

Comando de pre-copia 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. En el campo **Comando**, introduzca un comando o examine hasta encontrar un archivo por lotes. El programa no admite comandos interactivos, es decir, comandos que exijan la intervención del usuario (por ejemplo, “pause”).
2. En el campo **Directorio de trabajo**, especifique la ruta mediante la que se ejecutará el comando o archivo por lotes.
3. En el campo **Argumentos**, especifique los argumentos de ejecución del comando, si fuera necesario.
4. Dependiendo del resultado que desee obtener, seleccione la opción apropiada tal y como se describe en la siguiente tabla.
5. Haga clic en **Probar comando** para verificar si el comando es correcto.

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

Comando de post-copia de seguridad

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

1. En el campo **Comando**, ingrese un comando o examinar hasta encontrar un archivo por lotes.
2. En el campo **Directorio de trabajo**, especifique una ruta en donde se ejecutará el comando o archivo por lotes.
3. En el campo **Argumentos**, especifique los argumentos de ejecución del comando, si fuera necesario.
4. Si es crítico que la ejecución del comando sea satisfactoria para su estrategia de copia de seguridad, marque la casilla de verificación **para suspender la tarea si falla la ejecución del comando**. Si la ejecución del comando falla, el programa eliminará el archivo TIB y los archivos temporales resultantes, si fuera posible, y la tarea fallará.

   Cuando no se marca la casilla de verificación, los resultados de la ejecución de comando no afectarán el éxito o fallo cuando se ejecute la tarea. Se puede seguir los resultados de la ejecución de comandos al explorar el registro de errores y advertencias que se muestran en el **Tablero**.
5. Haga clic en **Probar comando** para verificar el archivo si el comando es correcto.

Comandos previos o posteriores a la captura de datos

Esta opción es eficaz tanto para los sistemas operativos de Windows como de Linux..

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 la realiza Acronis Backup & Recovery 10 al comienzo del procedimiento de copia de seguridad.

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

	<---------- Copia de seguridad ---------->			
Comando de precopia de seguridad	Comandos antes de la captura de datos	Captura de datos	Comandos Post de la captura de datos	Comando de Post-copia de seguridad

Si la opción Servicio de instantáneas de volumen está habilitada, la ejecución de los comandos y las acciones de Microsoft VSS se sucederán tal y como se indica a continuación:

Comandos "Antes de la captura de datos” -> Suspensión de VSS -> Captura de datos -> Reanudación de VSS -> Comandos "Después de la captura de datos".

El uso de comandos Pre/Post de la captura de datos, puede suspender y reanudar la base de datos o la aplicación que no sea compatible con VSS. A diferencia de los Comandos pre/post (pág. 52), los comandos antes/después de la captura de datos se ejecutarán antes y después del proceso de captura de datos. Esto demora segundos. El proceso completo de copia de seguridad puede demorar más tiempo, según la cantidad de datos que se incluirá en la copia de seguridad. Por lo tanto, el tiempo de inactividad de la base de datos o aplicación será mínimo.

Para especificar los comandos Pre/Post de la captura de datos

1. Puede habilitar la ejecución de comandos de captura de datos Pre/Post al marcar las siguientes opciones:
   - **Ejecutar antes de la captura de datos**
   - **Ejecutar después de la captura de datos**
2. Realice uno de los siguientes pasos:

- Haga clic en **Editar** para especificar un nuevo comando o un archivo por lotes
- Seleccione el comando existente o el archivo por lotes de la lista desplegable.

3. Haga clic en **Aceptar**.

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. En el campo **Comando**, introduzca un comando o examine hasta encontrar un archivo por lotes. El programa no admite comandos interactivos, es decir, comandos que exijan la intervención del usuario (por ejemplo, “pause”).
2. En el campo **Directorio de trabajo**, especifique la ruta mediante la que se ejecutará el comando o archivo por lotes.
3. En el campo **Argumentos**, especifique los argumentos de ejecución del comando, si fuera necesario.
4. Dependiendo del resultado que desee obtener, seleccione la opción apropiada tal y como se describe en la siguiente tabla.
5. Haga clic en **Probar comando** para verificar si el comando es correcto.

Casilla de verificación	**Selección**			
Hacer que la tarea de 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 tarea 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/A	Realizar la captura de datos al mismo tiempo que se ejecuta el comando, independientemente del resultado de la ejecución del comando.

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. En el campo **Comando**, introduzca un comando o examine hasta encontrar un archivo por lotes. El programa no admite comandos interactivos, es decir, comandos que exijan la intervención del usuario (por ejemplo, “pause”).
2. En el campo **Directorio de trabajo**, especifique la ruta mediante la que se ejecutará el comando o archivo por lotes.
3. En el campo **Argumentos**, especifique los argumentos de ejecución del comando, si fuera necesario.
4. Dependiendo del resultado que desee obtener, seleccione la opción apropiada tal y como se describe en la siguiente tabla.
5. Haga clic en **Probar comando** para verificar si el comando es correcto.

Casilla de verificación	**Selección**			
Hacer que la tarea falle si falla la ejecución del comando	Seleccionado	Borrado	Seleccionado	Borrado
No realizar la copia de seguridad hasta que finalice la ejecución de comandos	Seleccionado	Seleccionado	Borrado	Borrado
Resultado				
	Valor predeterminado Continúe la copia de seguridad solo después de que se ejecute el comando correctamente. Elimina el archivo tib y los archivos temporales y suspende la tarea si falla la ejecución del comando.	Continúe la copia de seguridad después de que se ejecute el comando a pesar del éxito o fallo de su ejecución.	N/A	Continuar la copia de seguridad al mismo tiempo que se ejecuta el comando, independientemente del resultado de la ejecución del comando.

Instantánea de la copia de seguridad a nivel de archivo

Esta opción es eficaz sólo para la copia de seguridad a nivel de archivo. En sistemas operativos de Windows y Linux.

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

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

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

Seleccione una de las siguientes opciones:

- **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. Para utilizar una instantánea, el plan de copia de seguridad se debe ejecutar con una cuenta que tenga los privilegios de Administrador o de Copia de seguridad. Si no se puede tomar una instantánea, la copia de seguridad fallará.
- **Crear instantáneas si es posible.**

  Realizar la copia de seguridad directamente si no es posible tomar una instantánea.
- **No crear una instantánea**

  Siempre realizar la copia de seguridad directamente. No son necesarios los privilegios de Administrador o de operador de copia de seguridad. 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.

Nivel de compresión

Esta opción es eficaz tanto para los sistemas operativos de Windows como de Linux y los medios de inicio.

Esta opción define el nivel de compresión que se aplicará a los datos que se incluyen en la copia de seguridad.

El valor predeterminado: **Normal.**

El nivel 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 del archivo comprimido si éste incluye archivos esencialmente comprimidos, como .jpg, .pdf o .mp3. Sin embargo, los formatos como .doc o .xls estarán bien comprimidos.

Para especificar el nivel de compresión de los datos.

Seleccione una de las siguientes:

- **Ninguno**: los datos se copiarán como se encuentra, sin ningún tipo de compresión. El tamaño de la copia de seguridad resultante será máximo.
- **Normal**: recomendado en la mayoría de los casos.
- **Alto:** El tamaño de la copia de seguridad resultante será menor al nivel típico **Normal**.
- **Máximo:** se comprimirá los datos tanto como sea posible. La duración de la copia de seguridad será máxima. Es posible que desee seleccionar compresión Máxima para los medios extraíbles y así reducir la cantidad de discos en blanco que necesite.

Rendimiento de la copia de seguridad.

Utilice este grupo de opciones para especificar la cantidad de recursos de la red y del sistema que desea asignar para el proceso de copia de seguridad.

Las opciones de rendimiento de la copia de seguridad pueden tener un efecto más o menos perceptible en la velocidad del proceso de copia de seguridad. Esto depende del configuración general del sistema y las características físicas de los dispositivos desde o hacia los que se realiza la copia de seguridad.

Prioridad de la copia de seguridad

Esta opción es eficaz tanto para los sistemas operativos de Windows como de Linux.

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

El valor predeterminado: **Bajo.**

Para especificar la prioridad del proceso de copia de seguridad

Seleccione una de las siguientes:

- **Bajo**: para minimizar el uso de recursos por parte del proceso de copia de seguridad lo que dejará más recursos para otros procesos que se ejecuten en el equipo.
- **Normal**: ejecución del proceso de copia de seguridad con la velocidad normal, lo que permite asignar recursos al mismo nivel de otros procesos
- **Alto:** maximizará la velocidad del proceso de copia de seguridad al tomar recursos de otros procesos.

Velocidad de escritura del HDD

Esta opción es eficaz tanto para los sistemas operativos de Windows como de Linux y los medios de inicio.

Esta opción se encuentra disponible cuando se realiza la copia de seguridad de un disco duro interno (fijo) del equipo al que se eligió como destino de la copia de seguridad.

La copia de seguridad en un disco duro (por ejemplo en Acronis Secure Zone) puede disminuir el rendimiento del sistema operativo y las aplicaciones por la gran cantidad de datos que se deben escribir en el disco. Puede limitar el uso del disco duro mediante el proceso de copia de seguridad al nivel deseado.

El valor predeterminado: **Máximo.**

Para establecer la velocidad de grabación del disco duro (HDD) para copia de seguridad

Realice uno de los siguientes:

- Haga Clic en **Velocidad de grabación indicada como un porcentaje de la velocidad máxima del disco duro de destino**, y luego arrastre el deslizador o seleccione un porcentaje en la caja
- Haga Clic en **Velocidad de grabación expresada en kilobytes por segundo**, y después ingrese la velocidad de grabación del disco en kilobytes por segundo

Velocidad de la conexión de red

Esta opción es eficaz tanto para los sistemas operativos de Windows como de Linux y los medios de inicio.

Esta opción se encuentra disponible cuando se selecciona una ubicación en la red (Redes compartidas, bóveda gestionada o un servidor FTP/SFTP) como el destino de la copia de seguridad.

Esta opción define el ancho de banda asignado a la conexión de red para la transferencia de los datos de la copia de seguridad.

Se establece la velocidad máxima de manera predeterminada, es decir que el software utiliza todo el ancho de banda que puede obtener cuando se transfieran los datos de la copia de seguridad. Utilice esta opción para reservar una parte del ancho de banda de la red para otras actividades de la red.

El valor predeterminado: **Máximo.**

Para establecer la velocidad de la conexión de red para la copia de seguridad.

Realice uno de los siguientes:

- Haga Clic en **Velocidad de transferencia indicada como un porcentaje de la velocidad máxima de la conexión de red**, y luego arrastre el deslizador o tipo de porcentaje en la caja
- Haga Clic en **Velocidad de transferencia expresada en kilobytes por segundo**, y después ingrese el límite de ancho de banda para la transferencia de datos de la copia de seguridad en kilobytes por segundo

Notificaciones

Acronis Backup & Recovery 10 proporciona la capacidad de informar a los usuarios sobre la finalización de una copia de seguridad por correo electrónico o servicio de mensajes.

Correo electrónico

Esta opción es eficaz tanto para los sistemas operativos de Windows como de Linux.

Esta opción no está disponible cuando se trabaja desde dispositivos de inicio.

La opción le permite recibir notificaciones por correo electrónico sobre la finalización satisfactoria de la tarea de copia de seguridad, fallo o necesidad de interacción por todo el registro de la tarea.

El valor predeterminado: **Deshabilitado**.

Configurar notificación por correo electrónico

1. Active la casilla de verificación **Enviar notificaciones por correo electrónico** para activar las notificaciones.
2. En el campo **Direcciones de correo electrónico**, escriba la dirección de correo electrónico a la que se enviarán las notificaciones. Puede introducir varias direcciones separadas por punto y coma.
3. Debajo de **Enviar notificaciones**, seleccione las casillas de verificación adecuadas como se indica a continuación:
   - **Cuando la copia de seguridad finaliza correctamente**: enviar una notificación cuando la copia de seguridad haya finalizado correctamente.
   - **Cuando la copia de seguridad falla**: enviar una notificación cuando la copia de seguridad falle.

   La casilla de verificación **Cuando la interacción del usuario sea necesaria** está activada.
4. Para que el mensaje de correo electrónico incluya las entradas del registro relacionadas con la copia de seguridad, active la casilla de verificación **Agregar registro completo a la notificación**.
5. Haga clic en **Parámetros adicionales de correo electrónico** para configurar parámetros adicionales de correo electrónico como se detalla a continuación y después haga clic en **Aceptar**:
   - **De**: escriba la dirección de correo electrónico del usuario emisor del mensaje. Si no completa este campo, los mensajes se crearán como si se enviaran desde la dirección de destino.

- **Utilizar cifrado**: puede optar por una conexión cifrada al servidor de correo. Los tipos de cifrado SSL y TLS se encuentran disponibles para su elección.
- 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 **Inicio de la sesión en el servidor de correo entrante** para habilitar el servidor POP y configurar sus ajustes:
  - **Servidor de correo entrante (POP)**: escriba el nombre del servidor POP.
  - **Puerto**: configure el puerto del servidor POP. De manera predeterminada, el puerto está configurado en 110.
  - **Nombre de usuario**: introduzca el nombre de usuario
  - **Contraseña**: introduzca la contraseña.
- Active la casilla de verificación **Utilizar el servidor de correo saliente especificado** para habilitar un servidor SMTP y configurar sus ajustes:
  - **Servidor de correo saliente (SMTP)**: escriba el nombre del servidor SMTP.
  - **Puerto:** configure el puerto del servidor SMTP. De manera predeterminada, el puerto se establece en 25.
  - **Nombre de usuario**: introduzca el nombre de usuario
  - **Contraseña**: introduzca la contraseña.

6. Haga clic en **Enviar mensaje de correo electrónico de prueba** para comprobar que los ajustes son correctos.

Servicio de Messenger (WinPopup)

Esta opción es eficaz para los sistemas operativos Windows y Linux del equipo emisor y sólo para Windows en el equipo receptor.

Esta opción no está disponible cuando se trabaja desde dispositivos de inicio.

La opción le permite recibir notificaciones WinPopup sobre la finalización satisfactoria de la tarea de copia de seguridad, fallo o necesidad de interacción.

El valor predeterminado: **Deshabilitado.**
Antes de configurar las notificaciones de WinPopup, asegúrese de que el servicio Messenger se encuentra activo tanto en el equipo que ejecuta la tarea como en el que recibirá los mensajes.

El servicio Messenger no se activa de manera predeterminada en la familia Microsoft Windows Server 2003. Cambie el servicio de Modo de inicio a Automático e inícielo.

Para configurar las notificaciones de WinPopup:

1. Active la casilla de verificación **Enviar notificaciones de WinPopup**.
2. En el campo **Nombre del equipo**, escriba el nombre del equipo al que se enviarán las notificaciones. No es posible introducir varios nombres.

Debajo de **Enviar notificaciones**, seleccione las casillas de verificación adecuadas como se indica a continuación:

- **Cuando se realiza la copia de seguridad satisfactoriamente**: envía una notificación cuando se completa satisfactoriamente la operación de copia de seguridad.
- **Cuando la copia de seguridad falla**: envía una notificación cuando la copia de seguridad falla.

Casilla de verificación **Cuando se requiere interacción con el usuario**: envía una notificación durante la operación cuando se requiere de la interacción con el usuario, siempre seleccionada.

Haga clic en **Enviar mensaje de WinPopup de prueba** para verificar si la configuración es correcta.

Seguimiento de sucesos

Es posible el envío de los sucesos registrados en las operaciones de copia de seguridad, que funcionan en un equipo gestionado, para los gestores SNMP especificados.

Notificaciones SNMP

Esta opción es eficaz tanto para los sistemas operativos de Windows como de Linux.

Esta opción no está disponible cuando se trabaja desde dispositivos de inicio.

Esta opción define si el agente operativo en el equipo gestionado debe enviar los sucesos de registro de las operaciones de copia de seguridad a los gestores especificados de Protocolo Simple Network Management (SNMP). Puede elegir los tipos de sucesos a enviar.

Para obtener información detallada acerca de cómo utilizar SNMP con Acronis Backup & Recovery 10, vaya a "Asistencia para SNMP (pág. 40)".

El valor predeterminado: **Use la configuración en las configuración del Equipo.**

Opción de seleccionar si se envía los sucesos de operaciones de copia de seguridad a los gestores SNMP:

Elija una de las siguientes opciones:

- **Usar la configuración establecida en las opciones del Equipo:** use la configuración establecida para el equipo. Para obtener más información, consulte opciones de Equipo (pág. 46).
- **Envío individual de notificaciones SNMP para sucesos de operación de copia de seguridad**:envía los sucesos de las operaciones de copia de seguridad al gestor SNMP especificado.
  - **Tipos de sucesos a enviar**: seleccione los tipos de sucesos a enviar. **Todos los sucesos, errores y advertencias**, o **sólo errores**.
  - **Nombre del servidor/IP:** ingrese el nombre o dirección IP del servidor en donde se ejecuta la aplicación de gestión de SNMP y a donde se enviarán los mensajes.
  - **Comunidad**: ingrese el nombre de la comunidad SNMP al que pertenece tanto el servidor que ejecuta la aplicación de gestión de SNMP y el equipo emisor. La comunidad típica es "pública".

  Haga clic en **Enviar mensaje de prueba** para verificar si la configuración es correcta.
- **No enviar notificaciones de SNMP:** deshabilita el envío de sucesos de registro de las operaciones de copia de seguridad de los gestores SNMP.

Copias de seguridad incrementales / diferenciales rápidas

Esta opción es eficaz tanto para los sistemas operativos Windows y Linux y los medios de inicio.

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

Esta opción define si se detecta el cambio de archivos por medio del tamaño de archivo y sellos de tiempo o la comparación del contenido de los archivos con aquellos guardados en el archivo comprimido.

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 desactiva esta característica, el programa comparará el contenido completo del archivo con el que esté guardado en el archivo comprimido.

División de copias de seguridad

Esta opción es eficaz tanto para los sistemas operativos de Windows como de Linux y los medios de inicio.

Esta opción define como se divide la copia de seguridad.

El valor predeterminado: **Automático**

Las siguientes configuraciones están disponibles:

Automático

Con esta configuración, Acronis Backup & Recovery 10 actuará de la siguiente manera.

- **Cuando se realiza una copia de seguridad en el disco duro:**

  Se creará un sólo archivo de copia de seguridad si el sistema de archivos del disco de destino permite el tamaño de archivo estimado.

  La copia de seguridad se dividirá automáticamente en varios archivos si el sistema de archivos del disco de destino no permite el tamaño estimado. Éste puede ser el caso cuando la copia de seguridad se ubica en sistemas de archivos FAT16 y FAT32 que tienen un límite de tamaño de archivo de 4 GB.

  Si el disco de destino se queda sin espacio libre mientras crea la copia de seguridad, la tarea ingresa en el estado **Necesita interacción**. Tiene la posibilidad de liberar espacio y reintentar la operación. Si lo hace, la copia de seguridad resultante se dividirá en las partes creadas antes y después del intento.
- **Cuando se realiza una copia de seguridad en un medio extraíble** (CD, DVD o dispositivo de cinta incluido a nivel local al equipo gestionado):

  La tarea ingresará en el estado **Necesita interacción** y le pedirá un disco nuevo cuando el anterior esté completo.

Tamaño fijo

Ingrese el tamaño de archivo deseado o selecciónelo de la lista desplegable. La copia de seguridad entonces se dividirá en múltiples archivos del tamaño especificado. Esto resulta conveniente cuando se crea una copia de seguridad que planea grabar en múltiples CD, DVD o DVD+R/RW más adelante. Es posible que también desee dividir la copia de seguridad destinada a un servidor FTP, ya que la recuperación de datos directamente desde un servidor FTP requiere que los archivos se dividan en archivos no mayores a los 2GB.

Componentes de medios

Esta opción es eficaz tanto para sistemas operativos de Windows como de Linux, cuando la copia de seguridad es un medio extraíble.

Cuando realice una copia de seguridad a una medio extraíble, puede hacer que ese medio funcione como cualquier medio de inicio (pág. 195) basado en Linux al escribirle componentes adicionales. Como resultado, no necesitará un disco de rescate por separado.

El valor predeterminado: **Ninguno seleccionado.**

Seleccione las casillas de verificación para los componentes que quiera guardar en el medio de inicio:

- **Restauracion con un solo clic** es un componente adicional mínimo para su copia de seguridad del disco almacenada en medio extraíble, lo que permite una recuperación fácil desde la copia de seguridad. Si arranca un equipo desde el dispositivo y hace clic en **Ejecutar Acronis One-click Restore,** todos los datos se recuperarán sin intervención a su ubicación inicial.

  Precaución: Debido a que el enfoque de un solo clic no incluye selecciones por parte del usuario, como seleccionar particiones para restaurar, *Acronis One-Click Restore siempre recupera el disco entero. Si su disco tiene varios volúmenes y planea usar Acronis One-Click Restore, incluya todos los volúmenes de la copia de seguridad. Cualquier volumen que falte en la copia de seguridad se perderá.*

- El **agente de arranque** es una utilidad de rescate de arranque (basado en el kernel de Linux) que incluye la mayoría de las funcionalidades del agente de Acronis Backup & Recovery 10. Guarde este componente en el medio si quiere una mayor funcionalidad durante la recuperación. Entonces podrá configurar la operación de recuperación de la misma manera que bajo un medio de inicio; utilice Active Restore o Universal Restore. Si el dispositivo se está creando en Windows, la función de gestión de disco también estará disponible.

Manejo de errores

Estas opciones son eficaces tanto para los sistemas operativos de Windows como de Linux y los medios de inicio.

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

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

El valor predeterminado: **Deshabilitado**.

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.

Reintentar si se produce un error.

El valor predeterminado: **Habilitado**. **Cantidad de intentos: 5. 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 5 veces. Se detendrán los intentos tan pronto como se reanude la operación o se realice el número de intentos especificados, lo que suceda primero.

Ignorar los sectores defectuosos

El valor predeterminado: **Deshabilitado**.

Cuando la opción está deshabilitada, el programa mostrará una ventana emergente cada vez que se encuentre con un sector defectuoso y le solicitará al usuario que decida si desea continuar o detener el procedimiento de copia de seguridad. 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.

Doble destino

La opción es eficaz para los sistemas operativos de Windows y Linux, cuando el destino primario de la copia de seguridad es una *carpeta local o Acronis Secure Zone* y el destino secundario es *otra carpeta local o red compartida*. Las bóvedas gestionadas y servidores FTP no son compatibles como destinos secundarios.

El valor predeterminado: **Deshabilitado.**

Cuando está habilitado el destino doble, el agente copiará automáticamente cada copia de seguridad creada localmente al segundo lugar de destino como una red compartida. Una vez que se complete la copia de seguridad al primer lugar de destino, el agente compara el contenido del primer archivo comprimido actualizado con el contenido del segundo archivo comprimido y copia todas las copias de seguridad que faltan al segundo lugar de destino junto a la nueva copia de seguridad.

Esta opción permite una copia de seguridad rápida por equipo a la unidad interna como un paso intermedio antes de guardar la copia de seguridad lista en la red. Esto es práctico en caso de que la red esté lenta u ocupada y cuando existen procedimientos de copia de seguridad que requieren mucho tiempo. La desconexión durante la transferencia de la copia no afectará el procedimiento de copia de seguridad, como sucede al realizar copias de seguridad directamente desde la ubicación remota.

Otras ventajas:

- La replicación mejoran la confiabilidad del archivo comprimido.
- Los usuarios itinerantes pueden realizar copias de seguridad de sus equipos portátiles en Acronis Secure Zone mientras están en circulación. Mientras el equipo portátil esté conectado a la red corporativa, se transferirán todos los cambios en el archivo comprimido a la copia estática después de la primera operación de copia de seguridad.

Si selecciona Acronis Secure Zone protegido con contraseña como destino primario, tenga en cuenta que el archivo comprimido en el destino secundario no está protegido con contraseña.

Para utilizar destino doble:

1. Seleccione la casilla de verificación **Utilizar destino doble**.
2. Examinar el segundo lugar de destino o ingrese la ruta completa de destino manualmente.
3. Haga clic en **Aceptar**.

Puede ser que deba proporcionar las credenciales de acceso para el segundo lugar de destino. Ingrese las credenciales cuando se lo pida.

Condiciones de inicio de la tarea

Esta opción es eficaz tanto para los sistemas operativos de Windows como de Linux.

Esta opción no está disponible cuando se trabaja desde dispositivos de inicio.

Esta opción determina el comportamiento del programa si hay una tarea de copia de seguridad que está por iniciarse (el momento programado u ocurra el suceso especificado en el programa) pero no se cumple con la condición (o cualquiera de las condiciones). Para obtener más información sobre las condiciones, consulte Programación (pág. 85) y Condiciones (pág. 92).

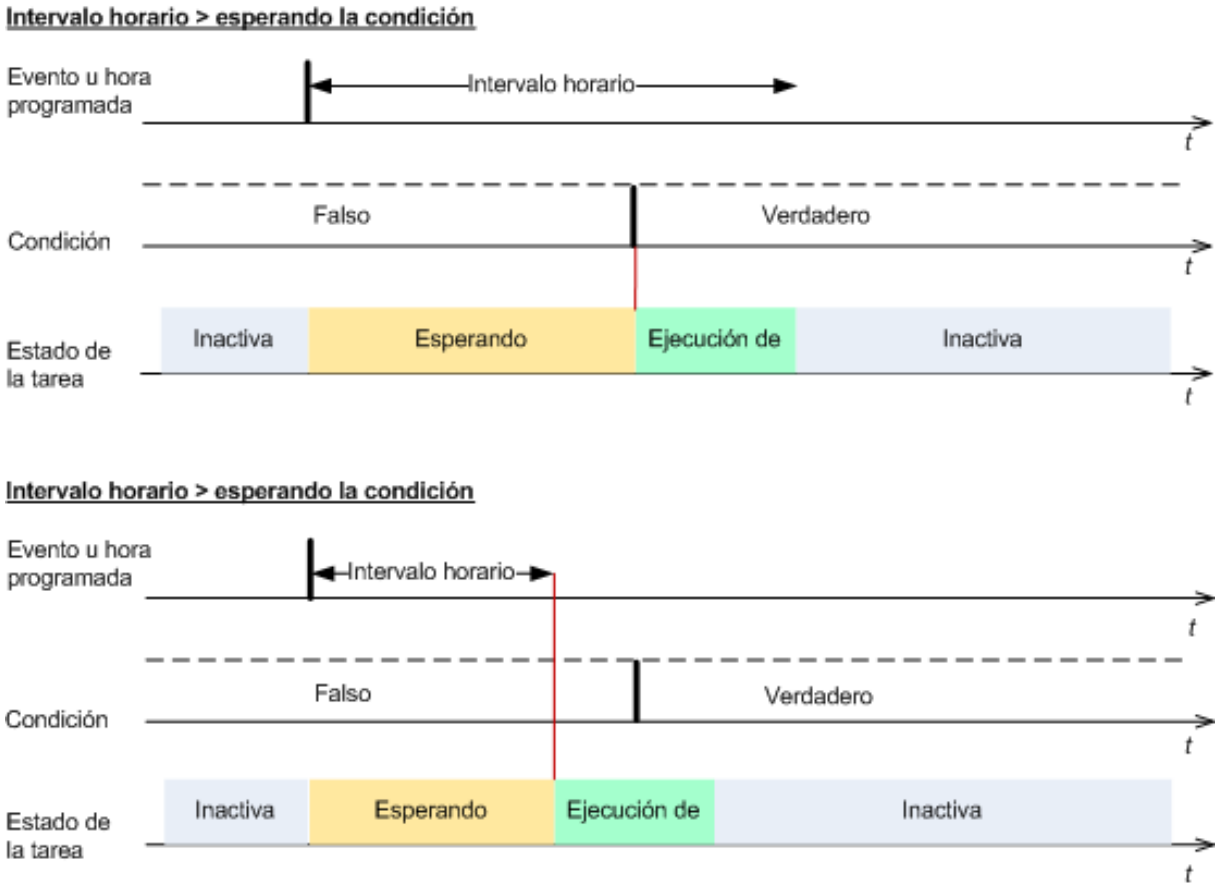
El valor predeterminado: **Esperar hasta que se cumplan las condiciones.**

Esperar hasta que se cumplan las condiciones

Con esta configuración, el Programado comienza a supervisar las condiciones e inicia la tarea cuando se cumplen las condiciones. Si no se cumplen las condiciones, la tarea no comenzará nunca.

Para manejar la situación cuando no se cumplen con las condiciones por mucho tiempo y el retraso de la copia de seguridad se vuelve peligroso, puede definir el intervalo del cual la tarea se ejecutará independientemente de la condición. Seleccione la casilla de verificación **Ejecutar la tarea de todos modos después** y especifique el intervalo de tiempo. La tarea comenzará tan pronto como se cumpla con las condiciones o pase el período máximo de tiempo, lo que suceda primero.

Diagrama temporal: Esperar hasta que se cumplan las condiciones



Omitir la ejecución de tarea

El retraso de una copia de seguridad puede ser inadmisible, por ejemplo, cuando necesite realizar una copia de seguridad estrictamente a la hora especificada. Entonces parece sensato omitir la copia de seguridad en vez de esperar a que se cumplan las condiciones, en especial si los sucesos son frecuentes.

Manejo de fallos de la tarea

Esta opción es eficaz tanto para los sistemas operativos de Windows como de Linux.

Esta opción no está disponible cuando se trabaja desde dispositivos de inicio.

Esta opción determina el comportamiento del programa cuando fallan cualquiera de las tareas del plan de copia de seguridad.

El valor predeterminado es **no reiniciar una tarea que falló.**

Si selecciona la casilla de verificación **Reiniciar una tarea que falló** y especifica la cantidad de intentos y el intervalo de tiempo entre los mismos, el programa intentará ejecutar la tarea que falló nuevamente. 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.

Si falla la tarea por un error en el plan de copia de seguridad, puede editar el plan mientras la tarea esté inactiva. Mientras se ejecute la tarea, debe detenerla antes de editar el plan de copia de seguridad.

Ajustes adicionales

Especifique los ajustes adicionales para la operación de copia de seguridad al seleccionar o desmarcar las siguientes casillas de verificación.

Sobrescribir los datos en una cinta sin solicitar la confirmación del usuario

Esta opción es eficaz sólo cuando se realiza una copia de seguridad en un dispositivo de cinta.

El valor predeterminado: **Deshabilitado**.

Cuando se comienza una copia de seguridad a un dispositivo de cinta que no está vacía en un dispositivo de cinta incluido a nivel local, el programa alerta sobre que perderá los datos en la cinta. Para desactivar esta advertencia, marque la casilla de verificación.

Desmontar dispositivos después de que la copia de seguridad haya finalizado

Esta opción es eficaz tanto para los sistemas operativos de Windows como de Linux.

Esta opción es eficaz cuando se realiza la copia de seguridad en un medio extraíble (CD, DVD, cinta o disquete.)

El valor predeterminado: **Deshabilitado.**

Se puede expulsar el CD/DVD de destino o se puede desmontar la cinta después de que se termine la copia de seguridad.

Solicitar el primer medio al realizar la copia de seguridad en un medio extraíble.

Esta opción es eficaz sólo cuando se realiza una copia de seguridad en un medio extraíble.

La opción define si se muestra la solicitud de medio **Insertar el primer medio** cuando se realiza una copia de seguridad en un medio extraíble.

El valor predeterminado: **Habilitado**.

Cuando la opción está habilitada, quizá no se pueda realizar la copia de seguridad en un medio extraíble si el usuario no se encuentra en el equipo, ya que el programa esperará a que alguien pulse la opción Aceptar en el cuadro de aviso. Por lo tanto, debe deshabilitar el mensaje al programar una copia de seguridad en un medio extraíble. Por lo tanto, si el medio extraíble está disponible (por ejemplo, DVD introducido) la tarea puede ejecutarse sin supervisión.

Restablecer el bit del archivo comprimido

Esta opción es eficaz solamente para copia de seguridad a nivel de archivo para sistemas operativos Windows y en medio de inicio.

El valor predeterminado: **Deshabilitado**.

En sistemas operativos Windows, cada archivo posee el atributo **Archivo listo para archivar** que está disponible al seleccionar **Archivo**->**Propiedades**- >**General**- >**Avanzado**- >**Atributos de archivos comprimidos e índices** El sistema operativo configura este atributo, también conocido como bit del archivo comprimido, cada vez que se modifica el archivo y puede restablecerse mediante las aplicaciones de copia de seguridad cada vez que se incluya un archivo en una copia de seguridad. Diversas aplicaciones utilizan el valor del bit del archivo comprimido, como por ejemplo, las bases de datos.

Cuando se selecciona la casilla de verificación **Reinicio del valor del bit del archivo comprimido,** Acronis Backup & Recovery 10 restablecerá los bits de archivos comprimidos de todos los archivos a los que se les realiza una copia de seguridad. Acronis Backup & Recovery 10 no usará el valor del bit de archivo comprimido. Cuando se realizan copias de seguridad incrementales o diferenciales, determina si se modificó el tamaño o la fecha y hora del archivo cuando se guardó por última vez.

Reiniciar el equipo automáticamente después de que finalice la copia de seguridad

Esta opción sólo está disponible cuando se trabaja desde dispositivos de inicio.

El valor predeterminado: **Deshabilitado**.

Cuando la opción está habilitada, Acronis Backup & Recovery 10 reiniciará el equipo después de completar el proceso de copia de seguridad.

Por ejemplo, si el equipo inicia desde una unidad de disco duro predeterminada y puede seleccionar la casilla de verificación, el equipo se reiniciará y el sistema operativo comenzará tan pronto como el agente de inicio termine de crear la copia de seguridad.

Deduplicar la copia de seguridad sólo después de transferirla a la bóveda (no deduplicar en el origen)

Esta opción está disponible solamente en las ediciones avanzadas de Acronis Backup & Recovery 10.

Esta opción es eficaz tanto para los sistemas operativos Windows como Linux y medios de inicio, cuando el destino de la copia de seguridad es una bóveda de desduplicación.

El valor predeterminado: **Deshabilitado**.

Al habilitar esta opción apaga la desduplicación de la copia de seguridad en el origen, lo que significa que Acronis Backup & Recovery 10 realizará la desduplicación de la copia. El Nodo de almacenamiento después de la copia de seguridad de la bóveda (se llama desduplicación en el destino).

La desactivación de la desduplicación en origen puede llevar a los procesos de copia de seguridad más rápidos pero mayor tráfico en la red y una carga más pesada del nodo de almacenamiento. El tamaño posible de la copia de seguridad en la bóveda es independiente de si está habilitada la desduplicación en el origen.

La desduplicación en el origen y en el destino se describen en Generalidades de Desduplicación.

Guarde el RAID por software y los metadatos de la LVM junto con las copias de seguridad

Esta opción es eficaz sólo para las copias de seguridad a nivel de disco de equipos que ejecutan Linux.

El valor predeterminado: **Habilitado.**

Cuando esta opción esté habilitada, Acronis Backup & Recovery 10 guardará la información sobre la estructura de los volúmenes lógicos (conocidos como volúmenes LVM) y de los dispositivos RAID por software de Linux (conocidos como dispositivos MD), en el directorio **/etc/Acronis** antes de crear la copia de seguridad.

Al recuperar dispositivos MD y volúmenes LVM en el dispositivo de arranque, se puede utilizar esta información para recrear la estructura del volumen de forma automática. Para obtener instrucciones consulte Recuperación de dispositivos MD y volúmenes lógicos (pág. 180).

Cuando utilice esta opción, asegúrese de que el volumen que contiene el directorio **/etc/Acronis** esté entre los volúmenes de los que se va a realizar la copia de seguridad.

Utilizar FTP en modo activo

El valor predeterminado: **Deshabilitado**.

Habilite esta opción si el servidor FTP es compatible con el modo activo y desea utilizar este modo en la transferencia de archivos.

3.3.2 Opciones predeterminadas de recuperación

Cada agente de Acronis tiene sus propias opciones predeterminadas de recuperación. Una vez instalado el agente, las opciones predeterminadas tienen valores predefinidos, que se consideran **preajustes** en la documentación. Cuando realiza una tarea de recuperación, puede utilizar una opción predeterminada o anular la opción predeterminada mediante el valor personalizado que se especificará únicamente para esta tarea.

También puede personalizar una opción predeterminada al cambiar su valor a otro diferente al predefinido. El nuevo valor se utilizará de manera predeterminada para todas las tareas de recuperación que realice en su equipo en adelante.

Para ver y cambiar las opciones de recuperación predeterminadas, conecte la consola al equipo gestionado y después seleccione **Opciones > Opciones predeterminadas de copia de seguridad y recuperación > Opciones predeterminadas de recuperación** en el menú superior.

Disponibilidad de las opciones de recuperación

El conjunto de opciones de recuperación disponibles depende de:

- El entorno en el que opera el agente (Linux, dispositivo de inicio)
- El tipo de datos que se está copiando (disco, archivo)
- El sistema operativo que se está recuperando de la copia de seguridad del disco.

La siguiente tabla resume la disponibilidad de las opciones de recuperación.

	Agente para Linux		**Dispositivo de inicio (basado en Linux o basado en PE)**	
	Recuperación del disco	**Recuperación de los archivos (también desde una copia de seguridad del disco)**	**Recuperación del disco**	**Recuperación de los archivos (también desde una copia de seguridad del disco)**
Comandos antes/después de la recuperación (pág. 70)	+	+	solo PE	solo PE
Prioridad de recuperación (pág. 71)	+	+	-	-
Seguridad a nivel de archivos (pág. 72):				
Recuperar archivos con su configuración de seguridad	-	+	-	+
Manejo de errores (pág. 75):				
No mostrar mensajes ni diálogos durante el procesamiento (modo silencioso)	+	+	+	+
Reintentar si se produce un error	+	+	+	+
Ajustes adicionales (pág. 75):				
Configure la fecha y hora actual para los archivos recuperados	-	+	-	+
Validar el archivo comprimido de copia de seguridad antes de la recuperación	+	+	+	+
Verificar sistema de archivos después de la recuperación	+	-	+	-
Reiniciar automáticamente el equipo si es necesario para la recuperación	+	+	-	-
Cambiar SID después de la recuperación	Recuperación de Windows	-	Recuperación de Windows	-
Notificaciones:				
Correo electrónico (pág. 72)	+	+	-	-
Win Pop-up (pág. 73)	+	+	-	-
Rastreo de eventos:				
SNMP (pág. 74)	+	+	-	-

Comandos pre / post

Esta opción es eficaz tanto para los sistemas operativos de Windows como de Linux y los medios de inicio basados en PE..

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:

- El uso del comando `Checkdisk` para encontrar y reparar los errores en el sistema de archivos en un volumen lógico, los errores físicos o sectores defectuosos se iniciará antes del comienzo de recuperación o después de la finalización de la recuperación.

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.

Para especificar comandos pre/post

1. Puede habilitar la ejecución de comandos pre/post al marcar las siguientes opciones:
   - **Ejecutar antes de la recuperación**
   - **Ejecutar después de la recuperación**
2. Realice uno de los siguientes:
   - Haga clic en **Editar** para especificar un nuevo comando o un archivo por lotes
   - Seleccione el comando existente o el archivo por lotes de la lista desplegable
3. Haga clic en **Aceptar**.

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. En el campo **Comando**, introduzca un comando o examine hasta encontrar un archivo por lotes. El programa no admite comandos interactivos, es decir, comandos que exijan la intervención del usuario (por ejemplo, “pause”).
2. En el campo **Directorio de trabajo**, especifique la ruta mediante la que se ejecutará el comando o archivo por lotes.
3. En el campo **Argumentos**, especifique los argumentos de ejecución del comando, si fuera necesario.
4. Dependiendo del resultado que desee obtener, seleccione la opción apropiada tal y como se describe en la siguiente tabla.
5. Haga clic en **Probar comando** para verificar si el comando es correcto.

Casilla de verificación	**Selección**			
Hacer que la tarea falle si falla la ejecución del comando	Seleccionado	Borrado	Seleccionado	Borrado
No recuperar	Seleccionado	Seleccionado	Borrado	Borrado

hasta que finalice la ejecución de comandos				
Resultado				
	Valor predeterminado Realizar la recuperación solo después de que se ejecute el comando correctamente. Hacer que la tarea 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/A	Realizar la recuperación al mismo tiempo que se ejecuta el comando, independientemente del resultado de la ejecución del comando.

Comandos posteriores a la recuperación

Para especificar un comando o archivo ejecutable después de completar la recuperación

1. En el campo **Comando**, introduzca un comando o examine hasta encontrar un archivo por lotes.
2. En el campo **Directorio de trabajo**, especifique una ruta en donde se ejecutará el comando o archivo por lotes.
3. En el campo **Argumentos**, especifique los argumentos de ejecución del comando, si fuera necesario.
4. Si es crítico que la ejecución del comando sea satisfactoria para su estrategia de copia de seguridad, marque la casilla de verificación **Suspende la tarea si falla la ejecución del comando**. Si la ejecución del comando falla, el resultado de la ejecución de tarea será Error.

   Cuando no se marca la casilla de verificación, los resultados de la ejecución de comando no afectarán el éxito o fallo cuando se ejecute la tarea. Se puede seguir los resultados de la ejecución de comandos al explorar el registro de errores y advertencias que se muestran en el **Tablero**.
5. Haga clic en **Probar comando** para verificar si el comando es correcto.

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

Prioridad de recuperación

Esta opción es eficaz tanto para los sistemas operativos de Windows como de Linux.

Esta opción no está disponible cuando se trabaja desde dispositivos de inicio.

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 velocidad de salida o entrada del disco o el tráfico en la red.

El valor predeterminado: **Normal.**

Para especificar la prioridad del proceso de recuperación

Seleccione una de las siguientes:

- **Bajo**: para minimizar el uso de recursos por parte del proceso de recuperación lo que dejará más recursos para otros procesos que se ejecuten en el equipo.
- **Normal**: ejecución del procesos de recuperación con la velocidad normal, lo que permite asignar recursos al mismo nivel de otros procesos.
- **Alto:** maximizará la velocidad del proceso de recuperación al tomar recursos de otros procesos.

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: **Recupera archivos con su configuración de seguridad**.

Si se preservan los permisos NTFS durante la copia de seguridad, puede elegir entre recuperar los permisos o permitir que los archivos hereden los permisos NTFS de la carpeta desde donde son recuperados.

Notificaciones

Acronis Backup & Recovery 10 proporciona la capacidad de informar a los usuarios sobre la finalización de la recuperación por correo electrónico o servicio de mensajes.

Correo electrónico

Esta opción es eficaz tanto para los sistemas operativos de Windows como de Linux.

Esta opción no está disponible cuando se trabaja desde dispositivos de inicio.

La opción le permite recibir notificaciones por correo electrónico sobre la finalización satisfactoria de la recuperación, fallo o necesidad de interacción con todo el registro de la tarea.

El valor predeterminado: **Deshabilitado**.

Configurar notificación por correo electrónico

1. Active la casilla de verificación **Enviar notificaciones por correo electrónico** para activar las notificaciones.
2. En el campo **Direcciones de correo electrónico**, escriba la dirección de correo electrónico a la que se enviarán las notificaciones. Puede introducir varias direcciones separadas por punto y coma.
3. Debajo de **Enviar notificaciones**, seleccione las casillas de verificación adecuadas como se indica a continuación:
   - **Cuando la copia de seguridad finaliza correctamente**: enviar una notificación cuando la copia de seguridad haya finalizado correctamente.
   - **Cuando la copia de seguridad falla**: enviar una notificación cuando la copia de seguridad falle.

   La casilla de verificación **Cuando la interacción del usuario sea necesaria** está activada.
4. Para que el mensaje de correo electrónico incluya las entradas del registro relacionadas con la copia de seguridad, active la casilla de verificación **Agregar registro completo a la notificación**.

5. Haga clic en **Parámetros adicionales de correo electrónico** para configurar parámetros adicionales de correo electrónico como se detalla a continuación y después haga clic en **Aceptar**:
   - **De**: escriba la dirección de correo electrónico del usuario emisor del mensaje. Si no completa este campo, los mensajes se crearán como si se enviaran desde la dirección de destino.
   - **Utilizar cifrado**: puede optar por una conexión cifrada al servidor de correo. Los tipos de cifrado SSL y TLS se encuentran disponibles para su elección.
   - 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 **Inicio de la sesión en el servidor de correo entrante** para habilitar el servidor POP y configurar sus ajustes:
     - **Servidor de correo entrante (POP)**: escriba el nombre del servidor POP.
     - **Puerto**: configure el puerto del servidor POP. De manera predeterminada, el puerto está configurado en 110.
     - **Nombre de usuario**: introduzca el nombre de usuario
     - **Contraseña**: introduzca la contraseña.
   - Active la casilla de verificación **Utilizar el servidor de correo saliente especificado** para habilitar un servidor SMTP y configurar sus ajustes:
     - **Servidor de correo saliente (SMTP)**: escriba el nombre del servidor SMTP.
     - **Puerto:** configure el puerto del servidor SMTP. De manera predeterminada, el puerto se establece en 25.
     - **Nombre de usuario**: introduzca el nombre de usuario
     - **Contraseña**: introduzca la contraseña.

Haga clic en **Enviar mensaje de correo electrónico de prueba** para comprobar que los ajustes son correctos.

Servicio de Messenger (WinPopup)

Esta opción es eficaz tanto para los sistemas operativos de Windows como de Linux.

Esta opción no está disponible cuando se trabaja desde dispositivos de inicio.

La opción le permite recibir notificaciones WinPopup sobre la finalización satisfactoria de la tarea de recuperación, fallo o necesidad de interacción.

El valor predeterminado: **Deshabilitado.**

Antes de configurar las notificaciones de WinPopup, asegúrese de que el servicio Messenger se encuentra activo tanto en el equipo que ejecuta la tarea como en el que recibirá los mensajes.

El servicio Messenger no se activa de manera predeterminada en la familia Microsoft Windows Server 2003. Cambie el servicio de Modo de inicio a Automático e inícielo.

Para configurar las notificaciones de WinPopup:

1. Active la casilla de verificación **Enviar notificaciones de WinPopup**.
2. En el campo **Nombre del equipo**, escriba el nombre del equipo al que se enviarán las notificaciones. No es posible introducir varios nombres.

3. Debajo de **Enviar notificaciones**, seleccione las casillas de verificación adecuadas como se indica a continuación:
   - **Cuando se realiza la recuperación satisfactoriamente**: envía una notificación cuando la tarea de recuperación se ha completado satisfactoriamente.
   - **Cuando falla la recuperación**: envía una notificación cuando no se realiza la tarea de recuperación.

   Casilla de verificación **Cuando se requiere interacción con el usuario**: envía una notificación durante la operación cuando se requiere de la interacción con el usuario, siempre seleccionada.
4. Haga clic en **Enviar mensaje de WinPopup de prueba** para verificar si la configuración es correcta.

Seguimiento de sucesos

Es posible el envío de los sucesos registrados de la recuperación, que funcionan en un equipo gestionado, para los gestores SNMP específicos.

Notificaciones SNMP

Esta opción es eficaz tanto para los sistemas operativos de Windows como de Linux.

Esta opción no está disponible cuando se trabaja desde dispositivos de inicio.

Esta opción define si el agente operativo en el equipo gestionado debe enviar los sucesos de registro de las operaciones de recuperación de seguridad a los gestores especificados de Protocolo Simple Network Management (SNMP). Puede elegir los tipos de sucesos a enviar.

Para obtener información detallada acerca de cómo utilizar SNMP con Acronis Backup & Recovery 10, vaya a "Asistencia para SNMP (pág. 40)".

El valor predeterminado: **Use la configuración en las configuración del Equipo.**

Opción de seleccionar si se envía los sucesos de operaciones de recuperación a los gestores SNMP:

Elija una de las siguientes opciones:

- **Usar la configuración establecida en las opciones del Equipo:** use la configuración establecida para el equipo. Para obtener más información, consulte opciones de Equipo (pág. 46).
- **Envío individual de notificaciones SNMP para sucesos de recuperación de copia de seguridad**:envía los sucesos de las operaciones de recuperación al gestor SNMP especificado.
  - **Tipos de sucesos a enviar**: seleccione los tipos de sucesos a enviar. **Todos los sucesos, errores y advertencias**, o **sólo errores**.
  - **Nombre del servidor/IP:** ingrese el nombre o dirección IP del servidor en donde se ejecuta la aplicación de gestión de SNMP y a donde se enviarán los mensajes.
  - **Comunidad**: ingrese el nombre de la comunidad SNMP al que pertenece tanto el servidor que ejecuta la aplicación de gestión de SNMP y el equipo emisor. La comunidad típica es "pública".

  Haga clic en **Enviar mensaje de prueba** para verificar si la configuración es correcta.

No enviar notificaciones de SNMP: deshabilita el envío de sucesos de registro de las operaciones de recuperación de los gestores SNMP.

Manejo de errores

Estas opciones son eficaces tanto para los sistemas operativos de Windows como de Linux y los medios de inicio.

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

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.

Reintentar si se produce un error.

El valor predeterminado: **Habilitado**. **Cantidad de intentos: 5. 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 a la ubicación de la red o si no está disponible, el programa intentará llegar al destino cada 30 segundos, pero sólo 5 veces. Se detendrán los intentos tan pronto como se reanude la operación o se realice el número de intentos especificados, lo que suceda primero.

Configuraciones adicionales

Especifique ajustes adicionales para la operación de recuperación al seleccionar o desmarcar las casillas de verificación.

Configure la fecha y hora actual para los archivos recuperados

Esta opción es eficaz sólo con los archivos de recuperación.

El valor predeterminado está **Habilitado**.

Esta opción define si recupera la fecha y hora de los archivos comprimidos o asigna los archivos a la fecha y hora actual.

Validar copia de seguridad antes de la recuperación

El valor predeterminado es **deshabilitado**.

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.

Verificar sistema de archivos después de la recuperación

Esta opción es eficaz sólo cuando se recupera discos o volúmenes.

Cuando funciona desde un dispositivo de inicio, esta opción no es eficaz para el sistema de archivos NTFS.

El valor predeterminado es **deshabilitado**.

Esta opción define si se verifica la integridad del sistema de archivos después de la recuperación del volumen.

Reinicio automático del equipo si es necesario para la recuperación

Esta opción es eficaz cuando se realiza la recuperación en un equipo que ejecuta un sistema operativo.

El valor predeterminado es **deshabilitado**.

La opción define si se reinicio automático del equipo si se los requiere para la recuperación. Éste puede ser el caso cuando se tiene que recuperar un volumen bloqueado por el sistema operativo.

Reinicio del equipo después de la recuperación

Esta opción no está disponible cuando se trabaja desde dispositivos de inicio.

El valor predeterminado es **deshabilitado**.

Esta opción permite que el equipo reinicie con el sistema operativo recuperado sin interacción con el usuario.

Cambiar SID después de finalizar la recuperación

Esta opción no es efectiva cuando el Agente de Acronis Backup & Recovery 10 para ESX/ESXi o el Agente de Acronis Backup & Recovery 10 para Hyper-V realiza la recuperación a una máquina virtual.

El valor predeterminado es **deshabilitado**.

Acronis Backup & Recovery 10 puede generar un identificador de seguridad único (SID) para el sistema recuperado. No necesita un nuevo SID cuando recupera un sistema sobre sí o cuando crea una réplica del sistema para restaurar el sistema original. Genere un nuevo SID si el original y el sistema recuperado funcionarán al mismo tiempo en el mismo grupo de trabajo o dominio.

Utilizar FTP en modo activo

El valor predeterminado: **Deshabilitado**.

Habilite esta opción si el servidor FTP es compatible con el modo activo y desea utilizar este modo en la transferencia de archivos.

4 Bóvedas

Una bóveda es una ubicación para almacenar archivos de copia de seguridad. Para facilitar el uso y la administración, una bóveda está asociada a los metadatos de los archivos comprimidos. La referencia a estos metadatos agiliza y facilita las operaciones con los archivos comprimidos y las copias de seguridad almacenados en la bóveda.

Una bóveda puede organizarse en una unidad local o de red, un medio extraíble o un dispositivo de cinta conectados a Acronis Backup & Recovery 10 Storage Node.

No hay configuración para limitar el tamaño de una bóveda o la cantidad de copias de seguridad de una bóveda. Puede limitar el tamaño de cada archivo comprimido con una limpieza, pero el tamaño total de los archivos comprimidos almacenados en la bóveda solo se limita por el tamaño de almacenamiento.

¿Por qué crear bóvedas?

Le recomendamos que cree una bóveda en cada uno de los destinos donde desee almacenar archivos de copia de seguridad. Esto facilitará su trabajo de la siguiente manera.

Acceso rápido a la bóveda

No tendrá que recordar las rutas a las carpetas donde están almacenados los archivos comprimidos. Al crear un plan de copia de seguridad o una tarea que requiere la selección de un archivo comprimido o el lugar de destino de un archivo comprimido, la lista de bóvedas estará disponible para su rápido acceso sin tener que desplazarse por el árbol de carpetas.

Gestión sencilla de archivos comprimidos

Es posible acceder a una bóveda desde el panel **Navegación**. Una vez que haya seleccionado la bóveda, podrá examinar los archivos comprimidos allí almacenados y realizar las siguientes operaciones de gestión de archivos comprimidos:

- obtener una lista de las copias de seguridad incluidas en cada archivo comprimido,
- recuperar datos desde una copia de seguridad,
- examinar el contenido de una copia de seguridad,
- validar todos los archivos comprimidos de la bóveda o archivos o copias de seguridad individuales,
- montar la copia de seguridad de un volumen para copiar archivos desde la copia de seguridad a un disco físico,
- eliminar de manera segura los archivos comprimidos y las copias de seguridad de los archivos comprimidos.

Es muy recomendable crear bóvedas, aunque esto no es obligatorio. Puede optar por no usar los accesos directos y especificar siempre la ruta completa a la bóveda de los archivos comprimidos. Todas las operaciones anteriores, excepto la eliminación de archivos comprimidos y copias de seguridad, pueden realizarse sin crear bóvedas.

Como resultado de la operación de crear una bóveda, se añade el nombre de la bóveda a la sección **Bóvedas** del panel **Navegación**.

Formas de trabajar con la vista "Bóvedas"

Bóvedas (en el panel de navegación): elemento principal del árbol de bóvedas. Haga clic en este elemento para mostrar los grupos de bóvedas centralizadas y personales.

Personales. Este grupo está disponible cuando la consola está conectada a un equipo gestionado. Expanda este grupo para mostrar una lista de las bóvedas personales creadas en el equipo gestionado.

Haga clic en cualquier bóveda personal del árbol de bóvedas para abrir la vista detallada de esta bóveda (pág. 78) y realizar acciones en la bóveda (pág. 80), los archivos comprimidos (pág. 81) y las copias de seguridad (pág. 82) allí almacenados.

4.1 Bóvedas personales

Una bóveda se denomina personal si fue creada usando una conexión directa entre la consola y un equipo gestionado. Las bóvedas personales son específicas para cada equipo gestionado. Cualquier usuario que pueda registrarse en el sistema puede ver las bóvedas personales. El permiso de un usuario de realizar una copia de seguridad en una bóveda personal está definido por el permiso del usuario para la carpeta o el dispositivo donde está ubicada la bóveda.

Una bóveda personal puede residir en una red compartida, un servidor FTP, un dispositivo extraíble, Acronis Online Backup Storage, un dispositivo de cintas o en una unidad de disco duro local en el equipo. Acronis Secure Zone se considera una bóveda personal disponible para todos los usuarios que puedan iniciar sesión en el sistema. Las bóvedas personales se crean automáticamente al realizar la copia de seguridad en cualquiera de las ubicaciones anteriores.

Las bóvedas personales pueden ser utilizadas por planes de copia de seguridad locales o tareas locales. Los planes de copia de seguridad centralizados no pueden utilizar bóvedas personales, a excepción de Acronis Secure Zone.

Uso compartido de una bóveda personal

Múltiples equipos pueden encontrarse en la misma ubicación física; por ejemplo, en la misma carpeta compartida. Sin embargo, cada uno de los equipos posee su propio acceso directo al árbol de las **Bóvedas**. Los usuarios que realizan una copia de seguridad en una carpeta compartida pueden ver y gestionar los archivos comprimidos de otros usuarios según sus permisos de acceso para esa carpeta. Para facilitar la identificación de los archivos comprimidos, la vista **Bóveda personal** tiene la columna **Propietario** que muestra el propietario de cada archivo comprimido. Para obtener más información sobre el concepto de propietario, consulte Propietarios y credenciales (pág. 23).

Metadatos

La carpeta **.meta** se crea durante la creación de la copia de seguridad en cada una de las bóvedas personales. Esta carpeta contiene información adicional sobre los archivos comprimidos y las copias de seguridad almacenados en la bóveda, como los propietarios de los archivos o el nombre del equipo. Si elimina accidentalmente la carpeta .meta, esta se creará nuevamente de manera automática la próxima vez que acceda a la bóveda. Pero es posible que se pierda alguna información, como los nombres de los propietarios y los nombres de los equipos.

4.1.1 Cómo trabajar con la vista "Bóveda personal"

Esta sección describe brevemente los principales elementos de la vista **Bóveda personal** y sugiere formas de trabajar con ellos.

Barra de herramientas de la bóveda

La barra de herramientas contiene botones operacionales que le permiten realizar operaciones con la bóveda personal seleccionada. Consulte la sección Acciones en bóvedas personales (pág. 80) para obtener más información.

Gráfico circular con leyenda

El **gráfico circular** le permite estimar la carga de la bóveda: muestra la proporción entre el espacio libre y el espacio ocupado de la bóveda.

- espacio libre: espacio en el dispositivo de almacenamiento donde está ubicada la bóveda. Por ejemplo, si la bóveda está ubicada en un disco duro, el espacio libre de la bóveda es el espacio libre del volumen correspondiente.

- espacio ocupado: el tamaño total de los archivos de copia de seguridad y sus metadatos, si están ubicados en la bóveda. No se tienen en cuenta otros archivos que un usuario pueda colocar en esta carpeta.

La **leyenda** muestra la siguiente información sobre la bóveda:

- ruta completa a la bóveda,
- cantidad total de archivos comprimidos y copias de seguridad almacenados en la bóveda,
- proporción entre el espacio ocupado y el tamaño de los datos originales.

Contenido de la bóveda

La sección **Contenido de la bóveda** contiene la tabla y la barra de herramientas de archivos comprimidos. La tabla de archivos comprimidos muestra los archivos comprimidos y las copias de seguridad almacenados en la bóveda. Utilice la barra de herramientas de archivos comprimidos para realizar acciones en los archivos comprimidos y copias de seguridad seleccionados. La lista de copias de seguridad se expande al hacer clic en el signo "más" ubicado a la izquierda del nombre del archivo comprimido. Todos los archivos comprimidos están agrupados por tipo en las siguientes pestañas:

- La pestaña **Archivos comprimidos del disco** enumera todos los archivos comprimidos que contienen copias de seguridad del disco o volumen (imágenes).
- La pestaña **Archivos comprimidos de archivos** enumera todos los archivos comprimidos que contienen copias de seguridad de archivos.

Secciones relacionadas:

Operaciones con archivos comprimidos almacenados en una bóveda (pág. 81)

Operaciones con copias de seguridad (pág. 82)

Filtrado y ordenamiento de archivos comprimidos (pág. 84)

Barras del panel "Acciones y herramientas"

- **[Nombre de la bóveda]** La barra **Acciones** está disponible al hacer clic en la bóveda en el árbol de bóvedas. Duplica las acciones de la barra de herramientas de la bóveda.
- **[Nombre del archivo comprimido]** La barra **Acciones** está disponible al seleccionar un archivo comprimido en la tabla de archivos comprimidos. Duplica las acciones de la barra de herramientas de archivos comprimidos.

- **[Nombre de la copia de seguridad]** La barra **Acciones** está disponible al expandir el archivo comprimido y hacer clic en cualquiera de sus copias de seguridad. Duplica las acciones de la barra de herramientas de archivos comprimidos.

4.1.2 Acciones en bóvedas personales

Para acceder a las acciones

1. Conecte la consola en el servidor de gestión.
2. En el panel de **Navegación**, haga clic en **Bóvedas** > **>Personal**.

Todas las operaciones descritas aquí se realizan al hacer clic en los botones correspondientes de la barra de herramientas de las bóvedas. También es posible acceder a estas operaciones desde el elemento acciones de **[nombre de la bóveda]** del menú principal.

La siguiente es una guía para realizar operaciones con bóvedas personales.

Para	Realizar
Crear una bóveda personal	Haga clic en **Crear**. El procedimiento de creación de bóvedas personales se describe en profundidad en la sección Creación de una bóveda personal (pág. 81).
Edición de una bóveda	1. Seleccione la bóveda. 2. Haga clic en **Editar**. La página **Edición de bóveda personal** permite editar el nombre y la información de la bóveda en el campo **Comentarios**.
Cambiar la cuenta de usuario para acceder a una bóveda	Haga clic en **Cambiar usuario**. En el cuadro de diálogo que aparece, proporcione las credenciales necesarias para acceder a la bóveda.
Crear Acronis Secure Zone	Haga clic en **Crear Acronis Secure Zone**. El procedimiento de creación de Acronis Secure Zone se describe en profundidad en la sección Creación de Acronis Secure Zone (pág. 168).
Explorar el contenido de una bóveda	Haga clic en **Explorar**. En la ventana Explorar que aparece, examine el contenido de la bóveda seleccionada.
Validar una bóveda	Haga clic en **Validar**. Pasará a la página Validación (pág. 152), en donde esta bóveda ya estará preseleccionada como origen. La validación de la bóveda verifica todos los archivos comprimidos almacenados en la bóveda.
Eliminar una bóveda	Haga clic en **Eliminar**. La operación de eliminación en realidad solo quita el acceso directo a la carpeta desde la vista **Bóvedas**. La carpeta en sí permanece intacta. Tiene la opción de conservar o eliminar los archivos comprimidos incluidos en la carpeta.
Actualizar la información de la tabla de bóvedas	Haga clic en **Actualizar**. Mientras revisa el contenido de la bóveda, pueden añadirse archivos comprimidos a la bóveda, como también eliminarse o modificarse. Haga clic en **Actualizar** para actualizar la información de la bóveda con los cambios más recientes.

Creación de una bóveda personal

Para crear una bóveda personal

1. En el campo **Nombre**, introduzca un nombre para la bóveda que se está creando.
2. [Opcional] En el campo **Comentarios**, añada una descripción de la bóveda.
3. En el campo **Ruta**, haga clic en **Cambiar...**
   En la ventana **Ruta de la bóveda personal** que se abre, especifique una ruta a la carpeta que se usará como la bóveda. Una bóveda personal puede organizarse en un medio extraíble o separable, en una red de intercambio, o en un FTP.
4. Haga clic en **Aceptar**. Como resultado, la bóveda creada aparecerá en el grupo **Personales** del árbol de bóvedas.

Combinación y movimiento de bóvedas personales

¿Qué sucede si necesito mover la bóveda existente de un lugar a otro?

Haga lo siguiente

1. Asegúrese de que ninguno de los planes de copia de seguridad utilice la bóveda existente mientras mueve los archivos o deshabilita temporalmente (pág. 107) los programas de los planes en cuestión.
2. Mueva la carpeta de la bóveda con todos sus archivos comprimidos a un nuevo lugar manualmente mediante un administrador de archivos de terceros.
3. Cree una nueva bóveda.
4. Edite los planes y las tareas de la copia de seguridad: redirija su destino a la nueva bóveda.
5. Elimine la bóveda anterior.

¿Cómo puedo combinar dos bóvedas?

Supongamos que tiene dos bóvedas, *A* y *B*, en uso. Los planes de copia de seguridad utilizan ambas bóvedas. Decide dejar solo la bóveda *B* y mover allí todos los archivos comprimidos de la bóveda *A*.

Para eso, haga lo siguiente

1. Asegúrese de que ninguno de los planes de copia de seguridad utilice la bóveda *A* mientras realiza la combinación o deshabilita temporalmente (pág. 107) los programas de los planes en cuestión.
2. Mueva los archivos comprimidos a la bóveda *B* manualmente mediante un administrador de archivos de terceros.
3. Edite los planes de copia de seguridad que utilizan la bóveda *A*: redirija su destino a la bóveda *B*.
4. En el árbol de bóvedas, seleccione la bóveda *B* para verificar si se muestran los archivos comprimidos. Si no aparecen, haga clic en **Actualizar**.
5. Elimine la bóveda *A*.

4.2 Operaciones comunes

4.2.1 Operaciones con archivos comprimidos almacenados en una bóveda

Para realizar cualquier operación con un archivo comprimido, primero deberá seleccionarlo. Si el archivo comprimido está protegido con una contraseña, se le solicitará que la introduzca.

Todas las operaciones descritas a continuación se realizan haciendo clic en los botones correspondientes de la barra de herramientas. También es posible acceder a estas operaciones desde la barra **Acciones de [nombre del archivo comprimido]** (en el panel **Acciones y herramientas**) y desde el elemento **Acciones de [nombre del archivo comprimido]** del menú principal respectivamente.

La siguiente es una guía para realizar operaciones con los archivos comprimidos almacenados en una bóveda.

Operación	Procedimiento
Validar un archivo comprimido	Haga clic en **Validar**. La página **Validación** (pág. 152) se abrirá con el archivo comprimido preseleccionado como origen. La validación de un archivo comprimido verificará todas las copias de seguridad del archivo comprimido.
Exportación de archivos comprimidos	Haga clic en **Exportar**. La página **Exportar** (pág. 160) se abrirá con el archivo comprimido preseleccionado como origen. La exportación de un archivo comprimido crea un duplicado del mismo con todas sus copias de seguridad en la ubicación que se especifique.
Eliminar un solo archivo comprimido o varios archivos comprimidos	1. Seleccione los archivos comprimidos o uno de los archivos comprimidos que desee eliminar. 2. Haga clic en **Eliminar**. El programa duplica la selección en la ventana **Eliminación de copias de seguridad** (pág. 83) que tiene casillas de verificación para cada archivo comprimido y cada copia de seguridad. Revise la selección y efectúe las correcciones necesarias (seleccione las casillas de verificación de los archivos comprimidos deseados) y después confirme la eliminación.
Eliminar todos los archivos comprimidos de la bóveda	Tenga en cuenta que si se aplicaron filtros a la lista de bóvedas, verá solo una parte del contenido de la bóveda. Asegúrese de que la bóveda no contenga archivos comprimidos que necesite conservar antes de iniciar la operación. Haga clic en **Eliminar todo**. El programa duplica la selección en la nueva ventana que tiene casillas de verificación para cada archivo comprimido y cada copia de seguridad. Revise la selección y efectúe las correcciones necesarias, y después confirme la eliminación.

4.2.2 Operaciones con copias de seguridad

Para realizar cualquier operación con una copia de seguridad, primero deberá seleccionarla. Para seleccionar una copia de seguridad, expanda el archivo comprimido y después haga clic en la copia de seguridad. Si el archivo comprimido está protegido con una contraseña, se le solicitará que la introduzca.

Todas las operaciones descritas a continuación se realizan haciendo clic en los botones correspondientes de la barra de herramientas. También es posible acceder a estas operaciones desde la barra **Acciones de "[nombre de la copia de seguridad]"** (en el panel **Acciones y herramientas**) y desde el elemento **Acciones de "[nombre de la copia de seguridad]"** del menú principal.

La siguiente es una guía para realizar operaciones con copias de seguridad.

Operación	Procedimiento
Ver el contenido de la copia de seguridad en una ventana separada	Haga clic en **Ver contenido**. En la ventana **Contenido de la copia de seguridad**, examine el contenido de la copia de seguridad.
Recuperar	Haga clic en **Recuperar**. La página **Recuperar datos** se abrirá con la copia de seguridad preseleccionada como origen.
Validar una copia de seguridad	Haga clic en **Validar**. La página **Validación (pág. 152)** se abrirá con la copia de seguridad preseleccionada como origen. La validación de la copia de seguridad de un archivo imita la recuperación de todos los archivos de la copia de seguridad en un destino simulado. La validación de la copia de seguridad de un disco calcula la suma de comprobación por cada bloque de datos guardado en la copia de seguridad.
Exportación de una copia de seguridad	Haga clic en **Exportar**. La página **Exportar** (pág. 160) se abrirá con la copia de seguridad preseleccionada como origen. La exportación de una copia de seguridad crea un nuevo archivo comprimido con una copia autosuficiente de la copia de seguridad en la ubicación que se especifique.
Eliminar una sola o varias copias de seguridad	Seleccione una de las copias de seguridad que desee eliminar y después haga clic en **Eliminar**. El programa duplica la selección en la ventana **Eliminación de copias de seguridad** (pág. 83) que tiene casillas de verificación para cada archivo comprimido y cada copia de seguridad. Revise la selección y efectúe las correcciones necesarias (seleccione las casillas de verificación de las copias de seguridad deseadas) y después confirme la eliminación.
Eliminar todos los archivos comprimidos y las copias de seguridad de la bóveda	Tenga en cuenta que si se aplicaron filtros a la lista de bóvedas, verá solo una parte del contenido de la bóveda. Asegúrese de que la bóveda no contenga archivos comprimidos que necesite conservar antes de iniciar la operación. Haga clic en **Eliminar todo**. El programa duplica la selección en la ventana **Eliminación de copias de seguridad** (pág. 83) que tiene casillas de verificación para cada archivo comprimido y cada copia de seguridad. Revise la selección y efectúe las correcciones necesarias, y después confirme la eliminación.

4.2.3 Eliminación de archivos comprimidos y copias de seguridad

La ventana **Eliminación de copias de seguridad** muestra la misma pestaña que la vista de las bóvedas, pero con casillas de verificación para cada archivo comprimido y copia de seguridad. El archivo comprimido o la copia de seguridad que eligió eliminar tienen la marca de verificación. Revise el archivo comprimido o la copia de seguridad que seleccionó para eliminar. Si necesita eliminar otros archivos comprimidos y copias de seguridad, seleccione las casillas de verificación respectivas y después haga clic en **Eliminar seleccionados** y confirme la eliminación.

Los filtros de esta ventana provienen de la lista de archivos comprimidos de la vista de bóvedas. Por lo tanto, si se aplicaron algunos filtros a la lista de archivos comprimidos, aquí se mostrarán solo los archivos comprimidos y las copias de seguridad correspondientes a estos filtros. Para ver todo el contenido, limpie todos los campos de los filtros.

¿Qué sucede si elimino una copia de seguridad que es la base de una copia de seguridad incremental o diferencial?

Para conservar la consistencia de los archivos comprimidos, el programa consolidará las dos copias de seguridad. Por ejemplo, elimina una copia de seguridad completa, pero retiene la siguiente incremental. Las copias de seguridad se combinarán en una sola copia de seguridad completa que tendrá la fecha de la copia de seguridad incremental. Cuando elimina una copia de seguridad incremental o diferencial desde la mitad de la cadena, el tipo de copia de seguridad resultante será incremental.

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.

Debe haber suficiente espacio en la bóveda para los archivos temporales creados durante la consolidación. Las copias de seguridad resultantes de la consolidación siempre usarán la compresión máxima.

4.2.4 Filtrado y ordenamiento de archivos comprimidos

La siguiente es una guía para filtrar y ordenar archivos comprimidos en la tabla de archivos comprimidos.

Para	Haga lo siguiente
Ordenar los archivos de copia de seguridad por cualquier columna	Haga clic en el encabezado de la columna para ordenar los archivos comprimidos en orden ascendente. Haga clic nuevamente sobre este para ordenar los archivos comprimidos en orden descendente.
Filtrar los archivos por nombre, propietario o equipo	En el campo ubicado debajo del encabezado de la columna correspondiente, escriba el nombre del archivo comprimido (el nombre del propietario o del equipo). Como resultado, verá la lista de archivos comprimidos cuyos nombres (nombres de los propietarios o de los equipos) coinciden total o solo parcialmente con el valor introducido.

Configuración de la tabla de archivos comprimidos

De manera predeterminada, la tabla muestra siete columnas, las otras están ocultas. De ser necesario, puede ocultar las columnas que se muestran y mostrar las ocultas.

Mostrar u ocultar columnas

1. Haga clic con el botón derecho en el encabezado de cualquier columna para abrir el menú contextual. Los elementos del menú que no estén seleccionados corresponden a los encabezados de las columnas presentadas en la tabla.
2. Haga clic sobre los elementos que quiera mostrar/ocultar.

5 Programación

El programador de Acronis ayuda a que el administrador adapte los planes de copia de seguridad a la rutina diaria de la empresa y al estilo de trabajo de cada empleado. Las tareas de los planes se iniciarán de forma sistemática y los datos importantes estarán protegidos.

El programador usa la hora local del equipo donde se encuentra el plan de copia de seguridad. Antes de crear una programación, asegúrese de que la configuración de fecha y hora del equipo sea correcta.

Programación

Para definir cuándo se debe ejecutar una tarea, tendrá que especificar uno o varios sucesos. La tarea se iniciará ni bien ocurran los sucesos. En la siguiente tabla se enumeran los sucesos disponibles para el sistema operativo Linux.

Sucesos
Período: diariamente, semanalmente, mensualmente
Tiempo transcurrido desde que se completó correctamente la última copia de seguridad (especifique la duración)
Inicio del sistema

Condición

Para operaciones de copia de seguridad únicamente, puede especificar una o varias condiciones además de los sucesos. Cuando ocurre alguno de los sucesos, el programador verifica la condición y ejecuta la tarea si la condición se cumple. En el caso de varias condiciones, deben cumplirse todas simultáneamente para que se ejecute la tarea. En la siguiente tabla se enumeran las condiciones disponibles para el sistema operativo Linux.

Condición: ejecute la tarea solo si
El servidor de ubicación no está disponible
El horario de ejecución de la tarea se encuentra dentro del intervalo especificado.
Transcurrió el período especificado desde que la última copia de seguridad se completó correctamente.

En caso de que el suceso ocurra, pero la condición (o alguna de ellas) no se cumpla, el comportamiento del programador estará definido por la opción de copia de seguridad Condiciones de inicio de la tarea (pág. 64).

Posibles situaciones

- **¿Qué sucede si ocurre un suceso (y se cumple una condición, si la hubiera) mientras la ejecución de la tarea anterior no se completó?**

  Se omitirá el suceso.
- **¿Qué sucede si ocurre un suceso mientras el programador está esperando que se cumpla la condición necesaria para el suceso anterior?**

  Se omitirá el suceso.
- **¿Qué sucede si la condición no se cumple durante un tiempo prolongado?**

Si retrasar la copia de seguridad resulta riesgoso, puede forzar la condición (pedir a los usuarios que cierren la sesión) o ejecutar la tarea manualmente. Para solucionar la situación de forma automática, puede establecer el intervalo después del cual la tarea se ejecutará, independientemente de la condición.

5.1 Programación diaria

La programación diaria es eficaz tanto para los sistemas operativos Windows como Linux.

Para especificar una programación diaria:

En el área **Programar**, seleccione el parámetro apropiado de la siguiente manera:

Cada: <...> día(s)	Establezca la cantidad de días que desea que transcurra entre la ejecución de las tareas. Por ejemplo, si establece Cada 2 día(s), la tarea se iniciará día de por medio.

En el área **Durante el día ejecute la tarea...**, seleccione una de las siguientes opciones:

Una vez a las: <...>	Establezca la hora en la cual se ejecutará la tarea una vez.
Cada: <...> **Desde: <...>** **Hasta: <...>**	Establezca la cantidad de veces que se reiniciará la tarea durante el intervalo especificado. Por ejemplo, si establece la frecuencia de la tarea como Cada 1 hora Desde 10:00:00 hasta 22:00:00, la tarea se ejecutará 12 veces: desde las 10:00 hasta las 22:00 durante un día.

En el área **Vigente...**, establezca las siguientes opciones:

Desde: <...>	Establezca una fecha para que se habilite esta programación (una fecha de entrada en vigencia). Si se desmarca esta casilla de verificación, la tarea se iniciará el día y la hora más próximos a los que especificó anteriormente.
Hasta: <...>	Establezca una fecha para que se deshabilite esta programación. Si se desmarca esta casilla de verificación, la tarea se ejecutará durante una cantidad indefinida de días.

La configuración de programación avanzada está disponible únicamente para equipos registrados en Acronis Backup & Recovery 10 Management Server. Para especificar esta configuración, haga clic en **Cambiar** en el área **Ajustes avanzados**.

Toda la configuración se muestra en el campo **Resultado** en la parte inferior de la ventana.

Ejemplos

Programación diaria "Simple"

Se ejecuta la tarea todos los días a las 18:00.

Los parámetros de programación se establecen de la siguiente manera:

1. Cada: **1** día(s).
2. Una vez a las: **18:00:00.**
3. Vigente:

   Desde: **no establecido**. La tarea se iniciará en el día actual, si se creó antes de las 18:00. Si creó la tarea después de las 18:00, se iniciará por primera vez al día siguiente a las 18:00.

   Hasta: **no establecido**. La tarea se llevará a cabo durante una cantidad indefinida de días.

Programación "Intervalo de tres horas durante tres meses"

Ejecutar la tarea cada tres horas. La tarea se inicia en una fecha determinada (digamos, 15 de septiembre de 2009) y termina al cabo de tres meses.

Los parámetros de programación se establecen de la siguiente manera:

1. Cada: **1** día(s).
2. Cada: **3** horas

   Desde: **12:00:00.** (medianoche) Hasta: **21:00:00**: en este caso, la tarea se realizará 8 veces por día con un intervalo de 3 horas. Después de la última repetición diaria a las 21:00, llega el día siguiente y la tarea vuelve a comenzar desde la medianoche.
3. Vigente:

   Desde: **15/09/09**. Si 15 de septiembre de 2009 es la fecha actual de creación de la tarea y, digamos, 13:15 es la hora de creación, la tarea se iniciará cuando llegue el intervalo más próximo: a las 15:00 en nuestro ejemplo.

   Hasta: **15/12/09**. En esta fecha la tarea se llevará acabo por última vez, pero continuará disponible en la vista **Tareas**.

Varias programaciones diarias para una tarea

En algunos casos, es posible que necesite que la tarea se ejecute varias veces por día, o incluso varias veces por día con intervalos distintos. En esas ocasiones, sería conveniente añadir varias programaciones para una única tarea.

Por ejemplo, supongamos que la tarea debe ejecutarse cada 3 días, desde el 20/09/09, cinco veces por día:

- por primera vez a las 08:00.
- por segunda vez a las 00:00. (mediodía)
- por tercera vez a las 15:00.
- por cuarta vez a las 17:00
- por quinta vez a las 19:00.

Lo más obvio es añadir cinco programaciones simples. Si lo analiza un minuto, seguro se le ocurrirá una manera más conveniente. Como puede ver, el intervalo entre la primera y la segunda repetición de la tarea es de 4 horas y entre la tercera, la cuarta y la quinta es de 2 horas. En este caso, la manera más conveniente es añadir dos programaciones a la tarea.

Primera programación diaria

1. Cada: **3** día(s).
2. Cada: **4** horas.

   Desde: **08:00:00.** Hasta: **12:00:00.**
3. Vigente:

   Desde: **09/20/2009**.

   Hasta: **no establecido**.

Segunda programación diaria

1. Cada: **3** día(s).
2. Cada: **2** hora(s).

   Desde: **15:00:00.** Hasta: **19:00:00.**

3. Vigente:

   Desde: **09/20/2009**.

   Hasta: **no establecido**.

5.2 Programación semanal

La programación semanal es eficaz tanto para los sistemas operativos Windows como de Linux.

Para especificar una programación semanal:

En el área **Programar**, seleccione el parámetro apropiado de la siguiente manera:

Cada: <...> semana(s) el: <...>	Especifique una cantidad de semanas y los días en los que desea que se ejecute la tarea. Por ejemplo: con la configuración Cada **2** semana(s) el **Lun** la tarea se realizará lunes de por medio.

En el área **Durante el día ejecute la tarea...**, seleccione una de las siguientes opciones:

Una vez a las: <...>	Establezca la hora en la cual se ejecutará la tarea una vez.
Cada: <...> **Desde: <...>** **Hasta: <...>**	Establezca la cantidad de veces que se ejecutará la tarea durante el intervalo especificado. Por ejemplo: si establece la frecuencia de la tarea como Cada **1** hora Desde **10:00:00** hasta **22:00:00**, la tarea se llevará a cabo 12 veces desde las 10:00 hasta las 22:00 durante un día.

En el área **Vigente...**, establezca las siguientes opciones:

Desde: <...>	Establezca una fecha para que se habilite esta programación (una fecha de entrada en vigencia). Si se desmarca esta casilla de verificación, la tarea se iniciará el día y la hora más próximos a los que especificó anteriormente.
Hasta: <...>	Establezca una fecha para que se deshabilite esta programación. Si se desmarca esta casilla de verificación, la tarea se llevará a cabo durante una cantidad indefinida de semanas.

La configuración de programación avanzada está disponible únicamente para equipos registrados en Acronis Backup & Recovery 10 Management Server. Para especificar esta configuración, haga clic en **Cambiar** en el área **Ajustes avanzados**.

Toda la configuración se muestra en el campo **Resultado** en la parte inferior de la ventana.

Ejemplos

Programación "Un día de la semana"

La tarea se ejecuta todos los viernes a las 10 p. m., se inicia un día en particular (digamos, 14/05/09) y finaliza al cabo de seis meses.

Los parámetros de programación se establecen de la siguiente manera:

1. Cada: **1** semana(s) los: **Vier**.
2. Una vez a las: **10:00:00 p. m**.
3. Vigente:

   Desde las: **13/05/09**. La tarea se iniciará el viernes siguiente a las 10 p. m.

   Hasta: **13/11/09**. La tarea se realizará por última vez en esta fecha, pero continuará disponible en la vista Tareas pasada esta fecha. (Si la fecha no cayera un viernes, la tarea se realizaría por última vez el viernes anterior a esa fecha).

Esta programación se utiliza comúnmente cuando se crea un esquema de copia de seguridad personalizado. La programación similar a "Un día de la semana" se añade a las copias de seguridad completas.

Programación "Días hábiles"

Ejecute la tarea todas las semanas los días hábiles: de lunes a viernes. Durante un día hábil, la tarea se inicia sólo una vez a las 21:00.

Los parámetros de programación se establecen de la siguiente manera:

1. Cada: **1** semana(s) los: **<Días hábiles>**: al seleccionar la casilla de verificación <Días hábiles> se marcarán automáticamente las casillas de verificación correspondientes (**Lun**, **Mar**, **Miér**, **Jue** y **Vier**) y las demás quedarán como están.
2. Una vez a las: **21:00:00.**
3. Vigente:

   Desde: **vacío**. Si creó la tarea, digamos, el lunes a las 11:30, se iniciará por primera vez el mismo día a las 21:00. Si creó la tarea, digamos, el viernes después de las 21:00, esta se iniciará por primera vez el siguiente día hábil (en nuestro ejemplo, el lunes) a las 21:00.

   Fecha de finalización: **vacío**. La tarea se reiniciará durante una cantidad indefinida de semanas.

Esta programación se utiliza comúnmente cuando se crea un esquema de copia de seguridad personalizado. La programación "Días hábiles" se añade a las copias de seguridad incrementales, mientras que las copias de seguridad completas se programan para realizarse un día de la semana. Para obtener más información, consulte el ejemplo de copias de seguridad completas e incrementales más limpieza en la sección Esquema de copia de seguridad personalizado (pág. 134).

Varias programaciones semanales para una tarea

En los casos en los que la tarea deba llevarse a cabo en diferentes días de las semanas con intervalos distintos, sería conveniente añadir una programación dedicada para cada día de la semana deseado, o para varios días.

Por ejemplo, si necesita que la tarea se ejecute con la siguiente programación:

- Lunes: dos veces, a las 00:00 (mediodía) y a las 21:00
- Martes: cada 3 horas, de 09:00 a 21:00
- Miércoles: cada 3 horas, de 09:00 a 21:00
- Jueves: cada 3 horas, de 09:00 a 21:00
- Viernes: dos veces, a las 00:00 y a las 21:00 (es decir, igual que los lunes)
- Sábado: una vez a las 21:00
- Domingo: una vez a las 21:00

Al combinar los horarios iguales, se pueden añadir las tres programaciones siguientes a la tarea:

Primera programación

1. Cada: **1** semana(s) los: **Lun**, **Vier**.
2. Cada: **9** horas

   Desde: **00:00:00.** Hasta: **21:00:00**.
3. Vigente:

   Desde: **no establecido**.

   Hasta: **no establecido**.

Segunda programación

1. Cada **1** semana(s) los: **Mar**, **Miér**, **Jue**.
2. Cada **3** horas
   Desde **09:00:00.** Hasta **21:00:00**.
3. Vigente:
   Desde: **no establecido**.
   Hasta: **no establecido**.

Tercera programación

1. Cada: **1** semana(s) los: **Sáb, Dom**.
2. Una vez a las: **21:00:00**.
3. Vigente:
   Desde: **no establecido**.
   Hasta: **no establecido**.

5.3 Programación mensual

La programación mensual es eficaz tanto para los sistemas operativos Windows como Linux.

Para especificar una programación mensual:

En el área **Programar**, seleccione el parámetro apropiado de la siguiente manera:

Meses: <...>	Seleccione los meses en los que desea ejecutar la tarea.
Días: <...>	Seleccione los días específicos en el mes para llevar a cabo la tarea. También puede seleccionar el último día del mes, independientemente de cuál sea la fecha.
Los: <...> <...>	Seleccione los días específicos de las semanas para ejecutar la tarea.

En el área **Durante el día ejecute la tarea...**, seleccione una de las siguientes opciones:

Una vez a las: <...>	Establezca la hora en la cual se ejecutará la tarea una vez.
Cada: <...> **Desde: <...>** **Hasta: <...>**	Establezca la cantidad de veces que se ejecutará la tarea durante el intervalo especificado. Por ejemplo: si establece la frecuencia de la tarea como Cada **1** hora Desde **10:00:00** hasta **22:00:00**, la tarea se llevará a cabo 12 veces desde las 10:00 hasta las 22:00 durante un día.

En el área **Vigente...**, establezca las siguientes opciones:

Desde: <...>	Establezca una fecha para que se habilite esta programación (una fecha de entrada en vigencia). Si se desmarca esta casilla de verificación, la tarea se iniciará el día y la hora más próximos a los que especificó anteriormente.
Hasta: <...>	Establezca una fecha para que se deshabilite esta programación. Si se desmarca esta casilla de verificación, la tarea se ejecutará durante una cantidad indefinida de meses.

La configuración de programación avanzada está disponible únicamente para equipos registrados en Acronis Backup & Recovery 10 Management Server. Para especificar esta configuración, haga clic en **Cambiar** en el área **Ajustes avanzados**.

Toda la configuración se muestra en el campo **Resultado** en la parte inferior de la ventana.

Ejemplos

Programación "Último día de cada mes"

Ejecute la tarea una vez a las 22:00 durante el último día de cada mes.

Los parámetros de programación se establecen de la siguiente manera:

1. Meses: **<Todos los meses>**.
2. Días: **Último**. La tarea se ejecutará el último día de cada mes, independientemente de cuál sea la fecha.
3. Una vez a las: **22:00:00**.
4. Vigente:

   Desde: **vacío**.

   Hasta: **vacío**.

Esta programación se utiliza comúnmente cuando se crea un esquema de copia de seguridad personalizado. La programación "Último día de cada mes" se añade a las copias de seguridad completas, mientras que las copias de seguridad diferenciales se programan para realizarse una vez por semana y las incrementales, los días hábiles. Para obtener más información, consulte el ejemplo de Copias de seguridad completas mensuales, diferenciales semanales e incrementales diarias más limpieza en la sección Esquema de copia de seguridad personalizado (pág. 134).

Programación "Estación"

La tarea se ejecuta todos los días hábiles durante las estaciones de otoño de 2009 y 2010 (para el hemisferio norte). Durante un día hábil, la tarea se realiza cada 6 horas desde las 12:00 (medianoche) hasta las 18:00.

Los parámetros de programación se establecen de la siguiente manera:

1. Meses: **septiembre, octubre, noviembre**.
2. Los: **<todos los> <días hábiles>**.
3. Cada: **6** horas.

   Desde: **12:00:00.** Hasta: **18:00:00**.
4. Vigente:

   Desde: **30/08/09**. En realidad, la tarea se iniciará el primer día hábil de septiembre. Al establecer esta fecha, lo único que definimos es que la tarea debe iniciarse en 2009.

   Hasta: **1/12/10**. En realidad, la tarea finalizará el último día hábil de noviembre. Al establecer esta fecha, lo único que definimos es que la tarea debe finalizar en 2010, cuando termina el otoño en el hemisferio norte.

Varias programaciones mensuales para una tarea

En los casos en los que la tarea deba ejecutarse en diferentes días de las semanas con intervalos distintos según el mes, sería conveniente añadir una programación dedicada para cada mes deseado, o para varios meses.

Supongamos que la tarea entra en vigencia el 1/11/09.

- Durante el invierno en el hemisferio norte, la tarea se ejecuta una vez a las 22:00 todos los días hábiles.
- Durante la primavera y el otoño (también del norte), la tarea se ejecuta cada 12 horas todos los días hábiles.

- Durante el verano (también del norte), la tarea se ejecuta todos los días primero y quince de cada mes a las 22:00.

Por lo tanto, se añaden las tres programaciones siguientes a la tarea:

Primera programación

1. Meses: **diciembre**, **enero**, **febrero**.
2. Los: **<todos> <todos los días hábiles>**
3. Una vez a las: **22:00:00**.
4. Vigente:
   Desde: **11/01/2009**.
   Hasta: **no establecido**.

Segunda programación

1. Meses: **marzo**, **abril**, **mayo**, **septiembre**, **octubre**, **noviembre**.
2. Los: **<todos> <todos los días hábiles>**.
3. Cada: **12 horas**
   Desde: **12:00:00.** Hasta: **00:00:00.**
4. Vigente:
   Desde: **11/01/2009**.
   Hasta: **no establecido**.

Tercera programación

1. Meses: **junio**, **julio**, **agosto**.
2. Días: **1**, **15**.
3. Una vez a las: **22:00:00**.
4. Vigente:
   Desde: **11/01/2009**.
   Hasta: **no establecido**.

5.4 Condiciones

Las condiciones otorgan más flexibilidad al programador y le permiten llevar a cabo tareas de copia de seguridad con respecto a ciertas condiciones. Cuando ocurre un suceso especificado (consulte la sección "Programación (pág. 85)" para ver los sucesos disponibles), el programador verifica la condición especificada y lleva a cabo la tarea si se cumple con dicha condición.

En caso de que el suceso ocurra pero la condición (o alguna de ellas si son varias) no se cumpla, el comportamiento del programador estará definido por la opción de copia de seguridad **Condiciones de inicio de la tarea** (pág. 64). Allí, podrá determinar la importancia de las condiciones para la estrategia de copia de seguridad:

- condiciones obligatorias: la ejecución de la tarea de copia de seguridad se pone en espera hasta que se cumplan todas las condiciones.
- condiciones opcionales, pero la ejecución de la tarea de copia de seguridad tiene mayor prioridad: la ejecución de la tarea de copia de seguridad se pone en espera durante el intervalo especificado. Si el intervalo finaliza y las condiciones no se cumplieron, la tarea se ejecuta de todas maneras. Con esta configuración, el programa controla la situación automáticamente

cuando las condiciones no se cumplen durante mucho tiempo y una mayor demora de la copia de seguridad no es conveniente.

- la hora de inicio de la tarea de copia de seguridad es importante: la tarea de copia de seguridad se omite si no se cumplieron las condiciones a la hora en que se debería iniciar la tarea. Omitir la tarea es conveniente si necesita realizar copias de seguridad de datos estrictamente a la hora especificada, especialmente si los sucesos ocurren con cierta frecuencia.

Las condiciones están disponibles tan solo cuando el esquema personalizado de copia de seguridad (pág. 134) esté siendo utilizado. Puede establecer las condiciones de forma separada para una copia de seguridad completa, incremental y diferencial.

Incorporación de varias condiciones

Si se añaden varias condiciones, deben cumplirse todas simultáneamente para que se lleve a cabo la tarea.

5.4.1 El servidor de ubicación no está disponible

Se aplica a: Windows, Linux

"El servidor de ubicación está disponible" significa que el equipo que alberga el destino para almacenar los archivos comprimidos en una unidad de red está disponible.

Ejemplo:

La creación de copias de seguridad de los datos en la ubicación de red se realiza los días hábiles a las 21:00 h. Si el servidor de ubicación no estuviera disponible en ese momento (por ejemplo, debido a trabajos de mantenimiento), la creación se omite y se espera al siguiente día hábil para iniciar la tarea. Se supone que directamente no se debería iniciar la tarea de copia de seguridad, en lugar de que ocurra un error.

- Suceso: **Semanalmente**, Cada **1** semana en **<días hábiles>**; Una vez a las **21:00:00.**
- Condición: **El servidor de ubicación no está disponible**
- Condiciones de inicio de la tarea: **Omitir la ejecución de la tarea**.

Como resultado:

(1) Si son las 21:00 h y el servidor de la ubicación está disponible, la tarea de copia de seguridad se iniciará a tiempo.

(2) Si son las 21:00 h pero el servidor no está disponible en ese momento, la tarea de copia de seguridad se iniciará el siguiente día hábil si el servidor de la ubicación está disponible.

(3) Si es imposible que el servidor de la ubicación esté disponible en días laborables a las 21:00 h, la tarea nunca se iniciará.

5.4.2 Coincidir con intervalo

Se aplica a: Windows, Linux

Limita la hora de inicio de una tarea de copia de seguridad a un intervalo especificado.

Ejemplo

Una empresa usa distintas ubicaciones en el mismo dispositivo de almacenamiento conectado a la red para realizar copias de seguridad de servidores y datos de usuarios. El día hábil empieza a las 08:00 y termina a las 17:00. Las copias de seguridad de los datos de los usuarios deben realizarse en cuanto ellos cierren la sesión, pero no antes de las 16:30 ni después de las 22:00. Todos los días, se hacen copias de seguridad de los servidores de la empresa a las 23:00. Por lo tanto, es preferible que las copias de seguridad de los datos de los usuarios se realicen antes de dicho horario, para liberar ancho de banda de la red. Al especificar el límite superior a las 22:00, se supone que realizar copias de seguridad de los datos de los usuarios no debería llevar más de una hora. Si un usuario ha iniciado sesión durante del intervalo especificado, o si cierra la sesión en cualquier otro momento, no se realizan copias de seguridad de los datos de los usuarios, es decir, se omite la ejecución de la tarea.

- Suceso: **Al cerrar sesión**, el siguiente usuario: **Cualquier usuario**.
- Condición: **Coincidir con intervalo,** desde las **16:30:00** hasta las **22:00:00**.
- Condiciones de inicio de la tarea: **Omitir la ejecución de la tarea**.

Como resultado:

(1) si el usuario cierra la sesión entre las 16:30:00 y las 22:00:00, la tarea de copia de seguridad se iniciará inmediatamente después de dicho cierre de sesión.

(2) si el usuario cierra la sesión en algún otro horario, la tarea se omitirá.

Posibles situaciones

¿Qué sucede si se programa una tarea para ejecutarse en un horario en particular que está fuera del intervalo especificado?

Por ejemplo:

- Suceso: **Diariamente**, Cada **1** día(s); Una vez a las **15:00:00**.
- Condición: **Coincidir con intervalo**, desde las **18:00:00** hasta las **23:59:59**.

En este caso, el hecho de que se inicie la tarea y el horario en que lo hará depende de las condiciones de inicio de la tarea:

- Si las condiciones de inicio de la tarea son **Omitir la ejecución de tarea**, la tarea nunca se ejecutará.
- Si las condiciones de inicio de la tarea son **Esperar hasta que se cumplan las condiciones** y la casilla de verificación **Ejecutar la tarea de todos modos después de** está *desmarcada*, la tarea (programada para ejecutarse a las 15:00) se iniciará a las 18:00, la hora en la que se cumple la condición.
- Si las condiciones de inicio de la tarea son **Esperar hasta que se cumplan las condiciones** y la casilla de verificación **Ejecutar la tarea de todos modos después de** está *marcada* con, digamos, el tiempo de espera de **1 hora**, la tarea (programada para ejecutarse a las 15:00) se iniciará a las 16:00, la hora en la que se cumple la condición.

5.4.3 Tiempo transcurrido desde la última copia de seguridad

Se aplica a: Windows, Linux

Permite poner en espera la ejecución de una tarea de copia de seguridad hasta que transcurra el intervalo especificado desde la última finalización correcta de la copia de seguridad.

Ejemplo:

Ejecutar la tarea de copia de seguridad al iniciarse el sistema, pero sólo si han transcurrido más de 12 horas desde la última tarea de copia de seguridad con éxito.

- Suceso: **Al iniciar**, Comenzar la tarea al iniciarse el equipo.
- Condición: **Tiempo transcurrido desde la última copia de seguridad**, Tiempo que transcurrió desde la última copia de seguridad: **12** hora(s).
- Condiciones de inicio de la tarea: **Esperar hasta que se cumplan las condiciones**.

Como resultado:

(1) si el equipo se reinicia antes de que transcurran 12 horas desde la finalización de la última tarea de copia de seguridad con éxito, el programador esperará a que transcurran 12 horas y entonces iniciará la tarea.

(2) si el equipo se reinicia una vez transcurridas 12 horas desde la finalización de la última tarea de copia de seguridad con éxito, la tarea de copia de seguridad se iniciará inmediatamente.

(3) si el equipo no se reinicia nunca, la tarea nunca se iniciará. De ser necesario, puede iniciar la copia de seguridad manualmente desde la vista **Planes y tareas de copia de seguridad**.

6 Gestión directa

Esta sección cubre las operaciones que pueden realizarse directamente en un equipo gestionado al utilizar la conexión directa de consola-agente. El contenido de esta sección es aplicable a las ediciones avanzadas y autónomas de Acronis Backup & Recovery 10.

6.1 Administrar un equipo gestionado

Esta sección describe las vistas que están disponibles a través del árbol de navegación de la consola conectada a un equipo gestionado y explica cómo trabajar en cada vista.

6.1.1 Tablero

Utilice el Tablero para estimar rápidamente si los datos se han protegido con éxito en el equipo. El tablero muestra el resumen de las actividades de los agentes Acronis Backup & Recovery 10 y permite identificar y resolver rápidamente cualquier problema.

Alertas

La sección Alertas llama su atención sobre los problemas que han ocurrido en el equipo y le ofrece maneras para repararlos o examinarlos. Los problemas más críticos se muestran en la parte superior. Si no hay alertas o advertencias en ese momento, el sistema muestra "No hay alertas ni advertencias".

Tipos de alertas

La siguiente tabla muestra los tipos de mensajes que podría observar.

	Descripción	Solución	Comentario
	Tareas fallidas: X	Resolver	**Resolve**r abrirá la vista **Planes y tareas de copia de seguridad** con las tareas fallidas, donde puede examinar la causa del fallo.
	Tareas que necesitan interacción: X	Resolver	Cuando una tarea requiere interacción humana, el Tablero muestra un mensaje para informarle qué acción hay que llevar a cabo (por ejemplo, introducir un nuevo CD o Detener/Reintentar/Ignorar cuando ocurre un error).
	Falla al intentar comprobar la licencia desde la edición actual. Faltan X día(s) para que el software deje de funcionar. Asegúrese de que dispone de una licencia válida en el Servidor de Licencia Acronis .	Conectar	El agente Acronis Backup & Recovery 10 conecta al Servidor de Licencia Acronis al comienzo y luego cada 1–5 días (1 día predeterminado), como se ve especificado por los parámetros de configuración de agente. Si la comprobación de licencia no es exitosa durante 1–60 días, como lo especifican los parámetros de configuración del agente (predeterminada en 30 días), el agente dejará de funcionar hasta que se realice una última comprobación de licencia exitosa.

	No puede realizar la comprobación de la clave de la licencia para la edición actual de X días. O bien el Acronis License Server no estaba disponible o los datos de la clave de licencia estaban dañados. Compruebe la conectividad con el servidor y ejecute el Acronis License Server para gestionar las licencias. Asegúrese de que dispone de una licencia válida en el Servidor de Licencia Acronis .	Conectar	Acronis Backup & Recovery 10 detenido. Durante los últimos *X* días, el agente no pudo comprobar si su licencia estaba disponible en el Servidor de Licencias Acronis. Probablemente esto se debe a que el servidor de licencias no está disponible. También puede querer asegurarse que las licencias se encuentren en el servidor de licencia, o que los datos de la clave de la licencia no estén corruptos. Luego de comprobación exitosa de licencia, el agente comenzará a funcionar.
	La versión de prueba del producto caduca en *X* día(s) Asegúrese de que dispone de una licencia válida en el Servidor de Licencia Acronis .	Conectar	Cuando se instala la versión de prueba del producto, el programa inicia la cuenta atrás de los días que faltan para que el periodo de prueba caduque.
	El período de prueba ha finalizado. Inicie el instalador e ingrese la clave de licencia completa. Asegúrese de que dispone de una licencia válida en el Servidor de Licencia Acronis .	Conectar	El periodo de prueba de 15 días ha caducado. Introduzca una clave de licencia completa
	Bóvedas con poco espacio libre: X	Ver bóvedas	**La vista de bóvedas** lo conducirá a la vista **Bóvedas** donde podrá examinar el tamaño de bóveda, el espacio libre, el contenido y dar los pasos necesarios para incrementar el espacio libre.
	El dispositivo de inicio no se creó	Crear ahora	Para poder recuperar un sistema operativo cuando un equipo no se puede iniciar, debe: 1. Realizar una copia de seguridad del volumen del sistema (y del volumen de inicio, si es diferente). 2. Crear al menos un dispositivo de inicio (pág. 195). **Crear ahora** ejecutará el Generador de dispositivos de inicio (pág. 191).
	No se han creado copias de seguridad durante *X* días	Crear copia de seguridad ahora	El Tablero le advierte que no se ha realizado ninguna copia de seguridad de los datos en el equipo durante un periodo considerablemente largo de tiempo. **Realizar copia de seguridad ahora** lo llevará a la página **Crear un plan de copia de seguridad** donde puede configurar y ejecutar la operación de copia de seguridad instantáneamente. Para configurar el intervalo de tiempo que se considera crítico, seleccione **Opciones > Opciones de consola > Alertas según el momento**.
	No ha estado conectado al servidor de gestión durante X días	Ver los equipos	Este tipo de mensaje puede aparecer en un equipo que está registrado en un servidor de gestión. El Tablero le advierte que se puede haber perdido la

			conexión o que el servidor puede no estar disponible y por lo tanto el equipo no está siendo gestionado de forma centralizada.

Actividades

El calendario le permite explorar el historial de las actividades del agente Acronis Backup & Recovery 10 en el equipo. Haga clic con el botón derecho en la fecha resaltada y seleccione **Ver registro** para ver la lista de las entradas del registro filtradas por fecha.

En la sección **Ver** (a la derecha del calendario), puede seleccionar las actividades para resaltar dependiendo de la presencia y gravedad de los errores.

	Cómo se determina
Errores	Se resalta la fecha en rojo si se aparece al menos una entrada de "Error" en el registro en esta fecha.
Advertencias	Se resalta la fecha en amarillo si no aparece ninguna entrada de "Error" y se encuentra al menos una entrada de "Advertencia" en el registro en esta fecha.
Información	Se resalta la fecha en verde si sólo se encuentran entradas de "Información" en el registro en esta fecha (actividad normal).

El enlace **Seleccionar fecha actual** aplica la fecha actual a la selección.

Vista Sistema

Muestra estadísticas resumidas de los planes de copia de seguridad, tareas e información breve sobre la última copia de seguridad. Haga clic en los elementos de esta sección para obtener la información correspondiente. Esto te llevará a la vista **Planes y tareas de copia de seguridad** (pág. 98) con tareas o planes de seguridad prefiltrados. Por ejemplo, si se hace clic en **Local** en **Planes de copia de seguridad**, la vista **Planes y tareas de copia de seguridad** se abrirá con los planes de copia de seguridad filtrados por origen **Local**.

Tareas que necesitan interacción

Esta ventana acumula todas las tareas que necesitan la interacción del usuario en un sitio. Esto le permite especificar su decisión como, por ejemplo, confirmar el reinicio o volver a intentarlo después de liberar espacio del disco, en todas las tareas. Hasta que por lo menos una tarea necesite su interacción, puede abrir esta ventana en cualquier momento desde el **Tablero** (pág. 96) del equipo gestionado.

Si selecciona la casilla de verificación para el parámetro **No mostrar esta ventana cuando las tareas necesitan interacción. Veré esta información en los detalles de tareas y en el tablero.** Las tareas se mostrarán en el **Tablero** entre otras alertas y advertencias.

O bien, puede revisar el estado de ejecución de la tarea en la vista **Planes y tareas de copia de seguridad** (pág. 98) y especificar su decisión en cada tarea en el panel **Información** (o en la ventana **Detalles de tareas** (pág. 107)).

6.1.2 Planes y tareas de la copia de seguridad

La vista **Planes y tareas de la copia de seguridad** lo mantiene informado de la protección de datos en un equipo determinado. Le permite monitorizar y gestionar las tareas y los planes de copias de seguridad.

Un plan de copias de seguridad es una serie de reglas que especifica cómo se protegerán los datos en un equipo determinado. Físicamente, un plan de copias de seguridad es un paquete de tareas configuradas para la ejecución en un equipo gestionado. Para averiguar lo que está haciendo exactamente un plan de copias de seguridad en un equipo, active el estado de ejecución de un plan de copias de seguridad (pág. 99). Un estado de copia de seguridad es un estado acumulado de las tareas del plan. El estatus de un plan de copias de seguridad (pág. 100) le ayuda a estimar si los datos se encuentran correctamente protegidos.

Una tarea es una serie de acciones secuenciales que deben realizarse en un equipo cuando pasa cierto tiempo o cuando ocurre un determinado evento. Para tener un control del progreso actual de una tarea, examine su estado (pág. 101). Compruebe el estatus (pág. 102) de una tarea para determinar el resultado de una tarea.

Modo de trabajo

- Use filtros para mostrar los planes de copias de seguridad que desee (tareas) en la tabla de planes de copias de seguridad. De manera predeterminada, la tabla muestra los planes del equipo gestionado por orden alfabético. También puede ocultar las columnas innecesarias y mostrar las ocultas. Para obtener más detalles, consulte la sección Filtrar y ordenar los planes de copias de seguridad (pág. 106).
- En la tabla de copia de seguridad, seleccione el plan (tarea) de copia de seguridad.
- Utilice los botones de la barra de herramientas para llevar a cabo una acción en el plan (tarea) seleccionado. Para obtener más detalles, consulte la sección Acciones en planes y tareas de la copia de seguridad (pág. 103). Puede ejecutar, editar, detener y eliminar los planes y tareas creados.
- Para revisar información detallada sobre el plan (tarea) seleccionado, utilice el panel **Información**. De manera predeterminada, el panel se encuentra minimizado. Para expandir el panel, haga clic en la flecha tipo  . El contenido del panel también está duplicado en las ventanas **Detalles del plan** (pág. 109) y **Detalles de la tarea** (pág. 107) respectivamente.

Comprender los estados y estatus

Estados de ejecución de planes de copia de seguridad

Un plan de copias de seguridad puede encontrarse en uno de los siguientes estados: **Inactiva, esperando, ejecutando, deteniendo, necesita interacción**.

Los nombres de los estados del plan son los mismos que para las tareas ya que el estado de un plan es el estado acumulado de las tareas del plan.

	Estado	Cómo se determina	Cómo manejarlo
1	**Necesita interacción**	Al menos una tarea necesita la interacción del usuario. En caso contrario, consulte el punto 2.	Identifique las tareas que necesitan interacción (el programa mostrará la acción a realizar) -> Detenga las tareas o active su ejecución (cambiar dispositivo, proporcionar espacio adicional a la bóveda, ignorar los errores de lectura, crear la Acronis Secure Zone no encontrada).
2	**Ejecución de**	Al menos una tarea se está ejecutando. En caso contrario, vea el punto 3.	No se necesita tomar ninguna medida.

3	**Esperando**	Al menos una tarea se encuentra en espera. De lo contrario, consulte el punto 4.	Esperando las condiciones. Esta situación es bastante normal, pero retrasar una copia de seguridad durante mucho tiempo es peligroso. La solución sería ajustar el plazo máximo o forzar la situación (pedir al usuario que cierre la sesión, permitir la conexión a la red que se necesita). Esperar mientras otra tarea consume los recursos necesarios. Un caso extraordinario de espera puede ocurrir cuando, por alguna razón en particular, el comienzo de una tarea dura mucho más de lo normal, y esto evita que comience otra diferente. La situación se resuelve automáticamente cuando la tarea que está obstruyendo el proceso finaliza. Contemple la posibilidad de interrumpir una tarea si tarda demasiado tiempo y evita que comience la tarea siguiente. Un solapamiento continuo de las tareas podría derivar de uno o varios planes programados de manera incorrecta. En este caso, lo lógico es editar el plan.
4	**Deteniendo**	Al menos una tarea está deteniéndose. De lo contrario, consulte el punto 5.	No se necesita tomar ninguna medida.
5	**Inactiva**	Todas las tareas se encuentran inactivas.	No se necesita tomar ninguna medida.

Estatus del plan de copias de seguridad

Un plan de copias de seguridad puede tener uno de los siguientes estatus: **Error; Advertencia; OK**.

El estatus de un plan de copias de seguridad deriva de los resultados de la última ejecución de las tareas de los planes.

	Estado	Cómo se determina	Cómo manejarlo
1	**Error**	Por lo menos una de las tareas ha fallado. De lo contrario, consulte el punto 2.	Identifique las tareas falladas -> Compruebe el registro de tareas para encontrar la causa del fallo y después lleve a cabo una o más de las siguientes tareas: ▪ Elimine la causa del fallo -> [opcionalmente] Inicie la tarea fallida manualmente ▪ Modifique el plan local para prevenir su futuro fallo en caso de que un plan local haya fallado ▪ Modifique la política de copias de seguridad en el servidor de gestión en caso de que un plan centralizado haya fallado Cuando se crea un plan o un política de copias de seguridad, el administrador puede activar la opción para detener la ejecución del plan de copias de seguridad en el momento que se detecta el estatus de Error. Se puede reanudar la ejecución del plan de copias de seguridad utilizando el botón Reiniciar.
2	**Advertencia**	Por lo menos una tarea se ha completado correctamente con advertencias. En caso contrario, vea el	Consulte el registro para leer las advertencias -> [opcionalmente] Realice las acciones para prevenir las advertencias o fallos futuros.

		punto 3.	
3	**OK**	Todas las tareas se han completado correctamente.	No se necesita tomar ninguna medida. Tenga en cuenta que un plan de copias de seguridad puede estar OK si aún no se ha iniciado ninguna de las tareas o si alguna de las tareas se detienen o se está deteniendo. Estas situaciones se consideran normales.

Estados de las tareas

Una tarea puede encontrarse en uno de los siguientes estados: **Inactiva**, **esperando**, **ejecutando**, **deteniendo**, **necesita interacción**. El estado inicial de una tarea es **Inactiva**.

Una vez que la tarea ha comenzado manualmente o que tiene lugar el evento especificado en la programación, la tarea pasa al estado **Ejecutando** o al estado **Esperando**.

Ejecución

Una tarea cambia al estado **Ejecutando** cuando tiene lugar el evento especificado en la programación Y se cumplen todas las condiciones configuradas en el plan de copias de seguridad Y no se está ejecutando ninguna otra tarea que consuma los recursos necesarios. En este caso, nada impide que la tarea se ejecute.

Esperando

Una tarea cambia al estado **Esperando** cuando la tarea está preparada para comenzar pero otra tarea que utiliza los mismos recursos continúa ejecutándose. Particularmente, no es posible ejecutar en un equipo más de una tarea de copia de seguridad o más de una tarea de recuperación al mismo tiempo. Una tarea de copia de seguridad y una de recuperación tampoco pueden ejecutarse de manera simultánea. Una vez que la tarea deja de consumir el recurso, la tarea en espera pasa al estado **Ejecutando**.

Una tarea también puede cambiar al estado **Esperando** cuando se lleva a cabo el evento especificado en la programación pero no se cumple una condición configurada en el plan de copias de seguridad. Para obtener más información, consulte Condiciones de inicio de la tarea (pág. 64).

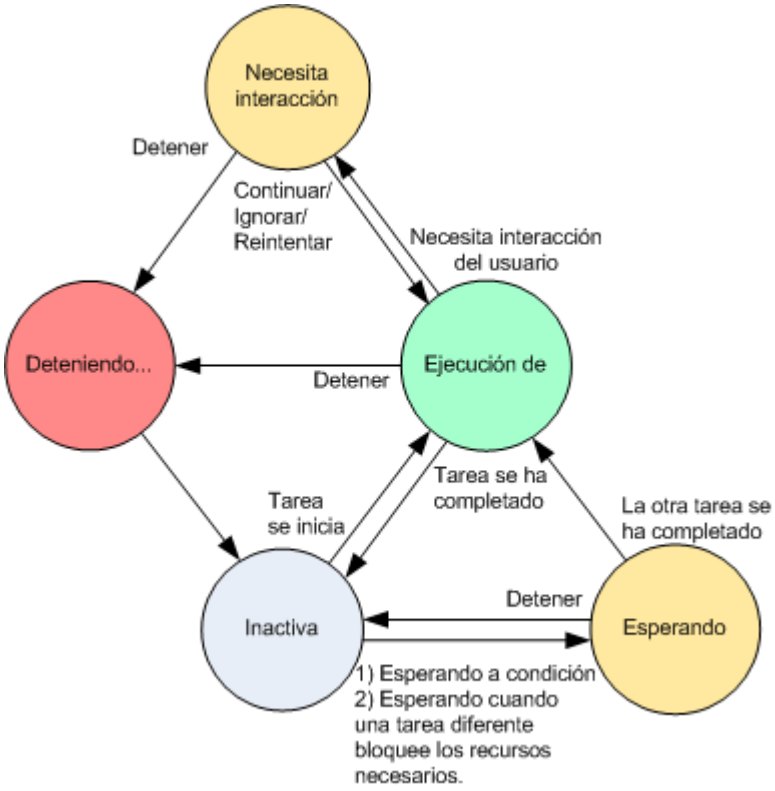
Necesita interacción

Cualquier tarea que esté ejecutándose puede pasar al estado **Necesita interacción** si necesita la interacción del usuario para, por ejemplo, cambiar un dispositivo o ignorar un error de lectura. El siguiente estado sería el de **Deteniendo** (si el usuario elige detener la tarea) o **Ejecutándose** (al seleccionar Ignorar/Reintentar u otra acción, tal como Reiniciar, que vuelva a cambiar la tarea al estado de **Ejecutando**).

Deteniendo

El usuario puede detener una tarea que se está ejecutando o una tarea que necesita interacción. Una tarea pasa del estado **Deteniendo** al estado **Inactiva**. También puede detenerse una tarea en espera. En este caso, ya que la tarea no está ejecutándose, "detener" significa eliminarla de la cola.

Diagrama de estado de las tareas



Estatus de las tareas

Una tarea puede tener uno de los siguientes estatus: **Error**; **Advertencia**; **OK**.

El estatus de una tarea deriva del resultado de la última ejecución de la tarea.

	Estado	Cómo se determina	Cómo afrontarlo
1	**Error**	El último resultado es "Fallido"	Identifique la tarea fallada -> Compruebe el registro de tareas para encontrar la causa del fallo, después lleve a cabo una o más de las siguientes tareas: ▪ Elimine la causa del fallo -> [opcionalmente] Inicie la tarea fallida manualmente ▪ Modifique la tarea fallida para prevenir su futuro fallo ▪ Modifique el plan local para prevenir su futuro fallo en caso de que un plan local haya fallado ▪ Modifique la política de copias de seguridad en el servidor de gestión en caso de que un plan centralizado haya fallado
2	**Advertencia**	El último resultado es "Completado correctamente con advertencias"	Vea el registro para leer las advertencias -> [opcionalmente] Realice las acciones para prevenir las advertencias o fallos futuros.
3	**OK**	El último resultado es "Completado correctamente", "-	No es necesario tomar ninguna medida. El estado "-" significa que la tarea nunca se ha iniciado o

		", o "Detenido"	se ha iniciado, pero aún no se ha completado y, por lo tanto, su resultado no está disponible.

Trabajar con los planes y las tareas de copia de seguridad

Acciones en los planes y tareas de copia de seguridad

A continuación se ofrece una guía para la realización de operaciones con planes y tareas de copia de seguridad.

Operación	Procedimiento
Cree un plan de copia de seguridad nuevo o una tarea	Haga clic en **Nuevo** y luego seleccione una de las siguientes opciones: ▪ Plan de copia de seguridad (pág. 113) ▪ Tarea de recuperación ▪ Tarea de validación (pág. 152)
Ver los detalles de un plan o una tarea	**Plan de copia de seguridad** Haga clic en **Ver detalles**. En la ventana de **Detalles del plan** (pág. 109), revise los detalles del plan. **Tarea** Haga clic en **Ver detalles**. En la ventana de **Detalles de la tarea** (pág. 107), revise los detalles de la tarea.
Ver el registro del plan o de la tarea	**Plan de copia de seguridad** Haga clic en **Ver registro**. Accederá a la sección de **Registro** (pág. 110), la cual incluye la lista de las entradas de registro relacionadas con el plan. **Tarea** Haga clic en **Ver registro**. Accederá a la sección de **Registro** (pág. 110), la cual incluye la lista de las entradas de registro relacionadas con la tarea.
Ejecutar un plan o una tarea	**Plan de copia de seguridad** Haga clic en **Ejecutar**. En la ventana **Ejecutar plan de copia de seguridad** (pág. 107), seleccione la tarea que necesita que se ejecute. La ejecución del plan de copia de seguridad inicia inmediatamente la tarea seleccionada de dicho plan, independientemente de la programación y de las condiciones. *¿Por qué no puedo ejecutar el plan de copia de seguridad?* ▪ No tiene el privilegio adecuado Un usuario no puede ejecutar planes de otros usuarios sin poseer los privilegios de Administrador. **Tarea** Haga clic en **Ejecutar**. La tarea se ejecutará inmediatamente, independientemente de la programación y de las condiciones.

Detener un plan o una tarea	**Plan de copia de seguridad** Haga clic en **Detener**. Al detener el plan de copia de seguridad en ejecución se detendrán todas las tareas. Por lo tanto, se cancelarán todas las operaciones de tareas. **Tarea** Haga clic en **Detener**. *¿Qué sucede si detengo la tarea?* Por lo general, al detener la tarea se cancela su operación (copia de seguridad, recuperación, validación, exportación, conversión, migración). La tarea pasa en primer lugar al estado Deteniendo y después al estado Inactiva. La programación de la tarea, en caso de haberla creado, aún será válida. Para completar la operación, tendrá que ejecutar la tarea de nuevo. ▪ Tarea de recuperación (desde la copia de seguridad del disco): El volumen de destino se eliminará y el espacio quedará no asignado. También obtendrá el mismo resultado si la recuperación no se realiza correctamente. Para recuperar el volumen "perdido", deberá ejecutar la tarea una vez más. ▪ tarea de recuperación (desde la copia de seguridad de archivos): La operación cancelada puede ocasionar cambios en la carpeta de destino. Algunos archivos se podrían recuperar pero otros no, dependiendo del momento en el que se haya detenido la tarea. Para recuperar todos los archivos deberá ejecutar la tarea una vez más.

Editar un plan o una tarea	**Plan de copia de seguridad** Haga clic en **Editar**. La edición del plan de copia de seguridad se realiza de la misma manera que la creación (pág. 113), excepto por las siguientes **limitaciones**: No siempre es posible utilizar todas las opciones de esquema cuando se edita un plan de copia de seguridad si el archivo comprimido creado no está vacío (es decir, contiene copias de seguridad). 1. No es posible cambiar el esquema a "abuelo-padre-hijo" o Torres de Hanói. 2. Si se utiliza el esquema de la Torres de Hanói, no es posible cambiar la cantidad de niveles. En los demás casos, se puede cambiar el esquema, y debería continuar funcionando como si los archivos comprimidos existentes se hubieran creado bajo el nuevo esquema. En los archivos comprimidos vacíos es posible realizar cualquier tipo de cambio. *¿Por qué no puedo editar el plan de copia de seguridad?* ▪ El plan de copia de seguridad se encuentra en ejecución en ese momento. La edición del plan de copia de seguridad actualmente en ejecución no está permitida. ▪ No tiene el privilegio adecuado Un usuario no puede editar planes de otros usuarios sin poseer los privilegios de Administrador. ▪ El plan de copia de seguridad posee un origen centralizado. La edición directa de los planes de copia de seguridad centralizados no está permitida. Debe editar la política de copia de seguridad original. **Tarea** Haga clic en **Editar**. *¿Por qué no puedo editar la tarea?* ▪ La tarea pertenece a un plan de copia de seguridad. Solo las tareas que no pertenecen a un plan de copia de seguridad, tales como las tareas de recuperación, pueden modificarse mediante edición directa. Cuando deba modificar una tarea que pertenece a un plan de copia de seguridad local, edite el plan de copia de seguridad. Las tareas que pertenecen a un plan de copia de seguridad centralizado se pueden modificar al editar la política centralizada que generó el plan. Esto sólo lo puede hacer el administrador del servidor de gestión. ▪ No tiene el privilegio adecuado Un usuario no puede modificar tareas de otros usuarios sin poseer los privilegios de Administrador.

Eliminar un plan o una tarea	**Plan de copia de seguridad** Haga clic en **Eliminar**. *¿Qué sucede si elimino el plan de copia de seguridad?* Si se elimina el plan, se eliminarán todas sus tareas. *¿Por qué no puedo eliminar el plan de copia de seguridad?* ▪ El plan de copia de seguridad se encuentra en el estado "En ejecución" El plan de copia de seguridad no podrá eliminarse si al menos una de sus tareas se encuentra en ejecución. ▪ No tiene el privilegio adecuado Un usuario no puede eliminar planes de otros usuarios sin poseer los privilegios de Administrador. ▪ El plan de copia de seguridad posee un origen centralizado. El administrador del servidor de gestión puede eliminar un plan centralizado al revocar la política de copia de seguridad que dio origen al plan. **Tarea** Haga clic en **Eliminar**. *¿Por qué no puedo eliminar la tarea?* ▪ La tarea pertenece a un plan de copia de seguridad. La tarea que pertenece a un plan de copia de seguridad no puede eliminarse por separado del plan. Edite el plan para quitar la tarea o elimine el plan completo. ▪ No tiene el privilegio adecuado Un usuario no puede eliminar tareas de otros usuarios sin poseer los privilegios de Administrador.
Actualizar la tabla	Haga clic en **Actualizar**. La consola de gestión actualizará la lista de los planes y las tareas de copia de seguridad presentes en el equipo con la información más reciente. Si bien la lista se actualiza automáticamente en función de los eventos, es posible que los datos no se recuperen inmediatamente del equipo gestionado debido a un breve periodo de latencia. La actualización manual garantiza la visualización de los datos más recientes.

Filtrar y ordenar planes y tareas de copia de seguridad

Para	Realizar
Ordenar planes y tareas de copia de seguridad por: nombre, estado, estatus, tipo, origen, etc.	Haga clic en el encabezado de la columna para ordenar los planes y las tareas de copia de seguridad por orden ascendente. Haga clic de nuevo para ordenar los planes y las tareas de copia de seguridad por orden descendente.
Filtrar planes o tareas por nombre o propietario.	Escriba el nombre del plan o la tarea de copia de seguridad o el nombre del propietario en el campo situado debajo del encabezado de la columna respectiva. Como consecuencia, verá la lista de las tareas cuyos nombres o nombres de propietario coinciden total o parcialmente con el valor introducido.

Filtrar planes y tareas por estado, estatus, tipo, origen, último resultado, programación.	En el campo situado debajo del encabezado de la columna respectiva, seleccione el valor que desee de la lista.

Configurar los planes de copias de seguridad y la tabla de tareas

De manera predeterminada, la tabla que se muestra se compone de seis columnas, las demás se encuentran ocultas. También puede ocultar las columnas innecesarias y mostrar las ocultas.

Mostrar u ocultar columnas

1. Haga clic con el botón derecho en el encabezado de cualquier columna para abrir el menú contextual. Los elementos del menú que no estén seleccionados corresponden a los encabezados de las columnas presentadas en la tabla.
2. Haga clic sobre los elementos que quiera mostrar/ocultar.

Ejecutar el plan de copias de seguridad

Se considera que el plan de copias de seguridad se está ejecutando si por lo menos una de sus tareas se está ejecutando. La ventana **Ejecutar plan de copias de seguridad** le permite ejecutar la tarea del plan de copias de seguridad seleccionada manualmente, independientemente de su programación.

Para ejecutar una tarea del plan de copias de seguridad seleccionado

1. Seleccione la tarea del plan de copias de seguridad que necesita ejecutar. Para asegurarse de que su selección es la correcta, compruebe la información de la tarea contenida en las pestañas de la parte inferior de la ventana. Esta información también se duplica en la ventana **Detalles de tareas** (pág. 107).
2. Haga clic en **Aceptar**.

Deshabilitar temporalmente un plan de copias de seguridad.

Es necesario deshabilitar temporalmente un plan de copias de seguridad cuando se mueven archivos comprimidos de una bóveda a otra por medio de un administrador de archivos de terceros.

Únicamente se aplica a los planes de copias de seguridad que usan esquemas de copia de seguridad personalizados.

Deshabilitar un plan de copias de seguridad.

1. Haga clic en **Editar**.
2. Entre en la opción de programación del esquema de copias de seguridad y deshabilite la programación para el periodo deseado al cambiar los parámetros de **Fecha de inicio** o **Fecha de finalización**.

Detalles de la tarea

La ventana **Detalles de la tarea** (también aparece en el panel **Información**) incluye toda la información sobre la tarea seleccionada.

Cuando una tarea requiere la interacción del usuario, aparecerá un mensaje y botones de acción sobre las pestañas. El mensaje contiene una breve descripción del problema. Los botones le permiten reintentar o detener la tarea o el plan de copia de seguridad.

Tipos de tareas

La siguiente tabla resume todos los tipos de tareas que existen en Acronis Backup & Recovery 10. Los tipos de tareas a los que pueda acceder dependerán de la edición del producto y del componente del producto al que está conectada la consola.

Nombre de la tarea	Descripción
Copia de seguridad (disco)	Copias de seguridad de discos y volúmenes
Copia de seguridad (archivo)	Copias de seguridad de archivos y carpetas
Copia de seguridad (máquina virtual)	Copias de seguridad de una máquina virtual completa o sus volúmenes
Recuperación (disco)	Recuperación de la copia de seguridad del disco
Recuperación (archivo)	Recuperación de archivos y carpetas
Recuperación (volumen)	Recuperación de volúmenes de una copia de seguridad del disco
Recuperación (MBR)	Recuperación del registro de inicio maestro
Recuperación (disco a VM existente)	Recuperación de una copia de seguridad del disco o volumen en una máquina virtual existente
Recuperación (disco a nueva VM)	Recuperación de una copia de seguridad del disco o volumen en una máquina virtual nueva
Recuperación (máquina virtual existente)	Recuperación de una copia de seguridad de una máquina virtual en una máquina virtual existente
Recuperación (máquina virtual nueva)	Recuperación de una copia de seguridad de una máquina virtual en una máquina virtual nueva
Validación (archivo comprimido)	Validación de un único archivo comprimido
Validación (copia de seguridad)	Validación de copias de seguridad
Validación (bóveda)	Validación de todos los archivos comprimidos almacenados en una bóveda
Limpieza	Eliminación de las copias de seguridad de un archivo de copia de seguridad de acuerdo con las reglas de retención
Creación de ASZ	Creación de Acronis Secure Zone
Gestión de ASZ	Modificación del tamaño, cambio de la contraseña, eliminación de Acronis Secure Zone
Gestión del disco	Operaciones de gestión del disco
Compactando	Tarea de servicio realizada en un nodo de almacenamiento
Indexando	La tarea de deduplicación realizada por el nodo de almacenamiento en la bóveda se completa luego de realizada la copia de seguridad

Según el tipo de tarea y si se está ejecutando o no, aparecerá una combinación de las siguientes pestañas:

Tarea

La pestaña **Tarea** es igual para todos los tipos de tareas. Proporciona información general sobre la tarea seleccionada.

Archivo comprimido

La pestaña **Archivo comprimido** está disponible para las tareas de copia de seguridad, de validación del archivo comprimido y de limpieza.

Proporciona información sobre el archivo comprimido: nombre, tipo, tamaño, ubicación de almacenamiento, etc.

Crear copia de seguridad

La pestaña **Copia de seguridad** está disponible para las tareas de recuperación, de validación de la copia de seguridad y de exportación.

Proporciona detalles sobre la copia de seguridad seleccionada: cuándo se creó, su tipo (completa, incremental, diferencial), información sobre el archivo comprimido y la bóveda en la que se encuentra la copia de seguridad.

Configuraciones

La pestaña **Configuración** muestra información sobre la programación y las opciones cambiadas en comparación con los valores predeterminados.

Progreso

La pestaña **Progreso** está disponible mientras se está ejecutando la tarea. Es igual para todos los tipos de tareas. Esta pestaña proporciona información sobre el progreso de la tarea, el tiempo transcurrido y otros parámetros.

Detalles del plan de copias de seguridad

La ventana de **Detalles del plan de copias de seguridad** (también duplicada en el panel **Información**) reúne en cuatro pestañas toda la información del plan de copias de seguridad seleccionado.

El mensaje respectivo aparecerá en la parte superior de las pestañas si una de las tareas del plan necesita la interacción del usuario. Contiene una descripción breve del problema y de los botones de acción que le permiten seleccionar la acción adecuada o detener el plan.

Plan de copias de seguridad

La pestaña del **plan de copias de seguridad** proporciona la siguiente información general sobre el plan seleccionado:

- **Nombre**, nombre del plan de copias de seguridad
- **Origen**, si el plan se ha creado en el equipo gestionado utilizando la gestión directa (origen local) o si ha aparecido en el equipo como resultado de la implementación de una política de copias de seguridad desde el servidor de gestión (origen centralizado).
- **Política** (para planes de copias de seguridad con origen centralizado), nombre de la política de plan de copias de seguridad, cuya implementación ha creado el plan de copias de seguridad.
- **Cuenta,** el nombre de la cuenta con la que se ejecuta el plan
- **Propietario**, el nombre del usuario que ha creado o modificado el plan la última vez
- **Estado**, estado de ejecución (pág. 99) del plan de copias de seguridad.
- **Estatus**, estatus (pág. 100) del plan de copias de seguridad.
- **Programación**, si la tarea es programada o se ha configurado para iniciarse manualmente.
- **Última copia de seguridad**, cuánto tiempo ha pasado desde la última copia de seguridad.
- **Creación**, fecha de creación del plan copia de seguridad.

- **Comentarios**, descripción del plan (si está disponible).

Origen

La pestaña **Origen** brinda la siguiente información sobre los datos seleccionados para la copia de seguridad:

- **Tipo de origen**, el tipo de datos (pág. 116) seleccionados para la copia de seguridad.
- **Elementos a incluir en la copia de seguridad**, elementos seleccionados para incluir en la copia de seguridad y su tamaño.

Destino

La pestaña **Destino** brinda la siguiente información:

- **Ubicación**, nombre de la bóveda o ruta que lleva hasta la carpeta en la que está almacenado el archivo comprimido.
- **Nombre del archivo comprimido**, nombre del archivo comprimido.
- **Comentarios del archivo comprimido**, comentarios sobre el archivo comprimido (si están disponibles).

Ajustes

La pestaña **Ajustes** muestra la siguiente información:

- **Esquema de copia de seguridad**, el esquema de copia de seguridad seleccionado y todos sus ajustes y programaciones.
- **Validación** (si está seleccionado), eventos que se han llevado a cabo antes o después de la validación y de la programación de la validación.
- **Opciones de copia de seguridad**, opciones de copia de seguridad que se han modificado sin respetar los valores predeterminados.

6.1.3 Registro

El Registro almacena el historial de las operaciones realizadas por Acronis Backup & Recovery 10 o las acciones llevadas a cabo por el usuario en el equipo utilizando el programa. Por ejemplo, cuando un usuario edita una tarea, se añade la entrada respectiva al registro. Cuando el programa ejecuta una tarea, añade numerosas entradas. Con el registro, se pueden examinar las operaciones y los resultados de la ejecución de las tareas, incluyendo los motivos de cualquier fallo, en caso de producirse.

Modo de trabajo con las entradas del registro

- Utilice los filtros para mostrar las entradas del registro que desee ver. También puede ocultar las columnas innecesarias y mostrar las ocultas. Para obtener más detalles, consulte la sección Filtrar y ordenar las entradas del registro (pág. 112).
- En la tabla del registro, seleccione la(s) entrada(s) del registro sobre la(s) que quiere llevar a cabo una acción. Para obtener más detalles, consulte la sección Acciones sobre las entradas del registro (pág. 111).
- Para revisar información detallada sobre la entrada del registro seleccionada, utilice el panel **Información**. De manera predeterminada, el panel se encuentra minimizado. Para expandir el panel, haga clic en la flecha tipo  . El contenido del panel también está duplicado en la ventana **Detalles de entrada del registro** (pág. 112).

Abrir el Registro con las entradas prefiltradas del registro

Si ha seleccionado elementos en otras vistas de administración (**Tablero**, **Planes y tareas de copia de seguridad**), puede abrir la vista del **Registro** con entradas de registro prefiltradas para el elemento en cuestión. Así, no será necesario que configure los filtros en la tabla de registro.

Vista	Acción
Tablero	En el calendario, haga clic con el botón derecho en cualquiera de las fechas resaltadas y después seleccione **Ver registro**. La vista **Registro** aparece con la lista de entradas del registro que ya se han filtrado por la fecha en cuestión.
Planes y tareas de la copia de seguridad	Seleccione un plan de copias de seguridad o una tarea y después haga clic en **Ver registro**. La vista Registro mostrará una lista de las entradas del registro relacionadas con el plan o tarea seleccionados.

Acciones en las entradas del registro

Todas las operaciones descritas a continuación se llevan a cabo haciendo clic en los elementos correspondientes en la **barra de herramientas** del registro. Todas estas operaciones se pueden llevar a cabo con el menú contextual (haciendo clic con el botón derecho en la entrada del registro), o con la barra **acciones del registro** (en el panel **Acciones y herramientas**).

A continuación se muestra una guía para llevar a cabo acciones en las entradas del registro.

Operación	Procedimiento
Seleccionar una entrada del registro	Haga clic en ella.
Seleccionar varias entradas del registro	▪ *no contiguas*: mantenga pulsada la tecla **CTRL** y haga clic en las entradas una a una ▪ *contiguas*: seleccione una entrada, mantenga pulsada la tecla **MAYÚSCULAS** y haga clic en otra entrada. Así se seleccionarán todas las entradas entre la primera y la última selección.
Ver información sobre las entradas del registro	1. Seleccione una entrada del registro 2. Realice uno de los siguientes procedimientos: ▪ Haga clic en **Ver detalles**. Los detalles de las entradas del registro se mostrarán en una ventana diferente. ▪ Expanda el Panel de información haciendo clic en la flecha tipo.
Guardar las entradas del registro seleccionadas en un archivo comprimido.	1. Seleccione una o varias entradas del registro. 2. Haga clic en **Guardar la selección en archivo**. 3. En la ventana abierta, especifique la ruta y un nombre para el archivo.
Guardar todas las entradas del registro a un archivo.	1. Asegúrese de que no se han configurado filtros. 2. Haga clic en **Guardar todo en archivo**. 3. En la ventana abierta, especifique la ruta y un nombre para el archivo.
Guardar todas las entradas filtradas del registro en un archivo comprimido.	1. Configure los filtros para obtener una lista de las entradas del registro que satisfagan los criterios. 2. Haga clic en **Guardar todo en archivo**. 3. En la ventana abierta, especifique la ruta y un nombre para el archivo.

	Como consecuencia, se guardarán las entradas del registro de la lista.
Eliminar todas las entradas del registro.	Haga clic en **Limpiar registro**. Todas las entradas del registro se eliminarán del mismo y se creará una nueva entrada. Esta contendrá información relacionada con quién eliminó las entradas y cuándo.

Filtrado y clasificación de entradas del registro

A continuación se muestra una guía para filtrar y ordenar las entradas del registro.

Operación	Procedimiento
Mostrar las entradas del registro para un periodo de tiempo determinado	1. En el campo **De**, seleccione la fecha a partir de la cual se mostrarán las entradas del registro. 2. En el campo **A**, seleccione la fecha hasta la cual se mostrarán las entradas del registro.
Filtrar las entradas del registro por tipo	Active o desactive los siguientes botones de la barra de herramientas: para filtrar mensajes de error para filtrar mensajes de advertencia para filtrar mensajes de información
Filtrar entradas del registro por tipo de plan de copia de seguridad original o entidad gestionada.	En el encabezado de la columna **Plan de copia de seguridad** (o **Tipo de entidad gestionada**), seleccione el plan de copia de seguridad o el tipo de entidad gestionada de la lista.
Filtrar entradas del registro por tarea, entidad gestionada, equipo, código o propietario.	Escriba el valor requerido (nombre de la tarea, del equipo, del propietario, etc.) en el campo situado debajo del encabezado de la columna respectiva. Como consecuencia, verá la lista de las entradas del registro que coinciden total o parcialmente con el valor introducido.
Ordenar las entradas del glosario por fecha y hora	Haga clic en el encabezado de la columna para ordenar las entradas del registro por orden ascendente. Haga clic de nuevo para ordenar las entradas del registro por orden descendente.

Configurar la tabla del registro

De manera predeterminada, la tabla muestra siete columnas, las otras están ocultas. Si fuera necesario, puede ocultar las columnas visibles y mostrar las ocultas.

Mostrar u ocultar columnas

1. Haga clic con el botón derecho en el encabezado de cualquier columna para abrir el menú contextual. Los elementos del menú que no estén seleccionados corresponden a los encabezados de las columnas presentadas en la tabla.
2. Haga clic sobre los elementos que quiera mostrar/ocultar.

Detalles de la entrada del registro

Muestra información detallada de la entrada del registro seleccionada y permite copiarla al portapapeles.

Para copiar los detalles, haga clic en el botón **Copiar al portapapeles**.

Campos de datos de entrada del registro.

Una entrada del registro local contiene los siguientes campos de datos:

- **Tipo**: tipo de evento (Error; Advertencia; Información)
- **Fecha**: fecha y hora en la que ocurre el evento
- **Plan de copias de seguridad**: el plan de copias de seguridad con el que se relaciona el evento (si hubiera)
- **Tarea**: tarea con la que se relaciona el evento (si hubiera)
- **Código**: el código de programa del evento. Cada tipo de evento del programa tiene su propio código. El código se compone de un número entero que puede utilizar el servicio de asistencia de Acronis para solucionar el problema.
- **Módulo**: número del módulo del programa en el que tuvo lugar el evento. Se trata de un número entero que puede utilizar el servicio de asistencia de Acronis para solucionar el problema.
- **Propietario**: nombre de usuario del propietario del plan de copias de seguridad (solo para el sistema operativo)
- **Mensaje**: una descripción textual del evento.

La información de la entrada del registro que se copiará tendrá el siguiente aspecto:

```
--------------------------Detalles de entrada del registro--------------------
-------
Tipo:                           Información
Fecha y hora:                   DD.MM.AAAA HH:MM:SS
Plan de copias de seguridad:    Nombre del plan de copias de seguridad
Tarea:                          Nombre de la tarea
Mensaje:                        Descripción de la operación
Código:                         12(3x45678A)
Módulo:                         Nombre del módulo
Propietario:                    Propietario del plan
------------------------------------------------------------------------
```

La presentación de la fecha y la hora depende de su ajuste local.

6.2 Crear un plan de copias de seguridad

Antes de crear su primer plan de copia de seguridad (pág. 196), familiarícese con los conceptos básicos (pág. 17) utilizados en Acronis Backup & Recovery 10.

Para crear un plan de copias de seguridad, siga los siguientes pasos.

General

Nombre del plan

[Opcional] Introduzca un solo nombre para el plan de copias de seguridad. Un nombre lógico le permitirá identificar este plan de entre otros.

Credenciales del plan (pág. 115)

[Opcional] El plan de copias de seguridad se ejecutará en nombre del usuario que haya creado el plan. Si es necesario, es posible cambiar las credenciales de las cuentas del plan. Para acceder a esta opción, seleccione la casilla de verificación **Vista avanzada**.

Comentarios

[Opcional] Escriba una descripción del plan de copias de seguridad. Para acceder a esta opción, marque la casilla de verificación **Vista avanzada**.

Etiqueta

[Opcional] Marque una etiqueta de texto para el equipo al que va a realizar la copia de seguridad. La etiqueta puede usarse para identificar el equipo en diversos escenarios. Para acceder a esta opción, marque la casilla de verificación **Vista avanzada**.

Qué incluir en la copia de seguridad

Tipo de fuente (pág. 116)

Seleccione el tipo de datos para incluir en la copia de seguridad. El tipo de datos depende de los agentes instalados en el equipo.

Elementos para incluir en la copia de seguridad (pág. 116)

Especifique los elementos de datos que incluirá en la copia de seguridad. La lista de elementos para incluir en la copia de seguridad depende del tipo de datos especificados con anterioridad.

Credenciales de acceso (pág. 118)

[Opcional] Proporcione credenciales para los datos de origen si las cuentas del plan no tienen permisos de acceso a los datos. Para acceder a esta opción, seleccione la casilla de verificación **Vista avanzada**.

Exclusiones (pág. 118)

[Opcional] Establezca exclusiones para los tipos de archivos específicos de los cuales no desea realizar una copia de seguridad. Para acceder a esta opción, marque la casilla de verificación **Vista avanzada**.

Dónde realizar copias de seguridad

Archivo comprimido (pág. 120)

Especifique la ruta en la que los archivos comprimidos de la copia de seguridad se almacenarán, así como el nombre del archivo comprimido. Se recomienda que el nombre del archivo comprimido sea único dentro de la ubicación. El nombre de archivo comprimido predeterminado es Archivo(N), donde N es el número de secuencia del archivo comprimido en la ubicación que se ha seleccionado.

Nombre los archivos de copia de seguridad utilizando el nombre del archivo comprimido tal como Acronis True Image Echo, en vez de utilizar nombres generados automáticamente

No disponible al hacer copias de seguridad en una cinta o en Acronis Secure Zone.

[Opcional] Seleccione esta casilla de verificación si desea utilizar nombres de archivos comprimidos simplificados para los archivos comprimidos de la copia de seguridad.

Credenciales de acceso (pág. 126)

[Opcional] Proporcione credenciales para la ubicación si la cuenta del plan no tiene permisos de acceso a la ubicación. Para acceder a esta opción, marque la casilla de verificación **Vista avanzada**.

Comentarios de archivo comprimido

[Opcional] Introduzca comentarios en el archivo comprimido. Para acceder a esta opción, marque la casilla de verificación **Vista avanzada**.

¿Cómo crear copias de seguridad?

Esquema de copias de seguridad (pág. 127)

Especifique dónde y con qué frecuencia realizar copias de seguridad de sus datos, establezca durante cuánto tiempo mantener los archivos comprimidos de la copia de seguridad en la ubicación seleccionada y configure una programación para el procedimiento de limpieza del archivo comprimido. Utilice esquemas de copia de seguridad optimizados y reconocidos

como Abuelo-Padre-Hijo (GFS) o Torres de Hanói y cree un esquema de copia de seguridad personalizado, o realice copias de seguridad solo una vez.

Validación de archivos comprimidos

Cuándo validar (pág. 138)

[Opcional] Defina cuándo y cada cuánto tiempo realizará la validación y si se desea validar todo el archivo comprimido o la última copia de seguridad del archivo.

Opciones de la copia de seguridad

Configuraciones

[Opcional] Configure los parámetros de la operación de copia de seguridad, como los comandos pre/post copia de seguridad, el ancho de banda de red máximo asignado para el flujo de copia de seguridad o el nivel de compresión del archivo de copia de seguridad. Si no hace nada en esta sección, se usarán los valores predeterminados (pág. 48).

Después de que se modifique cualquiera de las configuraciones con respecto al valor predeterminado, aparecerá una nueva línea que mostrará el valor recientemente establecido. El estado de la configuración cambia de **Predeterminada** a **Personalizada**. Si modifica nuevamente la configuración, la línea mostrará el nuevo valor, a menos que el nuevo valor sea el predeterminado. Cuando se fija un valor predeterminado, la línea desaparece. Por lo tanto, solo son visibles los valores que son diferentes a los valores predeterminados en esta sección de la página **Crear plan de copias de seguridad**.

Para restablecer toda la configuración a los valores predeterminados, haga clic en **Restablecer a los valores predeterminados**.

Tras realizar todos los pasos necesarios, haga clic en **Aceptar** para crear el plan de copias de seguridad.

Después, es posible que se le pida introducir una contraseña (pág. 115).

El plan que ha creado podrá examinarse y gestionarse en la vista **Planes y tareas de la copia de seguridad** (pág. 98).

6.2.1 ¿Por qué este programa me pide la contraseña?

Una tarea programada o pospuesta debe ejecutarse sin importar si los usuarios están conectados al sistema. En caso de que no haya especificado explícitamente las credenciales bajo las cuales se ejecutarán las tareas, el programa propone utilizar su cuenta. Introduzca su contraseña, especifique otra cuenta o cambie el inicio programado a manual.

6.2.2 Credenciales del plan de copias de seguridad

Proporcione credenciales para la cuenta con la que se ejecutarán las tareas del plan.

Para especificar las credenciales

1. Seleccione una de las siguientes opciones:
   - **Ejecutar bajo el usuario actual**

     Las tareas se ejecutarán bajo las credenciales de la cuenta con las que el usuario que inicia las tareas haya iniciado la sesión. Si alguna de las tareas debe ejecutarse según la programación, se le solicitará la contraseña de usuario actual al finalizar la creación de la tarea.

- **Utilizar las siguientes credenciales**

  Las tareas se ejecutarán siempre con las credenciales que especifique, ya sea que se inicie manualmente o según la programación.

  Especifique:

  - **Nombre de usuario**. Cuando introduzca el nombre de una cuenta de usuario de Active Directory, asegúrese de especificar también el nombre del dominio (DOMINIO\NombreDeUsuario o NombreDeUsuario@dominio)
  - **Contraseña**. La contraseña para la cuenta.

2. Haga clic en **Aceptar**.

Para obtener más información sobre las operaciones disponibles según los privilegios del usuario, consulte la sección Privilegios de usuario en un equipo gestionado (pág. 23).

6.2.3 Tipo de fuente

Seleccione el tipo de datos del que desea que haya una copia de seguridad en el equipo gestionado. La lista de tipos de datos disponible depende de los agentes ejecutándose en la máquina:

Archivos

Disponible si Acronis Backup & Recovery 10 Agent para Windows (o para Linux) está instalado.

Seleccione esta opción para realizar la copia de seguridad de archivos y carpetas específicas.

Si no le preocupa la recuperación del sistema operativo con todos los ajustes y las aplicaciones instalados, pero planea mantener seguros solo algunos datos (el proyecto en curso, por ejemplo), seleccione la copia de seguridad de archivo. Esto reducirá el tamaño del archivo comprimido, ahorrando así espacio de almacenamiento.

Discos/volúmenes

Disponible si el Acronis Backup & Recovery 10 Agent para Windows (o para Linux) está instalado.

Seleccione esta opción para realizar la copia de seguridad de discos y/o volúmenes. Para poder realizar la copia de seguridad de discos o volúmenes, debe tener privilegios de Administrador o de operador de copias de seguridad.

Realizar la copia de seguridad de discos y volúmenes le permite recuperar el sistema completo en caso de que suceda un fallo en el hardware o daño grave de los datos. El procedimiento de copia de seguridad es mucho más rápido que la copia de archivos y puede acelerar considerablemente el proceso de copia de seguridad cuando es necesario asegurar grandes volúmenes de datos.

Nota para los usuario de Linux: *Le recomendamos que desmonte los volúmenes que no contengan sistemas de archivos no diarios, como el sistema de archivos ext2, antes de realizar una copia de seguridad de los mismos. De lo contrario, estos volúmenes pueden contener archivos dañados tras la recuperación. Es posible que la recuperación de estos volúmenes falle.*

6.2.4 Elementos para incluir en la copia de seguridad

Los elementos para incluir en la copia de seguridad dependen del tipo de origen (pág. 116) seleccionado con anterioridad.

Seleccionar discos y volúmenes

Especificar los discos o volúmenes para incluir en la copia de seguridad

1. Seleccione las casillas de verificación para los discos o volúmenes para incluir en la copia de seguridad. Puede seleccionar un conjunto aleatorio de discos y particiones.

   Si su sistema operativo y su cargador residen en diferentes volúmenes, debe incluir siempre ambas particiones en la imagen. Los volúmenes debe recuperarse juntos, de otro modo existe el riesgo de que no inicie el sistema operativo.

   En Linux, los volúmenes lógicos y los dispositivos MD se muestran como **GPT y dinámicos**. Para obtener más información acerca de cómo hacer la copia de seguridad de dichos volúmenes y dispositivos, vaya a "Realización de copias de seguridad de volúmenes LVM y dispositivos MD (Linux) (pág. 35)".
2. [Opcional] Para crear una copia exacta de un disco o volumen en un nivel físico, seleccione la casilla de verificación **Copia de seguridad sector por sector** . La copia de seguridad resultante tendrá el mismo tamaño que el disco objeto de la copia de seguridad (si la opción de **Nivel de compresión** está establecida como **Ninguna**). Utilice la copia de seguridad sector por sector para realizar copias de seguridad de unidades con sistemas de archivos no reconocidos o incompatibles, o formatos de datos de terceros.
3. Haga clic en **Aceptar**.

¿Qué almacena una copia de seguridad de un disco o volumen?

Para sistemas de archivo compatibles, con la opción de sector por sector desactivada, una copia de seguridad de un disco o volumen almacena únicamente aquellos sectores que contienen datos. Esto reduce el tamaño de la copia de seguridad resultante y acelera las operaciones de copia de seguridad y recuperación.

Windows

Las copias de seguridad no incluyen el archivo de intercambio (pagefile.sys) ni el archivo que mantiene el contenido de la memoria RAM cuando el equipo está en estado de hibernación (hiberfil.sys). Después de la recuperación, los archivos se pueden volver a crear en el lugar apropiado con el tamaño cero.

Una copia de seguridad de volúmenes almacena todos los archivos y las carpetas del volumen seleccionado, independientemente de sus atributos (incluidos los archivos ocultos y del sistema), el registro de inicio, la tabla de asignación de archivos (FAT) si existe, la raíz y el registro cero del disco duro con el registro de inicio maestro (MBR). El código de inicio de los volúmenes GPT no se incluye en la copia de seguridad.

Un copia de seguridad del disco almacena todos los volúmenes del disco seleccionado (incluidos volúmenes ocultos como las particiones de mantenimiento del proveedor) y el registro cero con el registro de inicio maestro.

Linux

Una copia de seguridad de volúmenes almacena todos los archivos y las carpetas del volumen seleccionado, independientemente de sus atributos, un registro de inicio y el superbloque del sistema de archivos.

Una copia de seguridad del disco almacena todos los volúmenes del disco y también el registro cero junto con el registro de inicio maestro.

Seleccionar archivos y carpetas

Seleccionar los archivos o carpetas para incluir en la copia de seguridad

1. Expanda el árbol de las carpetas locales para poder ver las carpetas anidadas y sus archivos.

2. Seleccione un elemento al activar la casilla de verificación correspondiente en el árbol. Seleccionar una casilla de verificación para una carpeta significa que todo su contenido (archivos y carpetas) formará parte de la copia de seguridad. Ocurrirá lo mismo para el caso de los nuevos archivos nuevos que aparezcan en el futuro.

   Una copia de seguridad basada en archivos no es suficiente para recuperar el sistema operativo. Para recuperar el sistema operativo, debe realizar una copia de seguridad del disco.

   Utilice la tabla de la parte derecha de la ventana para explorar y seleccionar los elementos anidados. Al activar la casilla de verificación al lado del encabezado de la columna **Nombre**, automáticamente se seleccionan todos los elementos de la tabla. Al desactivar esta casilla de verificación, se anula automáticamente la selección de todos los elementos.
3. Haga clic en **Aceptar**.

6.2.5 Credenciales de acceso a los datos de origen

Especifique las credenciales que se necesitarán para el acceso a los datos que va a incluir en la copia de seguridad.

Para especificar las credenciales

1. Seleccione una de las siguientes opciones:
   - **Usar las credenciales del plan**

     El programa accederá a los datos de origen mediante las credenciales del plan de copias de seguridad especificado en la sección General.
   - **Utilice las siguientes credenciales.**

     El programa accederá a los datos de origen mediante las credenciales que especifique.Utilice esta opción si la cuenta del plan no dispone de permisos de acceso a los datos.

     Especifique:
     - **Nombre de usuario**. Cuando introduzca el nombre de una cuenta de usuario de Active Directory, asegúrese de especificar también el nombre del dominio (DOMINIO\NombreDeUsuario o NombreDeUsuario@dominio)
     - **Contraseña**. La contraseña de la cuenta.
2. Haga clic en **Aceptar**.

6.2.6 Exclusiones

[Opcional] Configure exclusiones para tipos de archivo específicos para los cuales no desea realizar copias de seguridad. Por ejemplo, quizá desee que los archivos y carpetas ocultos y del sistema, así como los archivos con extensiones específicas, no se almacenen en el archivo comprimido.

Para especificar los archivos y carpetas que desea excluir:

Configure alguno de los siguientes parámetros:

- **Excluir todos los archivos y carpetas ocultos**

  Esta opción está vigente sólo para sistemas de archivos compatibles con Windows. Seleccione esta casilla de verificación para omitir archivos y carpetas con el atributo **Oculto**. Si una carpeta está **Oculta**, se excluirán todos sus contenidos, incluso los archivos que no se encuentran **Ocultos**.
- **Excluir todos los archivos y carpetas del sistema**

Esta opción está vigente sólo 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**.

*Puede ver los atributos del archivo o de la carpeta en las propiedades del archivo/carpeta o mediante el comando **atrib**. Para obtener más información, consulte el Centro de Servicio Técnico y Ayuda de Windows.*

- **Excluir los archivos que coincidan con los siguientes criterios**

  Seleccione esta casilla de verificación para omitir los archivos y las carpetas cuyos nombres en la lista coincidan con alguno de los criterios, llamados máscaras del archivo; utilice los botones **Agregar**, **Editar**, **Eliminar** y **Eliminar todos** para crear la lista de máscaras del archivo.

  Puede utilizar uno o más caracteres comodín * y ? en una máscara de archivo:

  El asterisco (*) sustituye de cero a más caracteres del nombre del archivo; por ejemplo, la máscara de archivo Doc*.txt genera archivos Doc.txt y Document.txt

  El signo de interrogación (?) substituye a un único carácter; por ejemplo, la máscara de archivo Doc?.txt genera archivos Doc1.txt y Docs.txt, pero, por el contrario, no general archivos Doc.txt o Doc11.txt

Para excluir una carpeta especificada por una ruta que contiene la letra de unidad, agregue una barra invertida (\) al nombre de carpeta en el criterio; por ejemplo: C:\Finance\

Ejemplos de exclusión

Criterio	Ejemplo	Descripción
Windows y Linux		
Por nombre	F.log F	Excluye todos los archivos denominados "F.log" Excluye todas las carpetas denominadas "F"
Por máscara (*)	*.log F*	Excluye todos los archivos con la extensión .log Excluye todos los archivos y carpetas cuyos nombres comiencen con "F" (como carpetas F, F1 y archivos F.log, F1.log)
Por máscara (?)	F???.log	Excluye todos los archivos .log cuyos nombres contengan cuatro símbolos y comiencen con "F"
Windows		
Por ruta de archivo	C:\Finance\F.log	Excluye el archivo denominado "F.log" ubicado en la carpeta C:\Finance
Por ruta de carpeta	C:\Finance\F\	Excluye la carpeta C:\Finance\F (asegúrese de especificar la ruta completa, comenzando por la letra de unidad)
Linux		
Por ruta de archivo	/home/user/Finance/F.log	Excluye el archivo denominado "F.log", ubicado en la carpeta /home/user/Finance
Por ruta de carpeta	/home/user/Finance/	Excluye la carpeta /home/user/Finance

6.2.7 Archivo comprimido

Especifique dónde se almacenará el archivo comprimido y el nombre del archivo comprimido.

1. Seleccionar el destino

Introduzca la ruta de destino completa en el campo **Ruta** o seleccione el destino deseado en el árbol de carpetas.

- Para hacer una copia de seguridad de datos en Acronis Online Backup Storage, haga clic en **Iniciar sesión** y especifique las credenciales de acceso al almacenamiento en línea. Después, expanda el grupo **Almacenamiento de copia de seguridad en línea** y seleccione la cuenta.

  Antes de hacer una copia de seguridad del almacenamiento en línea, necesitará comprar una suscripción para el servicio de almacenamiento en línea y activar la suscripción en el(los) equipo(s) de los que desea realizar una copia de seguridad. La opción de copia de seguridad en línea no está disponible en Linux ni bajo dispositivo de inicio.

  Acronis Backup & Recovery Online es posible que no esté disponible en su región. Para obtener más información, haga clic aquí: http://www.acronis.es/my/backup-recovery-online/.

- Para realizar copias de seguridad de datos en una bóveda centralizada, amplíe el grupo **Centralizado** y haga clic en la bóveda.
- Para realizar copias de seguridad de datos en una bóveda personal, amplíe el grupo **Personalizado** y haga clic en la bóveda.
- Para realizar copias de seguridad de datos en una carpeta local del equipo, amplíe el grupo **Carpetas locales** y haga clic en la carpeta correspondiente.
- Para realizar copias de seguridad en una red compartida, amplíe el grupo **Carpetas de red**, seleccione el equipo en red correspondiente y después haga clic en la carpeta compartida. Si la red compartida requiere credenciales de acceso, el programa se las solicitará.

  Nota para los usuario de Linux: *Para especificar una red compartida de sistema de archivos de Internet común (CIFS) que esté montada en un punto de montaje como* ***/mnt/share****, seleccione este punto de montaje en lugar de la propia red compartida.*

- Para realizar copias de seguridad de datos en un servidor **FTP** o **SFTP**, escriba el nombre o dirección del servidor en el campo **Ruta** de la siguiente manera:

  ftp://ftp_server:port _number o **sftp://sftp_server:port number**

  Si no se especifica el número del puerto, se utilizará el puerto 21 para FTP y el puerto 22 para SFTP.

  Tras introducir las credenciales de acceso, las carpetas en el servidor estarán disponible. Haga clic en la carpeta correspondiente del servidor.

  Puede acceder al servidor como usuario anónimo, si el servidor permite ese tipo de acceso. Para esto, haga clic en **Usar acceso anónimo** en lugar de introducir las credenciales.

  Como se muestra en la especificación FTP original, los credenciales necesarios para acceder a los servidores FTP se transfieren a través de la red como texto sin formato. Esto significa que una persona no deseada puede interceptar el nombre de usuario y la contraseña utilizando un comprobador de paquetes.

- Para realizar copias de seguridad de datos en un dispositivo de cinta conectado a nivel local, amplíe el grupo **Unidades de cinta** y haga clic en el dispositivo correspondiente.

2. Uso de la tabla de archivos comprimidos

Para asistirle en la elección del destino correcto, la tabla muestra los nombres de los archivos comprimidos contenidos en cada una de las ubicaciones que seleccione. Mientras usted revisa el

contenido de la ubicación, otro usuario o el mismo programa pueden añadir, eliminar o modificar archivos comprimidos de acuerdo con las operaciones programadas. Utilice el botón **Actualizar** para actualizar la lista de archivos comprimidos.

3. Nombrar un archivo comprimido nuevo

Una vez que seleccione el destino del archivo comprimido, el programa genera un nombre para el nuevo archivo comprimido y lo muestra en el campo **Nombre**. El nombre aparece normalmente como Archivo(1). El nombre generado es único dentro de la ubicación seleccionada. Si está satisfecho con el nombre generado automáticamente, haga clic en **Aceptar**. De lo contrario, introduzca otro nombre único y haga clic en **Aceptar**.

Realizar una copia de seguridad en un archivo comprimido existente

Puede configurar el plan de copia de seguridad para realizar una copia de seguridad a un archivo comprimido existente. Para hacerlo, seleccione el archivo comprimido en la tabla de archivos comprimidos o escriba el nombre del archivo comprimido en el campo **Nombre**. Si el archivo comprimido está protegido con una contraseña, el programa le pedirá que la introduzca en una ventana emergente.

Al seleccionar un archivo comprimido existente, se está entrometiendo en el área de otro plan de copia de seguridad que utiliza el archivo comprimido. Esto no será un problema si el otro plan se ha interrumpido, pero en general debería seguir la regla: "un plan de copia de seguridad - un archivo comprimido". Lo contrario no provocará que el programa deje de funcionar pero no es práctico ni eficiente, a excepción de algunos casos específicos.

Por qué dos o más planes no deberían realizar copias de seguridad del mismo archivo comprimido

1. Realizar copias de seguridad de orígenes diferentes en el mismo archivo comprimido dificulta la utilización del archivo comprimido desde el punto de vista de la funcionalidad. Cuando se trata de recuperación, cada segundo es valioso, pero puede perderse en el contenido del archivo comprimido.

   Los planes de copias de seguridad que funcionan con el mismo archivo comprimido deberían realizar copias de seguridad de los mismos elementos de datos (por ejemplo, ambos planes realizan una copia de seguridad del volumen C).
2. Aplicar múltiples reglas de retención a un archivo comprimido hace que el contenido del mismo sea impredecible en cierta medida. Como cada una de las reglas se aplicarán al archivo comprimido completo, las copias de seguridad correspondientes a un plan de copias de seguridad se pueden borrar con facilidad junto con las copias de seguridad correspondientes al otro. Particularmente, no debe esperar el comportamiento clásico de los esquemas de copia de seguridad GFS y Torres de Hanói.

   Por lo general, cada plan de copias de seguridad complejo debe realizar la copia de seguridad de su propio archivo comprimido.

6.2.8 Asignación simplificada de nombre a los archivos de copia de seguridad

Si selecciona la casilla de verificación **Nombrar los archivos de copia de seguridad utilizando el nombre del archivo comprimido...**:

- El nombre de archivo de la primera copia de seguridad completa consistirá en el nombre del archivo comprimido; por ejemplo: **MyData.tib.** Los nombres de los archivos de posteriores copias

de seguridad (incrementales o diferenciales) tendrán un índice; por ejemplo: **MyData2.tib**, **MyData3.tib**y así sucesivamente.

Este sencillo esquema de nombres le permite crear una imagen portátil de un equipo en un medio extraíble o mover las copias de seguridad a una ubicación diferente utilizando un comando.

- Antes de crear una nueva copia de seguridad completa, el software eliminará el archivo comprimido entero e iniciará uno nuevo.

  Este comportamiento es muy útil cuando rote discos duros USB y cuando quiere que cada disco mantenga una sola copia de seguridad completa (pág. 124) o todas las copias de seguridad creadas a lo largo de una semana (pág. 124). Pero puede acabar sin ninguna copia de seguridad en el caso de que falle una copia de seguridad completa de una sola unidad.

  Este comportamiento puede ser eliminado si agrega la [Date] variable (pág. 125) al nombre de archivo comprimido.

Si *no* selecciona la casilla de verificación **Nombrar los archivos de copia de seguridad utilizando el nombre del archivo comprimido...**:

- Cada copia de seguridad tendrá un único nombre de archivo con el sello de tiempo exacto y el tipo de copia de seguridad; por ejemplo: **MyData_2010_03_26_17_01_38_960D.tib**. Esta forma estándar de nombre archivos permite una gama más amplia de destinos de copias de seguridad y de esquemas de copias de seguridad.

Restricciones

Al utilizar la simplificación de nombre de archivos, la siguiente funcionalidad deja de estar disponible:

- Configuración de copias de seguridad completas, incrementales y diferenciales dentro de un único plan de copias de seguridad. Necesita crear planes de copias de seguridad separados para cada tipo de copia de seguridad.
- Copia de seguridad de una bóveda gestionada, cinta Acronis Secure Zone o Acronis almacenamiento de copias de seguridad en línea
- Configuración de reglas de retención
- Configuración de una conversión regular de copias de seguridad a una máquina virtual
- Utilización de numerales al final del nombre del archivo comprimido

Consejo. *Los sistemas de archivos FAT16, FAT32 y NTFS no permiten los siguientes caracteres en el nombre de archivo: barra invertida (\), barra (/), dos puntos (:), asterisco (*), signo de interrogación (?), comillas ("), signo menos que (<), signo más que (>), y barra vertical (|).*

Ejemplos de uso

Esta sección proporciona ejemplos de cómo puede usar la simplificación de nombres de archivos.

Ejemplo 1. Realice una copia de seguridad diaria reemplazando el antiguo

Considere el siguiente escenario:

- Desea realizar una copia de seguridad diaria completa de su equipo.
- Desea almacenar la copia de seguridad de forma local en el archivo **MyMachine.tib**.
- Desea que cada copia de seguridad nueva reemplace a la antigua.

En este escenario, cree un plan de copia de seguridad con una programación diaria. Al crear el plan de copias de seguridad, especifique **MiEquipo** como el nombre del archivo comprimido, seleccione la

casilla de verificación **Nombrar los archivos de copia de seguridad utilizando el nombre del archivo comprimido...** y seleccione **Completa** como el tipo de copia de seguridad.

Resultado. El archivo comprimido consiste en un único archivo: MyMachine.tib. Este archivo se eliminará antes de crear una nueva copia de seguridad.

Ejemplo 2. Copias de seguridad completas diarias con sello de fecha.

Considere el siguiente escenario:

- Desea realizar una copia de seguridad diaria completa de su equipo.
- Desea mover las copias de seguridad más antiguas a una ubicación remota utilizando un comando.

En este escenario, cree un plan de copia de seguridad con una programación diaria. Al crear el plan de copias de seguridad, especifique **MiEquipo-[DATE]** como el nombre del archivo comprimido, seleccione la casilla de verificación **Nombrar los archivos de copia de seguridad utilizando el nombre del archivo comprimido...** y seleccione **Completa** como el tipo de copia de seguridad.

Resultado:

- Las copias de seguridad de el 1 de enero de 2011, 2 de enero de 2011 y así sucesivamente, son almacenadas respectivamente en MyMachine-1.1.2011.tib, MyMachine-1.2.2011.tib y así sucesivamente.
- Su comando puede mover las copias de seguridad más antiguas basadas en el sello de la fecha.

Vea también “La variable [Date]” (pág. 125).

Ejemplo 3. Copias de seguridad a la hora en un día.

Considere el siguiente escenario:

- Desea realizar copias de seguridad cada hora de sus archivos críticos todos los días.
- Desea que la primera copia de seguridad de cada día sea completa y se ejecute a medianoche; y que las posteriores copias de seguridad del día sean diferenciales y se ejecuten a la 01.00, a las 02.00 y así sucesivamente.
- Desea mantener las copias de seguridad más antiguas en el archivo comprimido.

En este escenario, cree un plan de copia de seguridad con una programación diaria. Al crear el plan de copia de seguridad, especifique **ServerFiles([Date])** como nombre del archivo comprimido; seleccione la casilla de verificación **Nombrar los archivos de copia de seguridad utilizando el nombre del archivo comprimido**..., especifique **Diferencial** como el tipo de copia de seguridad y programe las copias de seguridad para que se ejecuten cada hora desde la medianoche.

Resultado:

- Las 24 copias de seguridad de el 1 de enero de 2011, se almacenarán como ServerFiles(1.1.2011).tib, ServerFiles(1.1.2011)2.tib y así sucesivamente hasta ServerFiles(1.1.2011)24.tib.
- Al día siguiente, las copias de seguridad comenzarán con la copia de seguridad completa de ServerFiles(1.2.2011).tib.

Vea también “La variable [Date]” (pág. 125).

Ejemplo 4. Copias de seguridad completas diarias con intercambios de unidad

Considere el siguiente escenario:

- Desea realizar copias de seguridad completas diarias de su equipo al archivo **MyMachine.tib** en una unidad de disco duro externa.
- Tiene las dos unidades. Cualquiera de ellas tiene la letra de unidad **D** cuando está adjuntada al equipo.
- Desea intercambiar las unidades antes de cada copia de seguridad, de forma que una unidad contenga la copia de seguridad de hoy y la otra unidad la copia de seguridad de ayer.
- Desea que cada nueva copia de seguridad reemplace a la copia de seguridad de la unidad adjuntada actualmente.

En este escenario, cree un plan de copia de seguridad con una programación diaria. Al crear el plan de copias de seguridad, especifique **MiEquipo** como el nombre del archivo comprimido y **D:** como la ubicación del archivo comprimido, seleccione la casilla de verificación **Nombrar los archivos de copia de seguridad utilizando el nombre del archivo comprimido...** y seleccione **Completa** como el tipo de copia de seguridad.

Resultado. Cada unidad de disco duro contendrá una copia de seguridad completa. Mientras una de las unidades está adjuntada al equipo, puede mantener la otra unidad de forma externa para obtener una mayor protección de datos.

Ejemplo 5. Copias de seguridad diarias con intercambios de unidad semanales

Considere el siguiente escenario:

- Desea realizar copias de seguridad diarias de su equipo: una copia de seguridad completa cada lunes y copias de seguridad incrementales del martes al domingo.
- Desea hacer una copia de seguridad del archivo comprimido **MyMachine** en la unidad de disco duro externa.
- Tiene las dos unidades. Cualquiera de ellas tiene la letra de unidad **D** en el sistema operativo cuando está adjuntada al equipo.
- Desea intercambiar las unidades cada lunes, de forma que una unidad contenga copias de seguridad de la actual semana (de lunes a domingo) y que la otra unidad contenga las de la semana anterior.

En este escenario, necesita crear dos planes de copia de seguridad de la siguiente manera:

a) Al crear el primer plan de copia de seguridad especifique **MiEquipo** como el nombre de archivo comprimido y **D:** como la ubicación del archivo comprimido; seleccione la casilla de verificación **Nombrar los archivos de copia de seguridad utilizando el nombre del archivo comprimido...**, seleccione **Completa** como el tipo de copia de seguridad y programa las copias de seguridad para que se ejecuten el lunes de cada semana.

b) Al crear el segundo plan de copia de seguridad, especifique las mismas configuraciones que en el primer plan de copia de seguridad, pero seleccione **Incremental** como el tipo de copia de seguridad y programe las copias de seguridad para que se ejecuten cada semana de martes a domingo.

Resultado:

- Antes de crear una copia de seguridad de lunes, con el primer plan de copia de seguridad, todas las copias de seguridad quedarán eliminadas de la unidad adjuntada actualmente.
- Mientras una de las unidades está adjuntada al equipo, puede mantener la otra unidad de forma externa para obtener una mayor protección de datos.

Ejemplo 6. Copias de seguridad en horas de trabajo.

Considere el siguiente escenario:

- Desea realizar copias de seguridad de los archivos críticos de su servidor todos los días.
- Desea que la primera copia de seguridad de cada día sea completa y se ejecute a la 01:00.
- Desea que las copias de seguridad durante las horas de trabajo sean diferenciales y se ejecuten cada hora desde las 08:00 hasta las 17:00.
- Desea incluir una fecha de creación en el nombre de cada archivo de copia de seguridad.

En este escenario, necesita crear dos planes de copia de seguridad de la siguiente manera:

a) Al crear la primera copia de seguridad especifique **ServerFiles([DATE])** como el nombre del archivo comprimido; seleccione la casilla de verificación **Nombrar los archivos de copia de seguridad utilizando el nombre del archivo comprimido...**; seleccione **Completa** como el tipo de copia de seguridad y programa las copias de seguridad para que se ejecuten cada día a la 01:00.

b) Al crear el segundo plan de copia de seguridad, especifique las mismas configuraciones que en el primer plan de copia de seguridad, pero seleccione **Diferencial** como el tipo de copia de seguridad y programe las copias de seguridad como se explica a continuación:
   - **Ejecute la tarea**: **Diariamente**
   - **Cada**: **1 Hora(s)**
   - **Desde las**: **08:00:00**
   - **Hasta las**: **17:01:00**

Resultado:

- La copia de seguridad completa del 31 de enero de 2011, se almacenará como ServerFiles(1.31.2011).tib.
- Las 10 copias de seguridad diferenciales del 31 de enero de 2011, se almacenarán como ServerFiles(1.31.2011)2.tib, ServerFiles(1.31.2011)3.tib y así sucesivamente hasta ServerFiles(1.31.2011)11.tib.
- Al día siguiente, el 1 de febrero, las copias de seguridad comenzarán con la copia de seguridad completa de ServerFiles(2.1.2011).tib. Las copias de seguridad diferenciales comenzarán con ServerFiles(2.1.2011)2.tib.

Vea también “La variable [Date]” (pág. 125).

La variable [DATE]

Si especifica la variable **[DATE]** en el nombre del archivo comprimido, el nombre del archivo de cada copia de seguridad incluirá la fecha de creación de esa copia de seguridad.

Al utilizar esta variable, la primera copia de seguridad de cada día será una copia de seguridad completa. Antes de crear la siguiente copia de seguridad completa, el software elimina todas las copias de seguridad realizadas más pronto ese día. Se mantienen las copias de seguridad realizadas antes de ese día. Esto significa que puede almacenar múltiples copias de seguridad completas con o sin las incrementales, pero no más de una copia de seguridad completa por día. Puede clasificar las

copias de seguridad por día; copiar, mover y/o eliminar copias de seguridad de forma manual o bien utilizando un comando.

El formato de fecha es *mes.día.año*. Por ejemplo, para enero es el 1.31.2011 31, 2011. (Nota: ausencia de ceros).

Puede colocar esta variable en cualquier lugar del nombre del archivo comprimido. Puede usar letras tanto minúsculas como mayúsculas en esta variable.

Ejemplos

Ejemplo 1. Suponga que realiza copias de seguridad incrementales dos veces al día (a medianoche y al mediodía) durante dos días empezando el 31 de enero de 2011. Si el nombre del archivo comprimido es **MyArchive-[DATE]-**, a continuación la lista de archivos de copias de seguridad después del día dos:

MyArchive-1.31.2011-.tib (full, created on January 31 at midnight)
MyArchive-1.31.2011-2.tib (incremental, created on January 31 at noon)
MyArchive-2.1.2011-.tib (full, created on February 1 at midnight)
MyArchive-2.1.2011-2.tib (incremental, created on February 1 at noon)

Ejemplo 2. Suponga que realiza copias de seguridad completas, con la misma programación y nombre de archivo comprimido, siguiendo el ejemplo anterior. Así, la lista de archivos de copias de seguridad después del día dos es la que viene a continuación:

MyArchive-1.31.2011-.tib (completa, creada el 31 de enero a medianoche)
MyArchive-2.1.2011-.tib (completa, creada el 1 de febrero a medianoche)

Esto es porque las copias de seguridad completas creadas a medianoche fueron reemplazadas por copias de seguridad completas del mismo día.

Simplificación de nombre de archivos y división de copias de seguridad

Cuando se divide una copia de seguridad de acuerdo con las configuraciones de División de copias de seguridad (pág. 62), se utiliza la misma indexación para nombrar también las partes de la copia de seguridad. El nombre de archivo de la siguiente copia de seguridad tendrá el siguiente índice disponible.

Por ejemplo, suponga que la primera copia de seguridad del archivo comprimido **MyData** ha sido dividido en dos partes. Entonces los nombres de los archivos para esta copia de seguridad serán **MyData1.tib** y **MyData2.tib**. El nombre de la segunda copia de seguridad, suponiendo que no está dividida, será **MyData3.tib**.

6.2.9 Credenciales de acceso para la ubicación del archivo comprimido

Especifique las credenciales que se necesitarán para el acceso a la ubicación donde se almacenará el archivo comprimido de la copia de seguridad. El usuario cuyo nombre se especifique se considerará el propietario del archivo comprimido.

Para especificar las credenciales

1. Seleccione una de las siguientes opciones:
   - **Usar las credenciales del plan**

     El programa accederá a los datos de origen mediante las credenciales del plan de copias de seguridad especificado en la sección General.

- **Utilice las siguientes credenciales.**

  El programa accederá a los datos de origen mediante las credenciales que especifique.Utilice esta opción si la cuenta del plan no dispone de permisos de acceso a la ubicación. Quizás necesite atribuir credenciales especiales para una red compartida o para una bóveda de nodo de almacenamiento.

  Especifique:

  - **Nombre de usuario**. Cuando introduzca el nombre de una cuenta de usuario de Active Directory, asegúrese de especificar también el nombre del dominio (DOMINIO\NombreDeUsuario o NombreDeUsuario@dominio)
  - **Contraseña**. La contraseña de la cuenta.

2. Haga clic en **Aceptar**.

Advertencia: *Como se muestra en la especificación FTP original, los credenciales necesarios para acceder a los servidores FTP se transfieren a través de la red como texto sin formato. Esto significa que una persona no deseada puede interceptar el nombre de usuario y la contraseña utilizando un comprobador de paquetes.*

6.2.10 Esquemas de copia de seguridad

Elija uno de los esquemas de copia de seguridad disponibles:

- **Copia de seguridad ahora** – para crear una tarea de copia de seguridad para un inicio manual y ejecutar la tarea inmediatamente después de crearla.
- **Copia de seguridad más tarde** – para crear una tarea de copia de seguridad para un inicio manual O programar que la tarea se ejecute más tarde una vez.
- **Simple** – para programar cuándo y con qué frecuencia realizar copias de seguridad de los datos y especificar reglas de retención.
- **Abuelo-Padre-Hijo** – para utilizar el esquema de copia de seguridad Abuelo-Padre-Hijo. Este esquema sólo permite realizar copias de seguridad de los datos una vez al día.. Puede configurar los días de la semana en los que se llevará a cabo la copia de seguridad y seleccionar de entre esos días, la fecha para la copia de seguridad semanal o mensual. Después, debe ajustar los periodos de retención para las copias de seguridad diarias (llamadas "hijos"), semanales (llamadas "padres") y mensuales (llamadas "abuelos"). Las copias de seguridad caducadas se borrarán automáticamente.
- **Torre de Hanoi** – para utilizar el esquema de copia de seguridad Torre de Hanoi, en el que se programa cuándo y con qué frecuencia realizar copias de seguridad (sesiones) y se selecciona el número de niveles de copia de seguridad (hasta 16). Con este esquema, se puede realizar más de una copia de seguridad de los datos al día. Al configurar el calendario de copia de seguridad y seleccionar los niveles de copia de seguridad, se obtiene automáticamente el periodo de recuperación, es decir, el número garantizado de sesiones que se pueden a las que se puede volver en cualquier momento. El mecanismo de limpieza automático mantiene el periodo de recuperación necesario, borrando las copias de seguridad caducadas y conservando las copias de seguridad más recientes de cada nivel.
- **Personalizada** – para crear una copia de seguridad personalizada, en la que se puede configurar libremente la estrategia que mejor convenga a las necesidades de su empresa: especificar diferentes programaciones para diferentes tipos de copias de seguridad, añadir condiciones y especificar las reglas de retención.
- **Inserción inicial** - para guardar localmente una copia de seguridad completa cuyo destino final es Acronis Online Backup Storage.

Esquema Copia de seguridad ahora

Con el esquema **Copia de seguridad ahora**, la copia de seguridad se llevará a cabo inmediatamente después de que haga clic en el botón **Aceptar** en la parte inferior de la página.

En el campo **Tipo de copia de seguridad**, seleccione si desea crear una copia de seguridad completa, incremental o diferencial (pág. 21).

Esquema Copia de seguridad más tarde

Con el esquema Copia de seguridad más tarde, la copia de seguridad se llevará a cabo una sola vez, en la fecha y hora que especifique.

Especifique los ajustes adecuados de la siguiente manera

Tipo de copia de seguridad	Seleccione el tipo de copia de seguridad: completo, incremental o diferencial. Si no existe una copia de seguridad completa en el archivo comprimido, se creará una independientemente de su elección.
Fecha y hora	Especifique cuándo desea iniciar la copia de seguridad.
La tarea se iniciará manualmente	Seleccione esta casilla de verificación si no necesita colocar la tarea de copia de seguridad en una programación y desea iniciarla manualmente más tarde.

Esquema simple

Con el esquema simple de copia de seguridad, simplemente debe programar cuándo y con qué frecuencia realizar copias de seguridad de los datos y configurar la regla de retención. La primera vez se creará una copia de seguridad completa. Las siguientes copias de seguridad serán incrementales.

Para configurar el esquema simple de copia de seguridad, especifique los ajustes apropiados de la siguiente manera.

Crear copia de seguridad	Configure la programación de la copia de seguridad: cuándo y con qué frecuencia realizar copias de seguridad de los datos. Para obtener más información sobre cómo configurar el calendario, consulte la sección Programación (pág. 85).
Regla de retención	Con el esquema simple, solo se dispone de una regla de retención (pág. 32). Configure el periodo de retención para las copias de seguridad.

Esquema Abuelo-padre-hijo

De un vistazo

- Copias de seguridad incrementales diarias, diferenciales semanales y completas mensuales
- Día personalizado para las copias de seguridad semanales y mensuales
- Periodos de retención personalizados para las copias de seguridad de cada tipo

Descripción

Supongamos que queremos configurar un plan de copias de seguridad que produzca una serie de copias de seguridad regulares diarias (D), semanales (S) y mensuales (M). Este es el modo más normal para hacerlo: la siguiente tabla muestra un ejemplo de un periodo de dos meses para dicho plan.

	Lu	Ma	Mi	Ju	Vi	Sa	Do
1 Ene—7 Ene	D	D	D	D	S	-	-
8 Ene—14 Ene	D	D	D	D	S	-	-
15 Ene—21 Ene	D	D	D	D	S	-	-
22 Ene—28 Ene	D	D	D	D	M	-	-
29 Ene—4 Feb	D	D	D	D	S	-	-
5 Feb—11 Feb	D	D	D	D	S	-	-
12 Feb—18 Feb	D	D	D	D	S	-	-
19 Feb—25 Feb	D	D	D	D	M	-	-
26 Feb—4 Mar	D	D	D	D	S	-	-

Las copias de seguridad diarias se ejecutan todos los días laborables excepto los viernes, que se reservan para las copias de seguridad semanales y mensuales. Las copias de seguridad mensuales se llevan a cabo el cuarto viernes de cada mes y las semanales, los demás viernes del mes.

- Las copias de seguridad mensuales ("Abuelo") son completas;
- Las copias de seguridad semanales ("Padre") son diferenciales;
- Las copias de seguridad diarias ("Hijo") son incrementales.

Parámetros

Puede configurar los siguientes parámetros de un esquema Abuelo-Padre-Hijo (GFS).

Comienzo de la copia de seguridad en:	Especifica cuándo se inicia una copia de seguridad. El valor predeterminado son las 12:00.
Copia de seguridad en:	Especifica los días en los que se lleva a cabo la copia de seguridad. El valor predeterminado es el viernes.
Semanalmente/mensualmente:	Especifica cuál de los días elegidos en el campo **Realizar copias de seguridad el** desea reservar para las copias de seguridad semanales y mensuales. El cuarto día especificado del mes se llevará a cabo una copia de seguridad mensual. El valor predeterminado es el viernes.

Mantener copias de seguridad:	Especifica durante cuánto tiempo desea que se almacenen las copias de seguridad en el archivo comprimido. Se puede configurar en horas, días, semanas, meses o años. Para copias de seguridad mensuales, puede seleccionar también **Mantener indefinidamente** si desea que se almacenen para siempre. Los valores predeterminados para cada tipo de copia de seguridad son los siguientes. Diariamente: 7 días (mínimo recomendado) Semanalmente: 4 semanas Mensualmente: indefinidamente El periodo de retención para las copias de seguridad semanales debe ser mayor al establecido para las diarias. Del mismo modo, el periodo de retención para las copias de seguridad mensuales debe ser mayor al de las copias semanales. Le recomendamos configurar un periodo de retención de al menos una semana para las copias de seguridad diarias.

Nunca se elimina una copia de seguridad hasta que todas las copias de seguridad que dependen directamente de ella se puedan eliminar. Por esta razón, puede que observe que una copia de seguridad semanal o mensual permanece en el archivo comprimido incluso unos días después de la fecha de caducidad esperada.

Si la programación comienza con una copia de seguridad diaria o semanal, en su lugar se crea una copia de seguridad completa.

Ejemplos

Cada día de la semana pasada, cada semana del mes pasado

Permítanos sugerir un esquema de copia de seguridad GFS que podría encontrar útil.

- Realizar copias de seguridad cada día, fines de semana incluidos
- Tener la posibilidad de recuperar los archivos de cualquier fecha dentro de los últimos siete días
- Tener acceso a las copias de seguridad semanales del mes anterior.
- Mantener copias de seguridad mensuales indefinidamente.

Los parámetros del esquema de copia de seguridad se pueden configurar de la siguiente manera.

- Comienzo de la copia de seguridad en: **23:00**
- Copia de seguridad en: **Todos los días**
- Semanalmente/mensualmente: **Sábado** (por ejemplo)
- Mantener copias de seguridad:
  - Diariamente: **1 semana**
  - Semanalmente: **1 mes**
  - Mensualmente: **indefinidamente**

Por lo tanto, se creará un archivo comprimido de copias de seguridad diarias, semanales y mensuales. Las copias de seguridad diarias estarán disponibles durante siete días a partir de la fecha de creación. Por ejemplo, una copia de seguridad diaria con fecha de domingo, 1 de enero,

permanecerá disponible hasta el próximo domingo, 8 de enero; la primera copia de seguridad semanal, con fecha de sábado, 7 de enero, se almacenará en el sistema hasta el 7 de febrero. Las copias de seguridad mensuales no se eliminarán nunca.

Almacenamiento limitado

Si no desea fijar una gran cantidad de espacio para almacenar un archivo comprimido muy grande, debería configurar un esquema GFS para limitar la vida media de sus copias de seguridad, a la vez que garantiza que su información pueda recuperarse en caso de una pérdida de datos accidental.

Suponga que necesita:

- Realizar copias de seguridad al final de cada día laborable
- Tener la posibilidad de recuperar un archivo modificado o eliminado de manera accidental si se ha detectado relativamente pronto
- Tener acceso a una copia de seguridad semanal durante 10 días después de su creación.
- Conservar copias de seguridad mensuales durante 6 meses.

Los parámetros del esquema de copia de seguridad se pueden configurar de la siguiente manera.

- Comienzo de la copia de seguridad a las: **18:00**
- Copia de seguridad el: **Días hábiles**
- Semanalmente/mensualmente: **Viernes**
- Mantener copias de seguridad:
  - Diaria: **1 semana**
  - Semanal: **10 días**
  - Mensual: **6 meses**

Con este esquema, dispondrá de una semana para recuperar una versión anterior de un archivo dañado a partir de una copia de seguridad diaria, así como de 10 días de acceso a las copias de seguridad semanales. Las copias de seguridad completas mensuales estarán disponible durante 6 meses a partir de la fecha de creación.

Programación laboral

Supongamos que es consultor financiero y trabaja media jornada en una empresa los martes y jueves. Durante estos días, por lo general, realiza cambios en documentos financieros y declaraciones, y actualiza hojas de cálculo, etc. en su portátil. Para realizar copias de seguridad de estos datos, es conveniente que:

- Rastree los cambios en las declaraciones financieras, hojas de cálculo, etc. realizados los martes y jueves (copia de seguridad incremental diaria).
- Tenga un resumen semanal de los cambios en los archivos desde el mes pasado (copia de seguridad diferencial semanal).
- Tenga una copia de seguridad completa mensual de todos los archivos.

Además, supongamos que desea mantener el acceso a todas las copias de seguridad, incluidas las diarias, durante al menos seis meses.

El siguiente esquema GFS cumple estos fines:

- Iniciar copia de seguridad a las: **23:30.**
- Realizar copias de seguridad el: **Martes, Jueves, Viernes**
- Semanalmente/mensualmente: **Viernes**

- Mantener copias de seguridad:
  - Diariamente: **6 meses**
  - Semanalmente: **6 meses**
  - Mensualmente: **5 años**

Aquí, las copias de seguridad incrementales diarias se crearán los martes y jueves, con copias de seguridad semanales y mensuales que se realizarán los viernes. Tenga en cuenta que, para elegir **Viernes** en el campo **Semanalmente/mensualmente**, deberá seleccionarlo primero en el campo **Realizar copias de seguridad el**.

Ese archivo comprimido le permitirá comparar los documentos financieros a partir del primer y último día hábil, y tener un historial de cinco años de todos los documentos, etc.

Sin copias de seguridad diarias

Considere un esquema GFS diferente:

- Iniciar copia de seguridad a las: **12:00.**
- Realizar copias de seguridad el: **Viernes**
- Semanalmente/mensualmente: **Viernes**
- Mantener copias de seguridad:
  - Diariamente: **1 semana**
  - Semanalmente: **1 mes**
  - Mensualmente: **indefinidamente**

La copia de seguridad, por lo tanto, se realiza solo los viernes. Esto hace que el viernes sea la única opción para realizar copias de seguridad semanales y mensuales, sin que haya otra fecha para las copias de seguridad diarias. El archivo comprimido “Abuelo-padre” resultante, por lo tanto, consistirá solo de copias de seguridad diferenciales semanales y completas mensuales.

Si bien se puede utilizar el esquema GFS para crear dicho archivo comprimido, el esquema personalizado es más flexible para esta situación.

Esquema Torres de Hanói

De un vistazo

- Hasta 16 niveles de copias de seguridad completas, diferenciales e incrementales
- La frecuencia de las copias de seguridad del nivel siguiente es exactamente la mitad de la de las copias de seguridad de los niveles anteriores.
- Solo se almacena una copia de seguridad de cada nivel al mismo tiempo
- La cantidad de copias de seguridad recientes es mayor que la de las antiguas.

Parámetros

Puede configurar los siguientes parámetros de un esquema Torres de Hanói.

Programación	Configurar una programación diaria (pág. 86), semanal (pág. 88) o mensual (pág. 90). Se pueden crear programaciones simples al configurar los parámetros de la programación (ejemplo de una programación simple diaria: se realizará una tarea de copia de seguridad cada día 1 a las 10:00), así como programaciones más complejas (ejemplo de una programación compleja diaria: se realizará una tarea cada 3 días, comenzando a partir del 15 de enero. En los días especificados, la tarea se repetirá cada 2 horas desde las 10 hasta las 22 horas). De este modo, las programaciones complejas especifican las sesiones en las que el esquema debería ejecutarse. En los comentarios siguientes, se puede reemplazar por

	"sesiones programadas".
Número de niveles	Seleccione los niveles de copia de seguridad entre 2 a 16. Para obtener más información, consulte el siguiente ejemplo.
Periodo de recuperación	El número garantizado de sesiones a las que se puede volver en el archivo comprimido en cualquier momento. Se calcula automáticamente, dependiendo de los parámetros de programación y de los niveles que seleccione. Para obtener más información, consulte el siguiente ejemplo.

Ejemplo

Los parámetros de **Programación** se configuran de la siguiente manera

- Repetir: Cada día
- Frecuencia: Por primera vez a las 18:00

Número de niveles: 4

Para los 14 días siguientes (o 14 sesiones), este esquema de programación se verá de la siguiente manera: Los números sombreados indican los niveles de copia de seguridad.

1	2	3	4	5	6	7	8	9	10	11	12	13	14
4	1	2	1	3	1	2	1	4	1	2	1	3	1

Las copias de seguridad de niveles diferentes son de diferentes tipos:

- Las copias de seguridad de *último nivel* (en este caso, nivel 4) son completas;
- Las copias de seguridad de *niveles intermedios* (2, 3) son diferenciales;
- Las copias de seguridad de *primer nivel* (1) son incrementales.

Un mecanismo de limpieza garantiza que solo se mantienen las copias de seguridad más recientes de cada nivel. Este es el aspecto del archivo comprimido en el día 8, un día antes de crear una nueva copia de seguridad completa.

1	2	3	4	5	6	7	8
4	1	2	1	3	1	2	1

El esquema permite un almacenamiento eficiente de los datos: Se acumulan más copias de seguridad cuanto más cerca nos encontramos de la fecha actual. Con 4 copias de seguridad, se pueden recuperar datos de hoy, de ayer, de media semana o de una semana atrás.

Periodo de recuperación

El número de días a los que se puede volver en el archivo comprimido es diferente en función del día. El número mínimo de días garantizados se llama periodo de recuperación.

La siguiente tabla muestra los periodos de copia de seguridad completos y los periodos de recuperación para esquemas de diferentes niveles.

Número de niveles	**Copia de seguridad completa cada**	**En días diferentes, puede volver atrás**	**Periodo de recuperación**
2	2 días	De 1 a 2 días	1 día
3	4 días	De 2 a 5 días	2 días

4	8 días	De 4 a 11 días	4 días
5	16 días	De 8 a 23 días	8 días
6	32 días	De 16 a 47 días	16 días

Al aumentar un nivel, la duración de los periodos de copia de seguridad completa y de recuperación se multiplican por dos.

Para ver por qué varía el número de los días de recuperación, consulte el ejemplo siguiente.

A continuación se encuentran las copias de seguridad que tenemos en el día 12 (los números en gris indican las copias de seguridad eliminadas).

1	2	3	4	5	6	7	8	9	10	11	12
4	1	2	1	3	1	2	1	4	1	2	1

Todavía no se ha creado una copia de seguridad diferencial de nivel 3, por lo que la copia de seguridad del día 5 aún se encuentra almacenada. Esta copia de seguridad sigue estando disponible ya que depende de la copia de seguridad completa del día 1. Esto nos permite retroceder hasta 11 días, lo cual constituye el mejor de los casos posibles.

El día siguiente, sin embargo, se crea una nueva copia de seguridad diferencial de nivel 3 y se elimina la copia de seguridad completa antigua.

1	2	3	4	5	6	7	8	9	10	11	12	13
4	1	2	1	3	1	2	1	4	1	2	1	3

Esto nos proporciona solo un intervalo de recuperación de 4 días, lo que representa la peor situación posible.

En el día 14, el intervalo es de 5 días. En los días siguientes, este intervalo va aumentando hasta volver a reducirse, sucesivamente.

1	2	3	4	5	6	7	8	9	10	11	12	13	14
4	1	2	1	3	1	2	1	4	1	2	1	3	1

El periodo de recuperación muestra el número de días que están garantizados incluso en el peor de los casos. Para un esquema de cuatro niveles, es de 4 días.

Esquema personalizado de copia de seguridad

De un vistazo

- Programación personalizada y condiciones de copia de seguridad de cada tipo
- Programación personalizada y reglas de retención

Parámetros

Parámetro	Significado
Copia de seguridad completa	Especifica con qué programación y bajo qué condiciones realizar una copia de seguridad completa. Por ejemplo, la copia de seguridad completa puede configurarse para que se ejecute cada domingo a la 01:00, tan pronto como todos los usuarios hayan cerrado sus sesiones.
Incremental	Especifica con qué programación y bajo qué condiciones realizar una copia de seguridad incremental. Si el archivo comprimido no contiene copias de seguridad cuando se ejecute la tarea,

	se llevará a cabo una copia de seguridad completa en lugar de una incremental.
Diferencial	Especifica con qué programación y bajo qué condiciones realizar una copia de seguridad diferencial. Si el archivo comprimido no contiene copias de seguridad cuando se ejecute la tarea, se llevará a cabo una copia de seguridad completa en lugar de una diferencial.
Limpie el archivo comprimido	Especifica cómo eliminar copias de seguridad antiguas: ya sea aplicando reglas de retención (pág. 32) regularmente o limpiando el archivo durante la realización de una copia de seguridad cuando la ubicación de destino se queda sin espacio. De manera predeterminada, las reglas de retención no se especifican, lo cual significa que las copias de seguridad más antiguas no se eliminarán de forma automática. **Utilización de reglas de retención** Especifique las reglas de retención y cuándo aplicarlas. Se recomienda esta configuración para destinos de copias de seguridad como carpetas compartidas o bóvedas centralizadas. **Cuando no hay espacio suficiente mientras se realiza la copia de seguridad** El archivo comprimido se limpiará únicamente durante la realización de la copia de seguridad y sólo si no hay espacio suficiente para crear una copia de seguridad nueva. En este caso, el programa actuará de la siguiente manera: ▪ Eliminará la copia de seguridad más antigua y todas las copias de seguridad incrementales/diferenciales dependientes. ▪ Si queda sólo una copia de seguridad completa y otra está en progreso, eliminará la última copia de seguridad completa y todas las copias de seguridad incrementales/diferenciales dependientes ▪ Si queda sólo una copia de seguridad completa y hay una copia de seguridad incremental o diferencial en progreso, se producirá un error que le indicará que no hay espacio disponible Se recomienda esta configuración para realizar copias de seguridad en una unidad USB o Acronis Secure Zone. Esta configuración no se aplica a bóvedas gestionadas. Esta configuración permite la eliminación de la última copia de seguridad en el archivo comprimido, en caso de que su dispositivo de almacenamiento no pueda incluir más de una copia de seguridad. Sin embargo, si por alguna razón el programa no puede crear la copia de seguridad nueva, podría quedarse sin copias de seguridad.
Aplicar las reglas (solo si las reglas de retención están configuradas)	Especifica cuándo aplicar las reglas de retención (pág. 32). Por ejemplo, el procedimiento de limpieza puede configurarse para que se ejecute después de cada copia de seguridad y según la programación. Esta opción estará disponible únicamente si ha configurado al menos una regla de retención en **Reglas de retención**.
Programación de limpieza (solo si la opción **Según programación** está seleccionada)	Especifica una programación para la limpieza del archivo comprimido. Por ejemplo, la limpieza puede programarse para que comience el último día de cada mes. Esta opción estará disponible únicamente si ha seleccionado **Según programación** en **Aplicar las reglas**.

Ejemplos

Copia de seguridad completa semanal

El siguiente esquema genera una copia de seguridad completa que se realiza todos los viernes por la noche.

Copia de seguridad completa: **Programación: Semanalmente**, todos los **viernes**, a las **22:00.**

Aquí, todos los parámetros de **Copia de seguridad completa** quedan vacíos, excepto **Programar**. Todas las copias de seguridad se conservan indefinidamente en el archivo comprimido (no se realizan limpiezas del archivo).

Copia de seguridad incremental y completa más limpieza

Con el siguiente esquema, el archivo comprimido constará de copias de seguridad completas semanales e incrementales diarias. Más allá de eso, necesitamos que una copia de seguridad completa tenga lugar únicamente una vez que todos los usuarios hayan cerrado sesión.

Copia de seguridad completa: Programación: Semanal, cada **viernes** a las **22:00**

Copia de seguridad completa: Condiciones: El usuario ha cerrado sesión

Incremental: Programación: Semanal, cada día laborable a las **21:00**

Permita también que todas las copias de seguridad que tengan más de un año se eliminen del archivo comprimido, así como la realización de una limpieza que finalice con la creación de una nueva copia de seguridad.

Reglas de retención: Eliminar las copias de seguridad que tengas más de **12 meses**

Aplicar las reglas: Después de realizar la copia de seguridad

De manera predeterminada, no se eliminará una copia de seguridad completa a menos que se eliminen todas las copias de seguridad incrementales que dependen de ella. Para obtener más información, consulte Reglas de retención (pág. 32).

Copias de seguridad mensuales completas, semanales diferenciales y diarias incrementales más limpieza

Este ejemplo demuestra el uso de todas las opciones disponibles en el esquema personalizado.

Supongamos que necesitamos un esquema para generar copias de seguridad completas mensuales, diferenciales semanales e incrementales diarias. La programación de copia de seguridad podría ser la siguiente:

Copia de seguridad completa: **Programación: Mensualmente**, todos los **últimos domingos** del mes, a las **21:00.**

Incremental: Programación: Diariamente, todos los **días hábiles**, a las **19:00.**

Diferencial: Programación: Semanalmente, todos los **sábados**, a las **20:00.**

Además, queremos añadir condiciones que deben cumplirse para que se inicie una tarea de copia de seguridad. Estas opciones se establecen en los campos **Condiciones** de cada tipo de copia de seguridad.

Copia de seguridad completa: **Condiciones**: **Ubicación disponible**

Incremental: **Condiciones**: **El usuario cerró la sesión**

Diferencial: **Condiciones**: **El usuario está inactivo**

Por ese motivo, la copia de seguridad completa. originalmente programada para las 21:00, podría comenzar más tarde: en cuanto la ubicación de la copia de seguridad esté disponible. Del mismo modo, las tareas de copia de seguridad para copias incrementales y diferenciales no se iniciarán hasta que todos los usuarios hayan cerrado sesión y estén inactivos, respectivamente.

Por último, creamos reglas de retención para el archivo comprimido: que se conserven solo las copias de seguridad que tengan menos de seis meses y que se realice una limpieza después de cada tarea de copia de seguridad y también el último día de cada mes.

Reglas de retención: Eliminar las copias de seguridad con más de **6 meses**

Aplicar las reglas: **Después de realizar la copia de seguridad**, **Según la programación**

Programación de limpieza: **Mensualmente**, el **Último día** de **Todos los meses**, a las **22:00.**

De manera predeterminada, una copia de seguridad no se eliminará siempre que tenga otras copias dependientes que deban conservarse. Por ejemplo: si una copia de seguridad completa puede eliminarse, pero hay otras copias incrementales o diferenciales que dependen de ella, la eliminación se pospone hasta que también se puedan eliminar todas las copias de seguridad dependientes.

Para obtener más información, consulte Reglas de retención (pág. 32).

Tareas resultantes

Todos los esquemas personalizados originan siempre tres tareas de la copia de seguridad y, en caso de que se especifiquen las reglas de retención, una tarea de limpieza. Cada tarea se detalla en la lista de tareas como **Programada** (si se ha configurado la programación) o como **Manual** (si no se ha configurado la programación).

Puede ejecutar cualquier tarea de copia de seguridad o limpieza en cualquier momento, sin importar si se encuentra programada.

En el primero de los ejemplos anteriores, configuramos una programación únicamente para copias de seguridad completas. Sin embargo, el esquema seguirá originando tres tareas de copia de seguridad, permitiéndole así realizar manualmente una copia de seguridad de cualquier tipo:

- Copia de seguridad completa, se ejecuta cada viernes a las 22:00
- Copia de seguridad incremental, se ejecuta manualmente
- Copia de seguridad diferencial, se ejecuta manualmente

Puede ejecutar cualquiera de estas tareas de copia de seguridad al seleccionarlas en la lista de tareas en la sección **Planes y tareas de la copia de seguridad** situada en el panel izquierdo.

Si también ha especificado las reglas de retención en su esquema de copia de seguridad, el esquema originará cuatro tareas: tres tareas de copia de seguridad y una tarea de limpieza.

6.2.11 Validación de archivos comprimidos

Configure la validación de la tarea para comprobar si los datos de la copia de seguridad pueden recuperarse. Si la copia de seguridad no finaliza la validación correctamente, la tarea de validación falla y el plan de copias de seguridad establecerá su estado en Error.

Para configurar la validación, especifique los siguientes parámetros

1. **Cuándo validar**: seleccione cuándo realizar la validación. Ya que la validación es una operación que utiliza muchos recursos, puede ser conveniente **programar** la validación en el periodo de menor actividad del equipo gestionado. Por otro lado, si la validación es uno de los elementos clave de su estrategia de protección de datos y prefiere que se le notifique inmediatamente en el caso de que los datos de la copia de seguridad no estén dañado y puedan recuperarse correctamente, considere la posibilidad de comenzar la validación inmediatamente después de la creación de la copia de seguridad.
2. **Qué validar**: seleccione validar el archivo comprimido al completo o su última copia de seguridad en el archivo comprimido. La validación de la copia de seguridad de un archivo simula la recuperación de todos los archivos de la copia de seguridad a un destino ficticio La validación de la copia de seguridad del volumen calcula la suma de comprobación para cada bloque de datos guardados en la copia de seguridad. La validación del archivo comprimido validará todas las copias de seguridad de los archivos comprimidos y podría llevar un tiempo considerable y agotar muchos recursos.
3. **Programación de la validación** (aparece únicamente si ha seleccionado según programación en el paso 1): configure la programación de la validación. Para obtener más información, consulte la sección Programación (pág. 85).

6.3 Recuperación de datos

En cuanto a la recuperación de datos, en primer lugar deberá considerar el método más funcional: conecte la consola al **equipo gestionado que ejecuta el sistema operativo** y cree la tarea de recuperación.

Si el **sistema operativo del equipo gestionado no se puede iniciar** o necesita **recuperar datos desde cero**, inicie el equipo desde el dispositivo de inicio (pág. 195)o utilizando Acronis Startup Recovery Manager (pág. 42). Después, cree una tarea de recuperación.

Antes de recuperar los dispositivos RAID de Linux, conocidos como **dispositivos MD**, o los dispositivos creados por el Administrador de volúmenes lógicos (LVM), conocidos como **volúmenes lógicos**, es necesario crear la estructura del volumen correspondiente antes de comenzar la recuperación. Para obtener información sobre cómo hacerlo, consulte "Recuperación de los dispositivos MD y los volúmenes lógicos (pág. 180)".

Para crear una tarea de recuperación, realice los siguientes pasos

General

Nombre de la tarea

[Opcional] Introduzca un nombre único para la tarea de recuperación. Un nombre pensado deliberadamente le permite identificar de manera rápida una tarea entre las demás.

Credenciales de la tarea (pág. 140)

[Opcional] La tarea se ejecutará en nombre del usuario que cree la tarea. De ser necesario, podrá cambiar las credenciales de la cuenta de la tarea. Para acceder a esta opción, seleccione la casilla de verificación **Vista avanzada**.

Qué recuperar

Archivo comprimido (pág. 140)

Seleccione el archivo comprimido del que desea recuperar datos.

Tipo de datos (pág. 141)

Se aplica a: recuperación de discos

Elija el tipo de datos que necesita recuperar de la copia de seguridad del disco seleccionada.

Contenido (pág. 141)

Seleccione la copia de seguridad y el contenido que desea recuperar.

Credenciales de acceso (pág. 142)

[Opcional] Proporcione las credenciales para la ubicación del archivo comprimido si la cuenta de la tarea no tiene derecho para acceder a ésta. Para acceder a esta opción, marque la casilla de verificación **Vista avanzada**.

Dónde recuperar:

Esta sección aparece después de seleccionar la copia de seguridad necesaria y definir el tipo de datos que se desea recuperar. Los parámetros que especifique aquí dependerán del tipo de datos que se recuperen.

Discos

Volúmenes

Archivos (pág. 146)

Es posible que tenga que especificar las credenciales para el destino. Omita este paso cuando opere en un equipo iniciado con un dispositivo de inicio.

Credenciales de acceso (pág. 148)

[Opcional] Proporcione las credenciales para el destino si las credenciales de la tarea no permiten recuperar los datos seleccionados. Para acceder a esta opción, marque la casilla de verificación **Vista avanzada**.

Cuándo recuperar

Recuperar (pág. 148)

Seleccione cuándo desea iniciar la recuperación. La tarea puede iniciarse inmediatamente después de su creación, programarse para una determinada fecha y hora en el futuro o simplemente guardarse para su ejecución manual.

Opciones de recuperación

Configuraciones

[Opcional] Para personalizar la operación de recuperación, configure las opciones de recuperación, como los comandos pre/post recuperación, la prioridad de recuperación, el manejo de errores o las opciones de notificación. Si no hace nada en esta sección, se usarán los valores predeterminados (pág. 68).

Después de que se modifique cualquiera de las configuraciones con respecto al valor predeterminado, aparecerá una nueva línea que mostrará el valor recientemente establecido. El estado de la configuración cambia de **Predeterminada** a **Personalizada**. Si modifica nuevamente la configuración, la línea mostrará el nuevo valor, a menos que el nuevo valor sea el predeterminado. Cuando se establece el valor predeterminado, la línea desaparece, de modo que siempre verá sólo la configuración que difiere de los valores predeterminados en la sección **Configuración**.

Al hacer clic en **Restablecer a los valores predeterminados**, se restablece la configuración a los valores predeterminados.

Una vez que haya completado todos los pasos necesarios, haga clic en **Aceptar** para ejecutar la creación de la tarea de recuperación.

6.3.1 Credenciales de la tarea

Proporcione las credenciales para la cuenta con la que se ejecutará la tarea.

Para especificar las credenciales

1. Seleccione una de las siguientes opciones:
   - **Ejecutar con el usuario actual**

     La tarea se ejecutará con las credenciales de la cuenta con la que el usuario que inicia las tareas haya iniciado la sesión. Si la tarea debe ejecutarse según la programación, se le solicitará la contraseña del usuario actual al finalizar la creación de la tarea.
   - **Utilizar las siguientes credenciales**

     La tarea se ejecutará siempre con las credenciales que especifique, ya sea que se inicie manualmente o según la programación.

     Especifique:
     - **Nombre de usuario**. Cuando introduzca el nombre de una cuenta de usuario de Active Directory, asegúrese de especificar también el nombre del dominio (DOMINIO\NombreDeUsuario o NombreDeUsuario@dominio)
     - **Contraseña**. La contraseña de la cuenta.
2. Haga clic en **Aceptar**.

Para obtener más información sobre cómo utilizar las credenciales para Acronis Backup & Recovery 10, consulte la sección Propietarios y credenciales (pág. 23).

Para obtener más información sobre las operaciones disponibles según los privilegios del usuario, consulte la sección Privilegios de usuario en un equipo gestionado (pág. 23).

6.3.2 Selección de archivos comprimidos

Selección del archivo comprimido

1. Introduzca la ruta completa a la ubicación en el campo **Ruta** o seleccione la carpeta deseada en el árbol de carpetas.
   - Si el archivo comprimido se almacena en Acronis Online Backup Storage, haga clic en **Iniciar sesión** y especifique las credenciales de acceso al almacenamiento en línea. Después, expanda el grupo **Almacenamiento de copia de seguridad en línea** y seleccione la cuenta.

   Las copias de seguridad almacenadas en Acronis Online Backup Storage no son aptas para la exportación ni el montaje.
   - Si el archivo comprimido está almacenado en una bóveda centralizada, expanda el grupo **Centralizada** y haga clic en la bóveda.
   - Si el archivo comprimido está almacenado en una bóveda personal, expanda el grupo **Personal** y haga clic en la bóveda.
   - Si el archivo comprimido está almacenado en una carpeta local en el equipo, expanda en grupo **Carpetas locales** y haga clic en la carpeta correspondiente.

   Si el archivo comprimido se encuentra en un medio extraíble como, por ejemplo, un DVD, introduzca primero el último DVD y, a continuación, los discos en orden comenzando por el primero cuando el programa le pregunte.

- Si el archivo comprimido se encuentra en una red compartida, expanda el grupo **Carpetas de red** y, a continuación, seleccione el equipo en red correspondiente y haga clic en la carpeta compartida. Si la red compartida requiere credenciales de acceso, el programa se las solicitará.

Nota para los usuario de Linux: *Para especificar una red compartida de sistema de archivos de Internet común (CIFS) que esté montada en un punto de montaje como /mnt/share, seleccione este punto de montaje en lugar de la propia red compartida.*

- Si el archivo comprimido se encuentra en un servidor **FTP** o **SFTP**, escriba el nombre o la dirección del servidor en el campo **Ruta** tal y como se indica a continuación:

  ftp://ftp_server:port _number o sftp://sftp_server:port number

  Si no se especifica el número del puerto, se utilizará el puerto 21 para FTP y el puerto 22 para SFTP.

  Tras introducir las credenciales de acceso, las carpetas en el servidor estarán disponible. Haga clic en la carpeta correspondiente del servidor.

  Puede acceder al servidor como usuario anónimo, si el servidor permite ese tipo de acceso. Para esto, haga clic en **Usar acceso anónimo** en lugar de introducir las credenciales.

Como se muestra en la especificación FTP original, los credenciales necesarios para acceder a los servidores FTP se transfieren a través de la red como texto sin formato. Esto significa que una persona no deseada puede interceptar el nombre de usuario y la contraseña utilizando un comprobador de paquetes.

- Si el archivo comprimido se encuentra en un dispositivo de cinta conectado localmente, expanda el grupo **Dispositivos de cinta** y haga clic en el dispositivo correspondiente.

Cuando opere en un equipo iniciado con un dispositivo de inicio:

- Para acceder a la bóveda gestionada, escriba la siguiente cadena en el campo **Ruta**:

  bsp://dirección_nodo/nombre_bóveda/

- Para acceder a una bóveda centralizada sin gestionar, escriba la ruta completa de la carpeta de la bóveda.

2. En la tabla ubicada a la derecha del árbol, seleccione el archivo comprimido. La tabla muestra los nombres de los archivos comprimidos contenidos en cada una de las bóvedas/carpetas que seleccione.

   Mientras usted revisa el contenido de la ubicación, otro usuario o el mismo programa pueden añadir, eliminar o modificar archivos comprimidos de acuerdo con las operaciones programadas. Utilice el botón **Actualizar** para actualizar la lista de archivos comprimidos.
3. Haga clic en **Aceptar**.

6.3.3 Tipo de datos

Elija el tipo de datos para recuperar de la copia de seguridad del disco seleccionada.

- **Discos**: para recuperar discos
- **Volúmenes**: para recuperar volúmenes
- **Archivos**: para recuperar archivos y carpetas específicos

6.3.4 Selección del contenido

La representación de esta ventana depende del tipo de datos almacenados en el archivo comprimido.

Selección de discos/volúmenes

Para seleccionar una copia de seguridad y los discos/volúmenes para recuperar:

1. Seleccione una de las copias de seguridad sucesivas según su fecha y hora de creación. De este modo, puede revertir los datos del disco a un momento determinado.

   Especifique los elementos para recuperar. De manera predeterminada, se seleccionarán todos los elementos de la copia de seguridad seleccionada. Si no desea recuperar determinados elementos, simplemente desmárquelos.
   Para obtener información sobre un disco/volumen, haga clic con el botón secundario sobre éste y después haga clic en **Información**.
2. Haga clic en **Aceptar**.

Selección de un MBR

Por lo general, seleccionará el MBR del disco si:

- El sistema operativo no puede iniciarse.
- El disco es nuevo y no cuenta con un MBR.
- Desea recuperar cargadores de inicio personalizados o que no sean de Windows (como LILO y GRUB).
- La geometría del disco es diferente de la almacenada en la copia de seguridad.

Es probable que haya otros casos en que necesite recuperar el MBR, pero los anteriores son los más comunes.

Al recuperar el MBR de un disco en otro, Acronis Backup & Recovery 10 recupera la pista 0, que no afecta la tabla de partición ni la distribución de la partición del disco de destino. Acronis Backup & Recovery 10 actualiza automáticamente los cargadores de Windows después de la recuperación, de modo que no es necesario recuperar el MBR y la pista 0 para los sistemas Windows, a menos que el MBR esté dañado.

Selección de archivos

Para seleccionar una copia de seguridad y los archivos que se van a recuperar:

1. Seleccione una de las copias de seguridad sucesivas según su fecha/hora de creación. De esta manera, puede revertir los archivos/carpetas a un momento determinado.
2. Especifique los archivos y carpetas para recuperar al seleccionar las casillas de verificación correspondientes en el árbol de archivos comprimidos.

   Al seleccionar una carpeta, automáticamente se selecciona la totalidad de sus carpetas y archivos anidados.

   Utilice la tabla ubicada a la derecha del árbol de archivos comprimidos para seleccionar los elementos anidados. Al seleccionar la casilla de verificación del encabezado de la columna **Nombre**, se seleccionan automáticamente todos los elementos de la tabla. Al desmarcar esta casilla de verificación, se anula automáticamente la selección de todos los elementos.
3. Haga clic en **Aceptar**.

6.3.5 Credenciales de acceso para la ubicación

Especifique las credenciales necesarias para acceder a la ubicación donde está almacenado el archivo de copia de seguridad.

Para especificar las credenciales

1. Seleccione una de las siguientes opciones:

- **Utilizar las credenciales de la tarea**

  El programa accederá a la ubicación utilizando las credenciales de la cuenta de la tarea especificada en la sección General.

- **Utilizar las siguientes credenciales**

  El programa accederá a la ubicación utilizando las credenciales que especifique. Utilice esta opción si la cuenta de la tarea no dispone de permisos de acceso a la ubicación. Quizás necesite atribuir credenciales especiales para una red compartida o para una bóveda de nodo de almacenamiento.

  Especifique:

  - **Nombre de usuario**. Cuando introduzca el nombre de una cuenta de usuario de Active Directory, asegúrese de especificar también el nombre del dominio (DOMINIO\NombreDeUsuario o NombreDeUsuario@dominio)
  - **Contraseña**. La contraseña de la cuenta.

2. Haga clic en **Aceptar**.

Como se muestra en la especificación FTP original, los credenciales necesarios para acceder a los servidores FTP se transfieren a través de la red como texto sin formato. Esto significa que una persona no deseada puede interceptar el nombre de usuario y la contraseña utilizando un comprobador de paquetes.

6.3.6 Selección del destino

Especifique el destino en el cual se recuperarán los datos seleccionados.

Discos

La disponibilidad de los destinos de discos depende de los agentes que funcionan en el equipo.

Recuperar a:

Equipo físico

Los discos seleccionados se recuperarán en los discos físicos del equipo al que esté conectada la consola. Al seleccionar esta opción, continuará con el procedimiento regular de asignación de discos que se describe a continuación.

N.° de disco:

N.° de disco (MODELO) (pág. 145)

Seleccione el disco de destino para cada uno de los discos de origen.

Firma NT (pág. 144)

Seleccione el modo en que se gestionará la firma del disco recuperado. La firma del disco es utilizada por Windows, y por la versión 2.6 y versiones posteriores del kernel de Linux.

Destino del disco

Para especificar un disco de destino:

1. Seleccione el disco donde desea recuperar el disco seleccionado. El espacio del disco de destino debe tener al menos el mismo tamaño que los datos de la imagen sin comprimir.
2. Haga clic en **Aceptar**.

Todos los datos almacenados en el disco de destino se reemplazarán con los datos incluidos en la copia de seguridad; por lo tanto, tenga cuidado y controle si tiene datos sin copia de seguridad que pueda necesitar.

Firma NT

Cuando se selecciona el MBR junto con la copia de seguridad del disco, debe retener la capacidad de inicio del sistema operativo en el volumen del disco de destino. El sistema operativo debe tener la información de volumen del sistema (p. ej., la letra del volumen) coincidente con la firma NT del disco que se mantiene en el registro del disco MBR. Pero dos discos con la misma firma NT no pueden funcionar de manera correcta en un sistema operativo.

Si hay dos discos que tienen la misma firma NT e incluyen un volumen del sistema en un equipo, al inicio el sistema operativo se ejecuta desde el primer disco, descubre la misma firma en el segundo, genera de manera automática una nueva firma NT única y se la asigna al segundo disco. Como resultado, todos los volúmenes del segundo disco perderán sus letras, todas las rutas serán inválidas en el disco y los programas no encontrarán sus archivos. El sistema operativo de ese disco no se iniciará.

Para retener la capacidad de inicio del sistema en el volumen del disco de destino, elija una de las siguientes opciones:

- **Seleccione automáticamente**

  Se creará una nueva firma NT sólo si la existente difiere de la que se encuentra en la copia de seguridad. De lo contrario, se mantendrá la firma NT existente.

- **Crear nuevo**

  El programa generará una nueva firma NT para la unidad de disco duro de destino.

- **Recuperar a partir de la copia de seguridad**

  El programa reemplazará la firma NT del disco duro de destino por una de la copia de seguridad del disco.

  Puede que desee recuperar la firma del disco por las siguientes razones:

  - Acronis Backup & Recovery 10 crea tareas programadas usando la firma del disco duro de origen. Si recupera la misma firma del disco, no necesita volver a crear o editar las tareas que creó anteriormente.
  - Algunas aplicaciones instaladas utilizan la firma del disco para fines de licencias y otros fines.

- **Mantener los existentes**

  El programa dejará la firma NT existente del disco duro de destino tal como está.

Volúmenes

La disponibilidad de los destinos de volúmenes depende de los agentes que funcionan en el equipo.

Recuperar a:

Equipo físico

Los volúmenes seleccionados se recuperarán en los discos físicos del equipo al que esté conectada la consola. Al seleccionar esta opción, continuará con el procedimiento regular de asignación de volúmenes que se describe a continuación.

Recuperar [Nº de disco] MBR en: [Si se selecciona el Registro de inicio maestro (MBR) para la recuperación]

N° de disco: (pág. 145)

Escoja el disco donde recuperar el Registro de inicio maestro (MBR).

Firma NT: (pág. 144)

Seleccione la forma en la que se gestionará la firma del disco que se encuentra en el MBR. La firma del disco es utilizada por Windows, y por la versión 2.6 y versiones posteriores del kernel de Linux.

Recuperar [Volumen] en:

N.° de disco/Volumen (pág. 145)

Asigne de manera secuencial cada uno de los volúmenes de origen a un volumen o espacio no asignado del disco de destino.

Tamaño:

[Opcional] Cambie el tamaño, la ubicación y otras propiedades del volumen recuperado.

Destino MBR

Para especificar un disco de destino:

1. Seleccione el disco en el que desea recuperar el MBR.
2. Haga clic en **Aceptar**.

Destino del volumen

Para especificar un volumen de destino:

1. Seleccione un volumen o espacio no asignado donde desee que se recupere el volumen seleccionado. El volumen/espacio no asignado de destino deberá tener al menos el mismo tamaño que los datos de la imagen sin comprimir.
2. Haga clic en **Aceptar**.

Todos los datos almacenados en el volumen de destino se reemplazarán con los datos incluidos en la copia de seguridad; por lo tanto, tenga cuidado y controle si tiene datos sin copia de seguridad que pueda necesitar.

Cuando utilice un dispositivo de inicio

Las letras de los discos que se ven en los dispositivos de inicio de estilo Windows pueden diferir de la manera en que Windows identifica las unidades. Por ejemplo, la unidad D: de la utilidad de rescate puede corresponder a la unidad E: de Windows.

¡Cuidado! Para estar seguro, se aconseja asignar nombres únicos a los volúmenes.

Los dispositivos de inicio de estilo Linux muestran los discos y volúmenes locales como desmontados (sda1, sda2...).

Propiedades del volumen

Cambios de tamaño y ubicación

Al recuperar un volumen en un disco MBR básico, puede cambiar el tamaño y la ubicación del volumen al arrastrarlo o arrastrar sus bordes con el ratón, o al introducir los valores correspondientes en los campos apropiados. Al utilizar esta función, puede redistribuir el espacio de disco entre los volúmenes que se están recuperando. En este caso, deberá recuperar primero el volumen que se reducirá.

Consejo: *El tamaño de un volumen no puede modificarse cuando se recupera desde una copia de seguridad dividida en múltiples DVD o cintas. Para poder modificar el tamaño de un volumen, copie todas las partes de la copia de seguridad en una ubicación única en un disco duro.*

Propiedades

Tipo

Un disco MBR básico puede contener hasta cuatro volúmenes primarios o hasta tres volúmenes primarios, y varias unidades lógicas. De manera predeterminada, el programa selecciona el tipo del volumen original. Si fuera necesario, puede cambiar esta configuración.

- **Primarios**. La información sobre los volúmenes primarios está incluida en la tabla de partición del MBR. La mayoría de los sistemas operativos puede iniciarse solo desde el volumen primario del primer disco duro, pero la cantidad de volúmenes primarios es limitada.

  Si desea recuperar un volumen del sistema en un disco MBR básico, seleccione la casilla de verificación Activo. El volumen activo se usa para cargar un sistema operativo. Elegir la opción Activo para un volumen sin un sistema operativo instalado puede impedir el inicio del equipo. No puede establecer una unidad lógica o un volumen dinámico como activos.
- **Lógicos**. La información sobre los volúmenes lógicos no se encuentra en el MBR, sino en la tabla de partición extendida. La cantidad de volúmenes lógicos de un disco es ilimitada. Un volumen lógico no puede establecerse como activo. Si recupera un volumen del sistema en otro disco duro con sus propios volúmenes y sistema operativo, probablemente solo necesitará los datos. En este caso, puede recuperar el volumen como lógico para acceder únicamente a los datos.

Sistema de archivos

Si fuera necesario, cambie el sistema de archivos del volumen. De manera predeterminada, el programa selecciona el sistema de archivos del volumen original. Acronis Backup & Recovery 10 puede realizar las siguientes conversiones de sistemas de archivos: FAT 16 -> FAT 32 y Ext2 -> Ext3. Para volúmenes con otros sistemas de archivos nativos, esta opción no está disponible.

Supongamos que desea recuperar el volumen de un disco FAT16 antiguo y de poca capacidad en un disco más nuevo. FAT16 no sería efectivo y podría incluso ser imposible configurar en el disco duro de alta capacidad. Esto sucede porque FAT16 es compatible con volúmenes de hasta 4 GB, de manera que no podrá recuperar un volumen FAT16 de 4 GB en un volumen que exceda ese límite sin cambiar el sistema de archivos. En este caso, sería necesario cambiar el sistema de archivos de FAT16 a FAT32.

Los sistemas operativos más antiguos (MS-DOS, Windows 95 y Windows NT 3.x, 4.x) no son compatibles con FAT32 y no funcionarán después de recuperar un volumen y cambiar su sistema de archivos. Normalmente, estos sistemas solamente pueden recuperarse en un volumen FAT16.

Letra de unidad lógica (únicamente para Windows)

Asigne una letra al volumen recuperado. Seleccione la letra que desee de una lista desplegable.

- Con la selección AUTOMÁTICA predeterminada, la primera letra que no esté en uso será asignada al volumen.
- Si selecciona NO, no se asignará ninguna letra al volumen recuperado y se lo ocultará del sistema operativo. No debe asignar letras a volúmenes inaccesibles para Windows, como las que no son FAT o NTFS.

Destino del archivo

Para especificar un destino:

1. Seleccione una ubicación en la que se recuperarán los archivos incluidos en la copia de seguridad:
   - **Ubicación original:** los archivos y carpetas se recuperarán con la(s) misma(s) ruta(s) que tenían en la copia de seguridad. Por ejemplo, si realizó una copia de seguridad de todos los

archivos y carpetas en C:\Documentos\Finanzas\Informes\, los archivos se recuperarán con la misma ruta. Si la carpeta no existe, se creará automáticamente.

- **Nueva ubicación**: los archivos se recuperarán en la ubicación que especifique en el árbol. Los archivos y carpetas se recuperarán sin volver a crear una ruta completa, a menos que desmarque la casilla de verificación **Recuperar sin la ruta completa**.

2. Haga clic en **Aceptar**.

Exclusiones de la recuperación

Configure exclusiones para los archivos específicos que no desea recuperar.

Utilice los botones **Agregar**, **Editar**, **Eliminar** y **Eliminar todo** para crear la lista de máscaras de archivos. Durante la recuperación, se pasarán por alto los archivos cuyos nombres coincidan con alguna de las máscaras.

Puede utilizar uno o más caracteres comodín * y ? en una máscara de archivo:

- El asterisco (*) sustituye de cero a más caracteres del nombre del archivo; por ejemplo, la máscara de archivo Doc*.txt genera archivos Doc.txt y Document.txt
- El signo de interrogación (?) substituye a un único carácter; por ejemplo, la máscara de archivo Doc?.txt genera archivos Doc1.txt y Docs.txt, pero, por el contrario, no general archivos Doc.txt o Doc11.txt

Ejemplos de exclusión

Criterio	Ejemplo	Descripción
Windows y Linux		
Por nombre	F.log F	Excluye todos los archivos denominados "F.log" Excluye todas las carpetas denominadas "F"
Por máscara (*)	*.log F*	Excluye todos los archivos con la extensión .log Excluye todos los archivos y carpetas cuyos nombres comiencen con "F" (como carpetas F, F1 y archivos F.log, F1.log)
Por máscara (?)	F???.log	Excluye todos los archivos .log cuyos nombres contengan cuatro símbolos y comiencen con "F"
Windows		
Por ruta de archivo	Finance\F.log	Excluye los archivos denominados "F.log" de todas las carpetas con el nombre "Finance"
Por ruta de carpeta	Finance\F\ o Finance\F	Excluye las carpetas denominadas "F" de todas las carpetas con el nombre "Finance"
Linux		
Por ruta de archivo	/home/user/Finance/F.log	Excluye el archivo denominado "F.log", ubicado en la carpeta /home/user/Finance

Las configuraciones anteriores no se realizarán para los archivos o carpetas que se seleccionaron explícitamente para la recuperación. Por ejemplo, supongamos que seleccionó la carpeta MiCarpeta y el archivo MiArchivo.tmp fuera de esa carpeta, y seleccionó la opción de omitir todos los archivos

.tmp. En este caso, todos los archivos .tmp de la carpeta MiCarpeta serán omitidos durante el proceso de recuperación, pero no se omitirá el archivo MiArchivo.tmp.

Sobrescritura

Elija qué hacer si el programa encuentra un archivo en la carpeta de destino que tenga el mismo nombre que el que se encuentra en el archivo comprimido:

- **Sobrescribir el archivo existente**: esto le dará prioridad al archivo de la copia de seguridad sobre el archivo del disco duro
- **Sobrescribir el archivo existente en caso de que sea anterior**: esto le dará prioridad a la modificación más reciente del archivo, ya sea que se haya realizado en la copia de seguridad o en el disco.
- **No sobrescribir el archivo existente**: esto le dará prioridad al archivo del disco duro sobre el archivo de la copia de seguridad.

Si permite que los archivos se sobrescriban, aún tiene la opción de evitar la sobrescritura de archivos específicos excluyéndolos (pág. 147) de la operación de recuperación.

6.3.7 Credenciales de acceso para el destino

Para especificar las credenciales

1. Seleccione una de las siguientes opciones:
   - **Utilizar las credenciales de la tarea**

     El programa accederá al destino utilizando las credenciales de la cuenta de la tarea especificada en la sección General.
   - **Utilice las siguientes credenciales.**

     El programa accederá al destino utilizando las credenciales que usted especifique. Utilice esta opción si la cuenta de la tarea no tiene permisos de acceso para el destino.

     Especifique:
     - **Nombre de usuario**. Cuando introduzca el nombre de una cuenta de usuario de Active Directory, asegúrese de especificar también el nombre del dominio (DOMINIO\NombreDeUsuario o NombreDeUsuario@dominio)
     - **Contraseña**. La contraseña de la cuenta.
2. Haga clic en **Aceptar**.

6.3.8 Cuándo recuperar

Seleccione cuándo desea iniciar la tarea de recuperación:

- **Recuperar ahora**: la tarea de recuperación se iniciará inmediatamente después de que haga clic en **Aceptar**, en el paso final.
- **Recuperar más tarde**: la tarea de recuperación se iniciará en la fecha y hora que especifique.

Si no necesita programar la tarea y desea iniciarla manualmente después, seleccione la casilla de verificación **La tarea se iniciará manualmente (no programe la tarea)**.

6.3.9 Montaje de dispositivos MD para recuperación (Linux)

En Linux, cuando se realiza la recuperación desde una copia de seguridad de disco a un dispositivo MD existente (también llamado Linux Software RAID), asegúrese de que este **dispositivo esté montado** al momento de la recuperación.

Si el dispositivo no está montado, móntelo utilizando la utilidad **mdadm**. He aquí dos ejemplos:

Ejemplo 1. El siguiente comando monta el dispositivo /dev/md0 combinado de volúmenes /dev/sdb1 y /dev/sdc1:

```
mdadm --assemble /dev/md0 -ayes /dev/sdb1 /sdc1
```

Ejemplo 2. El siguiente comando monta el dispositivo /dev/md0 combinado de volúmenes /dev/sdb1 y /dev/sdc1:

```
mdadm --assemble /dev/md0 -ayes /dev/sdb /dev/sdc
```

Si la recuperación requiere reiniciar el equipo (normalmente, cuando los volúmenes a recuperar incluyen la partición de inicio) siga las siguientes directrices:

- Si todas las partes del dispositivo MD son volúmenes (un caso típico como en el primer ejemplo), asegúrese que el tipo de cada volumen —llamado tipo de partición o ID del sistema—sea **Linux raid automontaje**; el código hexadecimal de este tipo de partición es 0xFD. Esto garantizará que el dispositivo se montará de modo automático luego de reiniciar la máquina. Para ver o cambiar el tipo de partición, utilice una utilidad de particionamiento de disco como **fdisk**.
- En caso contrario (como en el segundo ejemplo) realice la recuperación desde un dispositivo de inicio. No necesitará reiniciar en ese caso. . En dispositivos de inicio, puede que necesite crear el dispositivo MD de forma manual o automática, como se describe en Recuperación de dispositivos MD y volúmenes lógicos (pág. 180).

6.3.10 Solución de problemas de capacidad de inicio

Si un sistema era inicializable al momento de realizar una copia de seguridad, se espera que se inicie después de la recuperación. Sin embargo, la información que el sistema operativo almacena y utiliza para el inicio puede desactualizarse durante la recuperación, especialmente si cambia los tamaños de volúmenes, las ubicaciones o las unidades de destino. Acronis Backup & Recovery 10 actualiza de manera automática los cargadores de Windows después de la recuperación. También puede haber otros cargadores que sean fijos, pero en algunos casos es necesario reactivar los cargadores. Específicamente al recuperar volúmenes de Linux, se necesita a veces efectuar reparaciones o realizar cambios en el inicio para que Linux se pueda iniciar y cargar correctamente.

A continuación, encontrará un resumen de las situaciones típicas que requieren acciones adicionales por parte del usuario.

Por qué un sistema operativo recuperado no se inicia

- **El BIOS del equipo está configurado para iniciarse desde otro disco duro.**

  Solución: configure el BIOS para que se inicie desde el disco duro donde reside el sistema operativo.

- **El sistema se recuperó en un hardware diferente y el nuevo hardware es incompatible con la mayoría de los controladores más críticos incluidos en la copia de seguridad.**

  Solución para Windows: vuelva a recuperar el volumen. Al configurar la recuperación, opte por usar Acronis Universal Restore y especifique los controladores de HAL y almacenamiento masivo apropiados.

- **Windows se recuperó en un volumen dinámico que no puede iniciarse**

  Solución: recupere Windows en un volumen básico, simple o replicado.

- **Un volumen del sistema se recuperó en un disco que no tiene un MBR**

  Cuando configure la recuperación de un volumen del sistema en un disco que no tenga un MBR, el programa le preguntará si desea recuperar el MBR junto con el volumen del sistema. Opte por no recuperarlo, solo si no desea que el sistema sea inicializable.

  Solución: vuelva a recuperar el volumen junto con el MBR del disco correspondiente.

- **El sistema utiliza Acronis OS Selector**

  Como el registro de inicio maestro (MBR) puede cambiarse durante la recuperación del sistema, es posible que Acronis OS Selector, que utiliza el MBR, deje de funcionar. Si esto sucede, reactive Acronis OS Selector de la siguiente manera.

  Solución: inicie el equipo desde el dispositivo de inicio de Acronis Disk Director y seleccione en el menú **Herramientas -> Activar OS Selector**.

- **El sistema utiliza el cargador de inicio GRUB y se recuperó a partir de una copia de seguridad normal (no una copia sin procesar, es decir, sector por sector)**

  Una parte del cargador GRUB reside en los primeros sectores del disco o en los primeros sectores del volumen. El resto se encuentra en el sistema de archivos de uno de los volúmenes. La capacidad de inicio del sistema puede recuperarse automáticamente solo cuando el GRUB reside en los primeros sectores del disco y en el sistema de archivos al cual es posible tener acceso directo. En otros casos, el usuario debe reactivar el cargador de inicio manualmente.

  Solución: reactive nuevamente el cargador de inicio. También es posible que tenga que reparar el archivo de configuración.

- **El sistema utiliza el cargador de Linux (LILO) y se recuperó a partir de una copia de seguridad normal (no una copia sin procesar, es decir, sector por sector)**

  LILO contiene numerosas referencias a números de sectores absolutos; por lo tanto, no puede repararse automáticamente, excepto cuando todos los datos se recuperan en los sectores que tienen los mismos números absolutos que el disco de origen.

  Solución: reactive nuevamente el cargador de inicio. También es posible que tenga que reparar el archivo de configuración del cargador por el motivo descrito en el punto anterior.

- **El cargador del sistema apunta al volumen equivocado**

  Esto puede suceder cuando los volúmenes del sistema o de inicio no se recuperan en su ubicación original.

  Solución:

  La modificación de los archivos boot.ini o boot\bcd permite reparar este problema para los cargadores de Windows. Acronis Backup & Recovery 10 hace esto de forma automática; por lo tanto, es poco probable que tenga este problema.

  Para los cargadores GRUB y LILO, deberá corregir los archivos de configuración del GRUB. Si el número de la partición raíz de Linux cambió, también se recomienda cambiar /etc/fstab para poder acceder correctamente al volumen SWAP.

- **Linux se recuperó a partir de la copia de seguridad de un volumen LVM en un disco MBR básico**

  Este sistema no puede iniciarse porque su kernel intenta montar el sistema de archivos raíz en el volumen LVM.

  Solución: cambie la configuración del cargador y /etc/fstab para que LVM no se utilice, y active el cargador de inicio.

Cómo reactivar GRUB y cambiar su configuración

Por lo general, debe consultar las páginas del manual correspondientes a cargadores de inicio para conocer el procedimiento apropiado. También se encuentra el artículo correspondiente en la Base de Conocimientos en el sitio Web de Acronis.

El siguiente es un ejemplo de cómo reactivar GRUB en caso que el disco del sistema (volumen) sea recuperado en un hardware idéntico.

1. Inicie Linux o cárguelo desde el medio iniciable, y luego presione CTRL+ALT+F2.
2. Monte el sistema que está recuperando:

```
mkdir /mnt/system/
mount -t ext3 /dev/sda2 /mnt/system/ # root particion
mount -t ext3 /dev/sda1 /mnt/system/boot/ # boot particion
```

3. Corra los sistemas de archivo **proc** y **dev** para el sistema que está recuperando:

```
mount -t proc none /mnt/system/proc/
mount -o bind /dev/ /mnt/system/dev/
```

4. Guarde una copia del archivo de menú GRUB, ejecutando uno de los siguientes comandos:

```
cp /mnt/system/boot/grub/menu.lst /mnt/system/boot/grub/menu.lst.backup
```

o

```
cp /mnt/system/boot/grub/grub.conf /mnt/system/boot/grub/grub.conf.backup
```

5. Edite el archivo **/mnt/system/boot/grub/menu.lst** (para las distribuciones Debian, Ubuntu, y SUSE Linux) o el archivo **/mnt/system/boot/grub/grub.conf** (para las distribuciones Fedora y Linux Enterprise Red Hat), por ejemplo, como figura a continuación:

```
vi /mnt/system/boot/grub/menu.lst
```

6. En el archivo **menu.lst** (respectivamente **grub.conf**), encuentre el elemento del menú que corresponde al sistema que está recuperando. Los elementos de este menú tienen la siguiente forma:

```
title Red Hat Enterprise Linux Server(2.6.24.4)
      root (hd0,0)
      kernel /vmlinuz-2.6.24.4 ro root=/dev/sda2 rhgb quiet
      initrd /initrd-2.6.24.4.img
```

   Las líneas que comienzan con **título**, **raíz,kernel e initrd** determinan respectivamente:

   - El título del elemento del menú.
   - El dispositivo en el cual el núcleo Linux se encuentra: típicamente, la partición de inicio o la partición de raíz, como la **raíz (hd0,0)** en este ejemplo.
   - La ruta al núcleo en ese dispositivo y la partición de raíz: en este ejemplo, la ruta es **/vmlinuz-2.6.24.4** y la partición de raíz es **/dev/sda2**. Puede especificar la partición de raíz por etiqueta (como **root=LABEL=/**), identificador (en la forma **root=UUID=***some_uuid*), o nombre de dispositivo (como **root=/dev/sda2**).
   - La ruta al servicio **initrd** en dicho dispositivo.

7. Edite el archivo **/mnt/system/etc/fstab** para corregir los nombres de cualquier dispositivo que haya cambiado como resultado de la recuperación.
8. Inicie la shell de GRUB ejecutando uno de los siguientes comandos:

```
chroot /mnt/system/ /sbin/grub
```

   o

```
chroot /mnt/system/ /sbin/grub
```

9. Especifique el disco en el cual se ubica GRUB: generalmente, la partición de inicio o de raíz:

```
root (hd0,0)
```

10. Instalar GRUB. Por ejemplo, para GRUB en el registro de inicio maestro (MBR) del primer disco, ejecute el siguiente comando:

```
setup (hd0)
```

11. Salir del shell de GRUB:

```
quit
```

12. Desmontar los sistemas de archivos montados y luego reiniciar:

```
umount /mnt/system/dev/
umount /mnt/system/proc/
umount /mnt/system/boot/
umount /mnt/system/
reboot
```

13. Reconfigurar el cargador de arranque utilizando las herramientas y documentación de distribución Linux que usa. Por ejemplo, en Debian y Ubuntu, puede precisar editar algunas líneas comentadas en el archivo **/boot/grub/menu.lst** y luego ejecutar el script **update-grub**; caso contrario, los cambios pueden no resultar efectivos.

6.4 Validar bóvedas, archivos comprimidos y copias de seguridad

La validación es una operación que verifica la posibilidad de recuperación de datos en una copia de seguridad.

La validación de la copia de seguridad de un archivo imita la recuperación de todos los archivos de la copia de seguridad a un destino simulado. La validación de la copia de seguridad de un disco o volumen calcula la suma de comprobación por cada bloque de datos guardados en la copia de seguridad. Ambos procedimientos utilizan muchos recursos.

La validación de un archivo comprimido validará las copias de seguridad del archivo comprimido. La validación de una bóveda (o una ubicación) validará todos los archivos comprimidos almacenados en esta bóveda (ubicación).

Si bien una validación satisfactoria implica una gran probabilidad de recuperación exitosa, no verifica todos los factores que tienen influencia sobre el proceso de recuperación. Si realiza una copia de seguridad del sistema operativo, solo se podrá garantizar una recuperación exitosa con una recuperación de prueba en el entorno de inicio a una unidad de disco duro libre. Al menos, asegúrese de que la copia de seguridad pueda validarse correctamente utilizando el dispositivo de inicio.

Diferentes formas de crear una tarea de validación

La forma más general de crear una tarea de validación consiste en usar la página Validación. En esa página puede validar inmediatamente o establecer una programación de validación para cualquier copia de seguridad, archivo comprimido o ubicación a la cual tenga permitido acceder.

La validación de un archivo comprimido o de la copia de seguridad más reciente del archivo comprimido puede programarse como parte del plan de copia de seguridad. Para obtener más información, consulte la sección Creación de un plan de copia de seguridad (pág. 113).

Puede acceder a la página **Validación** desde la vista **Bóvedas** (pág. 77). Haga clic con el botón secundario en el objeto que desee validar (archivo comprimido, copia de seguridad o bóveda), y seleccione **Validar** del menú contextual. La página Validación se abrirá con el objeto preseleccionado

como origen. Solo tiene que seleccionar cuándo debe realizarse la validación y (opcionalmente) proporcionar un nombre para la tarea.

Para crear una tarea de validación, realice los siguientes pasos.

General

Nombre de la tarea

[Opcional] Introduzca un nombre único para la tarea de validación. Un nombre pensado deliberadamente le permite identificar de manera rápida una tarea entre las demás.

Credenciales (pág. 153)

[Opcional] La tarea de validación se ejecutará en nombre del usuario que cree la tarea. De ser necesario, podrá cambiar las credenciales de la tarea. Para acceder a esta opción, marque la casilla de verificación **Vista avanzada**.

Qué validar

Validar

Elija un objeto para validar:

Archivo comprimido (pág. 154): en ese caso, es necesario que especifique el archivo comprimido.

Copia de seguridad (pág. 155): especifique primero el archivo y después seleccione la copia de seguridad deseada en este archivo comprimido.

Bóveda (pág. 155): seleccione la bóveda (u otra ubicación) cuyos archivos comprimidos desee validar.

Credenciales de acceso (pág. 156)

[Opcional] Proporcione las credenciales para acceder al origen si la cuenta de la tarea no tiene suficientes privilegios para acceder a este. Para acceder a esta opción, seleccione la casilla de verificación **Vista avanzada**.

Cuándo validar

Validar (pág. 156)

Especifique cuándo y con qué frecuencia debe realizarse la validación.

Una vez que haya establecido la configuración necesaria, haga clic en **Aceptar** para crear la tarea de validación.

6.4.1 Credenciales de la tarea

Proporcione las credenciales para la cuenta con la que se ejecutará la tarea.

Para especificar las credenciales

1. Seleccione una de las siguientes opciones:
   - **Ejecutar con el usuario actual**

     La tarea se ejecutará con las credenciales de la cuenta con la que el usuario que inicia las tareas haya iniciado la sesión. Si la tarea debe ejecutarse según la programación, se le solicitará la contraseña del usuario actual al finalizar la creación de la tarea.
   - **Utilizar las siguientes credenciales**

     La tarea se ejecutará siempre con las credenciales que especifique, ya sea que se inicie manualmente o según la programación.

     Especifique:

- **Nombre de usuario**. Cuando introduzca el nombre de una cuenta de usuario de Active Directory, asegúrese de especificar también el nombre del dominio (DOMINIO\NombreDeUsuario o NombreDeUsuario@dominio)
- **Contraseña**. La contraseña de la cuenta.

2. Haga clic en **Aceptar**.

Para obtener más información sobre cómo utilizar las credenciales para Acronis Backup & Recovery 10, consulte la sección Propietarios y credenciales (pág. 23).

Para obtener más información sobre las operaciones disponibles según los privilegios del usuario, consulte la sección Privilegios de usuario en un equipo gestionado (pág. 23).

6.4.2 Selección de archivos comprimidos

Selección del archivo comprimido

1. Introduzca la ruta completa a la ubicación en el campo **Ruta** o seleccione la carpeta deseada en el árbol de carpetas.
   - Si el archivo comprimido se almacena en Acronis Online Backup Storage, haga clic en **Iniciar sesión** y especifique las credenciales de acceso al almacenamiento en línea. Después, expanda el grupo **Almacenamiento de copia de seguridad en línea** y seleccione la cuenta.

   Las copias de seguridad almacenadas en Acronis Online Backup Storage no son aptas para la exportación ni el montaje.

   - Si el archivo comprimido está almacenado en una bóveda centralizada, expanda el grupo **Centralizada** y haga clic en la bóveda.
   - Si el archivo comprimido está almacenado en una bóveda personal, expanda el grupo **Personal** y haga clic en la bóveda.
   - Si el archivo comprimido está almacenado en una carpeta local en el equipo, expanda en grupo **Carpetas locales** y haga clic en la carpeta correspondiente.

   Si el archivo comprimido se encuentra en un medio extraíble como, por ejemplo, un DVD, introduzca primero el último DVD y, a continuación, los discos en orden comenzando por el primero cuando el programa le pregunte.

   - Si el archivo comprimido se encuentra en una red compartida, expanda el grupo **Carpetas de red** y, a continuación, seleccione el equipo en red correspondiente y haga clic en la carpeta compartida. Si la red compartida requiere credenciales de acceso, el programa se las solicitará.

   Nota para los usuario de Linux: *Para especificar una red compartida de sistema de archivos de Internet común (CIFS) que esté montada en un punto de montaje como /mnt/share, seleccione este punto de montaje en lugar de la propia red compartida.*

   - Si el archivo comprimido se encuentra en un servidor **FTP** o **SFTP**, escriba el nombre o la dirección del servidor en el campo **Ruta** tal y como se indica a continuación:

     ftp://ftp_server:port _number o sftp://sftp_server:port number

     Si no se especifica el número del puerto, se utilizará el puerto 21 para FTP y el puerto 22 para SFTP.

     Tras introducir las credenciales de acceso, las carpetas en el servidor estarán disponible. Haga clic en la carpeta correspondiente del servidor.

     Puede acceder al servidor como usuario anónimo, si el servidor permite ese tipo de acceso. Para esto, haga clic en **Usar acceso anónimo** en lugar de introducir las credenciales.

Como se muestra en la especificación FTP original, los credenciales necesarios para acceder a los servidores FTP se transfieren a través de la red como texto sin formato. Esto significa que una persona no deseada puede interceptar el nombre de usuario y la contraseña utilizando un comprobador de paquetes.

- Si el archivo comprimido se encuentra en un dispositivo de cinta conectado localmente, expanda el grupo **Dispositivos de cinta** y haga clic en el dispositivo correspondiente.

Cuando opere en un equipo iniciado con un dispositivo de inicio:

- Para acceder a la bóveda gestionada, escriba la siguiente cadena en el campo **Ruta**:

  bsp://dirección_nodo/nombre_bóveda/
- Para acceder a una bóveda centralizada sin gestionar, escriba la ruta completa de la carpeta de la bóveda.

2. En la tabla ubicada a la derecha del árbol, seleccione el archivo comprimido. La tabla muestra los nombres de los archivos comprimidos contenidos en cada una de las bóvedas/carpetas que seleccione.

   Mientras usted revisa el contenido de la ubicación, otro usuario o el mismo programa pueden añadir, eliminar o modificar archivos comprimidos de acuerdo con las operaciones programadas. Utilice el botón **Actualizar** para actualizar la lista de archivos comprimidos.
3. Haga clic en **Aceptar**.

6.4.3 Selección de la copia de seguridad

Para especificar una copia de seguridad para validar

1. En el panel superior, seleccione una copia de seguridad por su fecha/hora de creación.

   La parte inferior de la ventana muestra el contenido de la copia de seguridad seleccionada, lo cual le ayuda a encontrar la copia de seguridad correcta.
2. Haga clic en **Aceptar**.

6.4.4 Selección de la ubicación

Para seleccionar una ubicación

Introduzca la ruta completa a la ubicación en el campo **Ruta** o seleccione la ubicación deseada en el **árbol de carpetas**.

- Para seleccionar una bóveda centralizada, expanda el grupo **Centralizada** y haga clic en la bóveda.
- Para seleccionar una bóveda personal, expanda el grupo **Personal** y haga clic en la bóveda.
- Para seleccionar la carpeta local (unidad de CD/DVD, o dispositivo de cintas adjunto local), expanda el grupo de **Carpetas locales** y haga clic en la carpeta que precisa.
- Para seleccionar una red compartida, amplíe el grupo **Carpetas de red**, seleccione el equipo en red correspondiente y después haga clic en la carpeta compartida. Si la red compartida requiere credenciales de acceso, el programa se las solicitará.
- Para seleccionar un servidor **FTP** o **SFTP**, amplíe el grupo correspondiente y haga clic en la carpeta correspondiente del servidor.

Como se muestra en la especificación FTP original, los credenciales necesarios para acceder a los servidores FTP se transfieren a través de la red como texto sin formato. Esto significa que una persona no deseada puede interceptar el nombre de usuario y la contraseña utilizando un comprobador de paquetes.

Uso de la tabla de archivos comprimidos

Para ayudarle a elegir la ubicación correcta, la tabla muestra los nombres de los archivos comprimidos incluidos en cada ubicación que seleccione. Mientras usted revisa el contenido de la ubicación, otro usuario o el mismo programa pueden añadir, eliminar o modificar archivos comprimidos de acuerdo con las operaciones programadas. Utilice el botón **Actualizar** para actualizar la lista de archivos comprimidos.

6.4.5 Credenciales de acceso para el origen

Especifique las credenciales necesarias para acceder a la ubicación donde está almacenado el archivo de copia de seguridad.

Para especificar las credenciales

1. Seleccione una de las siguientes opciones:
   - **Utilizar las credenciales de la tarea**

     El programa accederá a la ubicación utilizando las credenciales de la cuenta de la tarea especificada en la sección General.
   - **Utilizar las siguientes credenciales**

     El programa accederá a la ubicación utilizando las credenciales que especifique. Utilice esta opción si la cuenta de la tarea no dispone de permisos de acceso a la ubicación. Quizás necesite atribuir credenciales especiales para una red compartida o para una bóveda de nodo de almacenamiento.

     Especifique:
     - **Nombre de usuario**. Cuando introduzca el nombre de una cuenta de usuario de Active Directory, asegúrese de especificar también el nombre del dominio (DOMINIO\NombreDeUsuario o NombreDeUsuario@dominio)
     - **Contraseña**. La contraseña de la cuenta.
2. Haga clic en **Aceptar**.

Como se muestra en la especificación FTP original, los credenciales necesarios para acceder a los servidores FTP se transfieren a través de la red como texto sin formato. Esto significa que una persona no deseada puede interceptar el nombre de usuario y la contraseña utilizando un comprobador de paquetes.

6.4.6 Cuándo validar

Como la validación es una operación que utiliza muchos recursos, es conveniente programar la validación para el período de menor actividad del equipo gestionado. Por otro lado, si prefiere que le informen de inmediato si los datos no están dañados y pueden recuperarse correctamente, considere la opción de iniciar la validación de inmediato después de la creación de la tarea.

Elija una de las siguientes opciones:

- **Ahora**: para iniciar la tarea de validación inmediatamente después de su creación, es decir, después de hacer clic en Aceptar en la página Validación.
- **Más tarde**: para iniciar la tarea de validación solo una vez en la fecha y hora que especifique.

  Especifique los parámetros apropiados de la siguiente manera:
  - **Fecha y hora**: la fecha y hora en que debe comenzar la tarea.
  - **La tarea se iniciará manualmente (no programe la tarea)**: seleccione esta casilla de verificación si desea iniciar la tarea manualmente más tarde.

- **Según programación**: para programar la tarea. Para obtener más información sobre cómo configurar los parámetros de programación, consulte la sección Programación (pág. 85).

6.5 Montaje de una imagen

El montaje de volúmenes a partir de una copia de seguridad del disco (imagen) le permite acceder a los volúmenes como si se tratara de discos físicos. Se pueden montar varios volúmenes incluidos en la misma copia de seguridad dentro de una única operación de montaje. La operación de montaje está disponible cuando la consola está conectada a un equipo gestionado que ejecuta Windows o Linux.

El montaje de volúmenes en el modo de lectura-grabación le permite modificar el contenido de la copia de seguridad, es decir, guardar, mover, crear o eliminar archivos o carpetas, y ejecutar ejecutables que consten de un archivo.

Limitación: *No es posible realizar el montaje de copias de seguridad del volumen en el nodo de almacenamiento de Acronis Backup & Recovery 10.*

Escenarios de uso:

- **Compartir**: las imágenes montadas pueden compartirse fácilmente con los usuarios en red.
- **Solución de recuperación de base de datos "Band aid"**: monte una imagen que contenga una base de datos SQL desde una máquina que falló recientemente. Esto dará acceso a la base de datos hasta que se recupere la máquina que falló.
- **Limpieza de virus fuera de línea**: Si una máquina es atacada, el administrador la cierra, la reinicia con medios reiniciables y crea una imagen. Luego, el administrador configura esta imagen en modo de lectura/escritura, la escanea y limpia con un programa antivirus, y finalmente recupera la máquina.
- **Comprobación de errores**: si falla la recuperación debido a un error de disco, monte la imagen en el modo lectura/escritura. Luego, compruebe el disco en búsqueda de errores por medio del comando **chkdsk /r**.

Para montar una imagen, realice los siguientes pasos.

Origen

Archivo comprimido (pág. 158)

Especifique la ruta a la ubicación del archivo comprimido y seleccione el archivo comprimido que contenga copias de seguridad del disco.

Crear copia de seguridad (pág. 159)

Seleccione la copia de seguridad.

Credenciales de acceso (pág. 159)

[Opcional] Proporcione las credenciales para la ubicación del archivo comprimido. Para acceder a esta opción, marque la casilla de verificación **Vista avanzada**.

Configuración del montaje

Volúmenes (pág. 159)

Seleccione los volúmenes para montar y establezca la configuración del montaje para cada volumen: asigne una letra o introduzca el punto de montaje, elija el modo de acceso de lectura/grabación o de sólo lectura.

Cuando haya completado todos los pasos obligatorios, haga clic en **Aceptar** para montar los volúmenes.

6.5.1 Selección de archivos comprimidos

Selección del archivo comprimido

1. Introduzca la ruta completa a la ubicación en el campo **Ruta** o seleccione la carpeta deseada en el árbol de carpetas.

   - Si el archivo comprimido se almacena en Acronis Online Backup Storage, haga clic en **Iniciar sesión** y especifique las credenciales de acceso al almacenamiento en línea. Después, expanda el grupo **Almacenamiento de copia de seguridad en línea** y seleccione la cuenta.

   Las copias de seguridad almacenadas en Acronis Online Backup Storage no son aptas para la exportación ni el montaje.

   - Si el archivo comprimido está almacenado en una bóveda centralizada, expanda el grupo **Centralizada** y haga clic en la bóveda.
   - Si el archivo comprimido está almacenado en una bóveda personal, expanda el grupo **Personal** y haga clic en la bóveda.
   - Si el archivo comprimido está almacenado en una carpeta local en el equipo, expanda en grupo **Carpetas locales** y haga clic en la carpeta correspondiente.

   Si el archivo comprimido se encuentra en un medio extraíble como, por ejemplo, un DVD, introduzca primero el último DVD y, a continuación, los discos en orden comenzando por el primero cuando el programa le pregunte.

   - Si el archivo comprimido se encuentra en una red compartida, expanda el grupo **Carpetas de red** y, a continuación, seleccione el equipo en red correspondiente y haga clic en la carpeta compartida. Si la red compartida requiere credenciales de acceso, el programa se las solicitará.

   Nota para los usuario de Linux: *Para especificar una red compartida de sistema de archivos de Internet común (CIFS) que esté montada en un punto de montaje como /mnt/share, seleccione este punto de montaje en lugar de la propia red compartida.*

   - Si el archivo comprimido se encuentra en un servidor **FTP** o **SFTP**, escriba el nombre o la dirección del servidor en el campo **Ruta** tal y como se indica a continuación:

     ftp://ftp_server:port _number o sftp://sftp_server:port number

     Si no se especifica el número del puerto, se utilizará el puerto 21 para FTP y el puerto 22 para SFTP.

     Tras introducir las credenciales de acceso, las carpetas en el servidor estarán disponible. Haga clic en la carpeta correspondiente del servidor.

     Puede acceder al servidor como usuario anónimo, si el servidor permite ese tipo de acceso. Para esto, haga clic en **Usar acceso anónimo** en lugar de introducir las credenciales.

   Como se muestra en la especificación FTP original, los credenciales necesarios para acceder a los servidores FTP se transfieren a través de la red como texto sin formato. Esto significa que una persona no deseada puede interceptar el nombre de usuario y la contraseña utilizando un comprobador de paquetes.

   - Si el archivo comprimido se encuentra en un dispositivo de cinta conectado localmente, expanda el grupo **Dispositivos de cinta** y haga clic en el dispositivo correspondiente.

   Cuando opere en un equipo iniciado con un dispositivo de inicio:

   - Para acceder a la bóveda gestionada, escriba la siguiente cadena en el campo **Ruta**:

     bsp://dirección_nodo/nombre_bóveda/

- Para acceder a una bóveda centralizada sin gestionar, escriba la ruta completa de la carpeta de la bóveda.

2. En la tabla ubicada a la derecha del árbol, seleccione el archivo comprimido. La tabla muestra los nombres de los archivos comprimidos contenidos en cada una de las bóvedas/carpetas que seleccione.

   Mientras usted revisa el contenido de la ubicación, otro usuario o el mismo programa pueden añadir, eliminar o modificar archivos comprimidos de acuerdo con las operaciones programadas. Utilice el botón **Actualizar** para actualizar la lista de archivos comprimidos.
3. Haga clic en **Aceptar**.

6.5.2 Selección de la copia de seguridad

Para seleccionar una copia de seguridad:

1. Seleccione una de las copias de seguridad por su fecha/hora de creación.
2. Para ayudarle a elegir la copia de seguridad correcta, la tabla de la parte inferior muestra los volúmenes incluidos en la copia de seguridad seleccionada.

   Para obtener información sobre un volumen, haga clic con el botón secundario sobre este y después haga clic en **Información**.
3. Haga clic en **Aceptar**.

6.5.3 Credenciales de acceso

Para especificar las credenciales

1. Seleccione una de las siguientes opciones:
   - **Utilizar las credenciales actuales de usuario**

     El programa accederá a la ubicación utilizando las credenciales del usuario actual.
   - **Utilice las siguientes credenciales.**

     El programa accederá a la ubicación mediante las credenciales que especifique. Utilice esta opción si la cuenta del usuario actual no tiene permisos de acceso para la ubicación. Es posible que tenga que proporcionar credenciales especiales para una red compartida o una bóveda del nodo de almacenamiento.

     Especifique:
     - **Nombre de usuario**. Cuando introduzca el nombre de una cuenta de usuario de Active Directory, asegúrese de especificar también el nombre del dominio (DOMINIO\NombreDeUsuario o NombreDeUsuario@dominio)
     - **Contraseña**. La contraseña de la cuenta.
2. Haga clic en **Aceptar**.

Como se muestra en la especificación FTP original, los credenciales necesarios para acceder a los servidores FTP se transfieren a través de la red como texto sin formato. Esto significa que una persona no deseada puede interceptar el nombre de usuario y la contraseña utilizando un comprobador de paquetes.

6.5.4 Selección de volúmenes

Seleccione los volúmenes para montar y configure los parámetros de montaje para cada uno de los volúmenes seleccionados de la siguiente manera:

1. Seleccione la casilla de verificación para cada volumen que necesite montar.

2. Haga clic en el volumen seleccionado para establecer sus parámetros de montaje.
   - **Modo de acceso**: elija el modo en que desea montar el volumen:
     - **Sólo lectura**: permite explorar y abrir archivos dentro de la copia de seguridad sin ejecutar ningún cambio.
     - **Lectura/grabación**: con este modo, el programa asume que se modificará el contenido de la copia de seguridad, y crea una copia de seguridad incremental para capturar los cambios.
   - **Asignar letra** (en Windows): Acronis Backup & Recovery 10 asignará una letra que no esté en uso al volumen montado. Si fuera necesario, seleccione otra letra para asignar de la lista desplegable.
   - **Punto de montaje** (en Linux): especifique el directorio donde desea que se monte el volumen.
3. Si se seleccionan varios volúmenes para montar, haga clic en cada volumen para establecer sus parámetros de montaje, tal como se describió en el paso anterior.
4. Haga clic en **Aceptar**.

6.6 Gestión de imágenes montadas

Una vez que se haya montado un volumen, podrá examinar los archivos y carpetas incluidos en la copia de seguridad con un administrador de archivos, y copiar los archivos deseados en cualquier destino. Por lo tanto, si necesita sacar solo algunos archivos y carpetas de la copia de seguridad de un volumen, no es necesario que realice el procedimiento de recuperación.

Exploración de imágenes

La exploración de volúmenes montados le permite ver y modificar el contenido del volumen (si el montaje se realizó en el modo de lectura/grabación).

Para explorar un volumen montado, selecciónelo en la tabla y haga clic en **Explorar**. Se abrirá la ventana del administrador de archivos predeterminado, lo que permitirá al usuario examinar el contenido del volumen montado.

Desmontaje de imágenes

Mantener los volúmenes montados ocupa una cantidad considerable de recursos del sistema. Se recomienda que desmonte los volúmenes una vez que se hayan completado las operaciones necesarias. Si no se desmonta manualmente, un volumen permanecerá montado hasta que se reinicie el sistema operativo.

Para desmontar una imagen, selecciónela en la tabla y haga clic en **Desmontar**.

Para desmontar todos los volúmenes montados, haga clic en **Desmontar todo**.

6.7 Exportación de archivos comprimidos y copias de seguridad

La operación de exportación crea una copia de un archivo comprimido o una copia parcial de un archivo comprimido en la ubicación especificada. El archivo comprimido original permanece intacto.

La operación de exportación puede aplicarse a:

- **un único archivo comprimido** - se creará una copia exacta del archivo comprimido
- **una única copia de seguridad** - se creará un archivo comprimido que contiene una única copia de seguridad completa. La exportación de una copia de seguridad incremental o diferencial se realiza utilizando la consolidación de las copias de seguridad anteriores hasta la última copia de seguridad completa
- **su selección de copias de seguridad** que pertenecen al mismo archivo comprimido, el archivo comprimido resultante contendrá sólo las copias de seguridad especificadas. La consolidación se realiza según sus necesidades, para que el archivo comprimido resultante pueda contener copias de seguridad completas, incrementales y diferenciales.

Escenarios de usos:

La exportación le permite separar una copia de seguridad específica de una cadena de copias de seguridad incrementales para una rápida recuperación, escribir sobre dispositivos extraíbles u otros propósitos.

Ejemplo. Al realizar una copia de seguridad de datos a una ubicación remota mediante una conexión de red inestable o con un bajo ancho de banda (como una copia de seguridad a través de WAN con acceso VPN), es posible que desee guardar la copia de seguridad completa inicial a un dispositivo extraíble. Después, enviar el dispositivo a la ubicación remota. Allí la copia de seguridad se exportará desde el dispositivo al almacenamiento de destino. Las copias de seguridad incrementales posteriores, que generalmente son mucho más pequeñas, se pueden transferir a través de la red.

Al exportar una bóveda gestionada a un dispositivo extraíble, obtiene una bóveda portátil sin gestionar que puede utilizarse en las siguientes situaciones:

- la conservación de una copia externa de su bóveda o de los archivos comprimidos más importantes
- el transporte físico de una bóveda a una sucursal distante
- la recuperación sin acceso al nodo de almacenamiento en el caso de problemas de red o fallos en el nodo de almacenamiento
- la recuperación del nodo de almacenamiento mismo.

La exportación desde una bóveda basada en HDD a un dispositivo de cinta puede considerarse como un simple ajuste de archivo bajo petición.

El nombre del archivo comprimido resultante

De manera predeterminada, el archivo comprimido exportado hereda el nombre del archivo original. Debido a que tener varios archivos con el mismo nombre en la misma ubicación no es conveniente, las siguientes acciones están desactivadas en el nombre de archivo comprimido predeterminado:

- exportación de parte de un archivo comprimido a la misma ubicación
- exportación de un archivo comprimido o parte de un archivo comprimido a una ubicación donde existe un archivo comprimido con el mismo nombre
- exportación de un archivo comprimido o parte de un archivo comprimido a la misma ubicación dos veces

En cualquiera de los casos anteriores, proporcione un nombre de archivo comprimido que sea único en la carpeta o bóveda de destino. Si debe rehacer la exportación utilizando el mismo nombre de archivo comprimido, elimine primero el archivo comprimido que resultó de la operación de exportación anterior.

Las opciones del archivo comprimido resultante

El archivo comprimido exportado hereda las opciones del archivo comprimido original, incluyendo el cifrado y la contraseña. Al exportar un archivo comprimido protegido con contraseña, se le pedirá que introduzca la contraseña. Si el archivo comprimido está cifrado, se utilizará la contraseña para cifrar el archivo comprimido resultante.

Ubicación del origen y el destino

Cuando la consola está conectada a un **equipo gestionado**, puede exportar un archivo comprimido o parte de un archivo hacia y desde cualquier ubicación accesible al agente que reside en el equipo. Estos incluyen bóvedas personales, dispositivos de cinta conectados localmente, medios extraíbles y, en las versiones avanzadas de los productos, bóvedas centralizadas gestionadas y sin gestionar.

Cuando la consola esté conectada al **management server**, están disponibles dos métodos de exportación:

- exportación desde una **bóveda centralizada**. El nodo de almacenamiento que gestiona la bóveda realiza la exportación. El destino puede ser una red compartida o una carpeta local del nodo de almacenamiento.
- exportación desde un **bóveda centralizada sin gestionar**. El agente instalado en el equipo gestionado que usted especifique realiza la exportación. El destino puede ser cualquier ubicación accesible al agente, incluyendo una bóveda gestionada.

Consejo. *Cuando configure una exportación a una bóveda gestionada de deduplicación, seleccione un equipo donde esté instalado el complemento de deduplicación en el agente. De lo contrario la tarea de exportación fallará.*

Operaciones con una tarea de exportación

Una tarea de exportación comienza inmediatamente después de que complete su configuración. Una tarea de exportación puede detenerse o eliminarse de la misma manera que cualquier otra tarea.

Una vez que ha finalizado la tarea de exportación, puede ejecutarla nuevamente en cualquier momento. Antes de hacerlo, elimine el archivo comprimido que resultó de la ejecución de la tarea anterior si el archivo comprimido aún existe en la bóveda de destino. De lo contrario la tarea fallará. No puede editar una tarea de exportación para especificar otro nombre para el archivo comprimido de destino (esto es una limitación).

Consejo. *Puede implementar el ajuste de la situación manualmente ejecutando regularmente la tarea de eliminación del archivo comprimido seguida de la tarea de exportación.*

Maneras diferentes de crear una tarea de exportación

La forma más general de crear una tarea de exportación consiste en usar la página **Exportación**. Aquí, puede exportar cualquier copia de seguridad o archivo comprimido al que tenga permiso para acceder.

Puede acceder a la página **Exportación** desde la vista **Bóvedas**. Haga clic en el objeto a exportar (archivos comprimidos o copias de seguridad) y seleccione **Exportar** desde el menú contextual. La página **Exportar** se abrirá con el objeto preseleccionado como origen. Todo lo que debe hacer es seleccionar el destino y (de manera opcional) proporcionar un nombre para la tarea.

Para exportar un archivo comprimido o una copia de seguridad siga los siguientes pasos.

General

Nombre de la tarea

[Opcional] Introduzca un nombre único para la tarea. Un nombre pensado deliberadamente le permite identificar de manera rápida una tarea entre las demás.

Credenciales de la tarea (pág. 163)

[Opcional] La tarea de exportación se ejecutará en nombre del usuario que cree la tarea. De ser necesario, podrá cambiar las credenciales de la tarea. Para acceder a esta opción, marque la casilla de verificación **Vista avanzada**.

Qué exportar

Exportar

Seleccione un objeto para exportar:

Archivo comprimido (pág. 140) - en ese caso, debe especificar solamente el archivo comprimido.

Copias de seguridad (pág. 165) - primero especifique el archivo comprimido y luego seleccione las copias de seguridad deseadas en este archivo comprimido

Credenciales de acceso (pág. 165)

[Opcional] Proporcione las credenciales para acceder al origen si la cuenta de la tarea no tiene suficientes privilegios para acceder a este. Para acceder a esta opción, marque la casilla de verificación **Vista avanzada**.

Dónde exportar

Archivo comprimido (pág. 166)

Introduzca la ruta a la ubicación donde se creará el archivo comprimido nuevo.

Asegúrese de proporcionar un nombre distintivo e introduzca un comentario para el nuevo archivo comprimido.

Credenciales de acceso (pág. 167)

[Opcional] Proporcione las credenciales para el destino si las credenciales de la tarea no tienen suficientes privilegios para accederlas. Para acceder a esta opción, marque la casilla de verificación **Vista avanzada**.

Después de realizar todos los pasos requeridos, haga clic en **Aceptar** para comenzar a exportar la tarea.

6.7.1 Credenciales de la tarea

Proporcione las credenciales para la cuenta con la que se ejecutará la tarea.

Para especificar las credenciales

1. Seleccione una de las siguientes opciones:
   - **Ejecutar con el usuario actual**

     La tarea se ejecutará con las credenciales de la cuenta con la que el usuario que inicia las tareas haya iniciado la sesión. Si la tarea debe ejecutarse según la programación, se le solicitará la contraseña del usuario actual al finalizar la creación de la tarea.
   - **Utilizar las siguientes credenciales**

     La tarea se ejecutará siempre con las credenciales que especifique, ya sea que se inicie manualmente o según la programación.

Especifique:

- **Nombre de usuario**. Cuando introduzca el nombre de una cuenta de usuario de Active Directory, asegúrese de especificar también el nombre del dominio (DOMINIO\NombreDeUsuario o NombreDeUsuario@dominio)
- **Contraseña**. La contraseña de la cuenta.

2. Haga clic en **Aceptar**.

Para obtener más información sobre cómo utilizar las credenciales para Acronis Backup & Recovery 10, consulte la sección Propietarios y credenciales (pág. 23).

Para obtener más información sobre las operaciones disponibles según los privilegios del usuario, consulte la sección Privilegios de usuario en un equipo gestionado (pág. 23).

6.7.2 Selección de archivos comprimidos

Selección del archivo comprimido

1. Introduzca la ruta completa a la ubicación en el campo **Ruta** o seleccione la carpeta deseada en el árbol de carpetas.
   - Si el archivo comprimido se almacena en Acronis Online Backup Storage, haga clic en **Iniciar sesión** y especifique las credenciales de acceso al almacenamiento en línea. Después, expanda el grupo **Almacenamiento de copia de seguridad en línea** y seleccione la cuenta.

   Las copias de seguridad almacenadas en Acronis Online Backup Storage no son aptas para la exportación ni el montaje.

   - Si el archivo comprimido está almacenado en una bóveda centralizada, expanda el grupo **Centralizada** y haga clic en la bóveda.
   - Si el archivo comprimido está almacenado en una bóveda personal, expanda el grupo **Personal** y haga clic en la bóveda.
   - Si el archivo comprimido está almacenado en una carpeta local en el equipo, expanda en grupo **Carpetas locales** y haga clic en la carpeta correspondiente.

   Si el archivo comprimido se encuentra en un medio extraíble como, por ejemplo, un DVD, introduzca primero el último DVD y, a continuación, los discos en orden comenzando por el primero cuando el programa le pregunte.

   - Si el archivo comprimido se encuentra en una red compartida, expanda el grupo **Carpetas de red** y, a continuación, seleccione el equipo en red correspondiente y haga clic en la carpeta compartida. Si la red compartida requiere credenciales de acceso, el programa se las solicitará.

   Nota para los usuario de Linux: *Para especificar una red compartida de sistema de archivos de Internet común (CIFS) que esté montada en un punto de montaje como /mnt/share, seleccione este punto de montaje en lugar de la propia red compartida.*

   - Si el archivo comprimido se encuentra en un servidor **FTP** o **SFTP**, escriba el nombre o la dirección del servidor en el campo **Ruta** tal y como se indica a continuación:

     ftp://ftp_server:port _number o sftp://sftp_server:port number

     Si no se especifica el número del puerto, se utilizará el puerto 21 para FTP y el puerto 22 para SFTP.

     Tras introducir las credenciales de acceso, las carpetas en el servidor estarán disponible. Haga clic en la carpeta correspondiente del servidor.

Puede acceder al servidor como usuario anónimo, si el servidor permite ese tipo de acceso. Para esto, haga clic en **Usar acceso anónimo** en lugar de introducir las credenciales.

Como se muestra en la especificación FTP original, los credenciales necesarios para acceder a los servidores FTP se transfieren a través de la red como texto sin formato. Esto significa que una persona no deseada puede interceptar el nombre de usuario y la contraseña utilizando un comprobador de paquetes.

- Si el archivo comprimido se encuentra en un dispositivo de cinta conectado localmente, expanda el grupo **Dispositivos de cinta** y haga clic en el dispositivo correspondiente.

Cuando opere en un equipo iniciado con un dispositivo de inicio:

- Para acceder a la bóveda gestionada, escriba la siguiente cadena en el campo **Ruta**:

  bsp://dirección_nodo/nombre_bóveda/
- Para acceder a una bóveda centralizada sin gestionar, escriba la ruta completa de la carpeta de la bóveda.

2. En la tabla ubicada a la derecha del árbol, seleccione el archivo comprimido. La tabla muestra los nombres de los archivos comprimidos contenidos en cada una de las bóvedas/carpetas que seleccione.

   Mientras usted revisa el contenido de la ubicación, otro usuario o el mismo programa pueden añadir, eliminar o modificar archivos comprimidos de acuerdo con las operaciones programadas. Utilice el botón **Actualizar** para actualizar la lista de archivos comprimidos.
3. Haga clic en **Aceptar**.

6.7.3 Selección de la copia de seguridad

Para especificar una copia de seguridad a exportar

1. En la parte superior de la ventana, seleccione la casilla de verificación correspondiente.

   Para asegurarse de que seleccionó la copia de seguridad correcta, haga clic en la copia de seguridad y observe la tabla de la parte inferior que muestra el volumen que contiene la copia de seguridad seleccionada.

   Para obtener información sobre un volumen, haga clic con el botón secundario sobre éste y después seleccione **Información**.
2. Haga clic en **Aceptar**.

6.7.4 Credenciales de acceso para el origen

Especifique las credenciales necesarias para acceder a la ubicación donde está almacenado el archivo comprimido (o la copia de seguridad) de origen.

Para especificar las credenciales

1. Seleccione una de las siguientes opciones:
   - **Utilizar las credenciales de la tarea**

     El programa accederá a la ubicación utilizando las credenciales de la cuenta de la tarea especificada en la sección General.
   - **Utilizar las siguientes credenciales**

     El programa accederá a la ubicación utilizando las credenciales que especifique. Utilice esta opción si la cuenta de la tarea no dispone de permisos de acceso a la ubicación. Quizás necesite atribuir credenciales especiales para una red compartida o para una bóveda de nodo de almacenamiento.

     Especifique:

- **Nombre de usuario**. Cuando introduzca el nombre de una cuenta de usuario de Active Directory, asegúrese de especificar también el nombre del dominio (DOMINIO\NombreDeUsuario o NombreDeUsuario@dominio)
- **Contraseña**. La contraseña de la cuenta.

2. Haga clic en **Aceptar**.

Como se muestra en la especificación FTP original, los credenciales necesarios para acceder a los servidores FTP se transfieren a través de la red como texto sin formato. Esto significa que una persona no deseada puede interceptar el nombre de usuario y la contraseña utilizando un comprobador de paquetes.

6.7.5 Selección de la ubicación

Especifique un destino donde se almacenará el objeto exportado. La exportación de copias de seguridad al mismo archivo comprimido no está permitida.

1. Selección de destino de la exportación

Introduzca la ruta de destino completa en el campo **Ruta** o seleccione el destino deseado en el árbol de carpetas.

- Para exportar datos a una bóveda centralizada sin gestionar, expanda el grupo **Bóvedas centralizadas** y haga clic en la bóveda.
- Para exportar datos a una bóveda personal, expanda el grupo **Bóvedas personales** y haga clic en la bóveda.
- Para exportar datos a una carpeta local en el equipo, expanda el grupo **Carpetas locales** y haga clic en la carpeta requerida.
- Para exportar datos a una red compartida, expanda el grupo **Carpetas de red**, seleccione el equipo en red requerido y luego haga clic en la carpeta compartida. Si la red compartida requiere credenciales de acceso, el programa se las solicitará.

  Nota para los usuario de Linux: *Para especificar una red compartida de sistema de archivos de Internet común (CIFS) que esté montada en un punto de montaje como /mnt/share, seleccione este punto de montaje en lugar de la propia red compartida.*

- Para exportar datos a un servidor **FTP** o **SFTP**, escriba el nombre o la dirección del servidor en el campo **Ruta** de la siguiente manera:

  ftp://ftp_server:port _number o **sftp://sftp_server:port number**

  Si no se especifica el número del puerto, se utilizará el puerto 21 para FTP y el puerto 22 para SFTP.

  Tras introducir las credenciales de acceso, las carpetas en el servidor estarán disponible. Haga clic en la carpeta correspondiente del servidor.

  Puede acceder al servidor como usuario anónimo, si el servidor permite ese tipo de acceso. Para esto, haga clic en **Usar acceso anónimo** en lugar de introducir las credenciales.

  De acuerdo con la especificación FTP original, los credenciales necesarios para acceder a los servidores FTP se transfieren a través de la red como texto sin formato. Esto significa que una persona no deseada puede interceptar el nombre de usuario y la contraseña utilizando un comprobador de paquetes.

- Para exportar datos a un dispositivo de cinta conectado a nivel local, amplíe el grupo **Unidades de cinta** y haga clic en el dispositivo correspondiente.

2. Uso de la tabla de archivos comprimidos

Para asistirle en la elección del destino correcto, la tabla a la derecha muestra los nombres de los archivos comprimidos contenidos en cada una de las ubicaciones que seleccione en el árbol.

Mientras usted revisa el contenido de la ubicación, otro usuario o el mismo programa pueden añadir, eliminar o modificar archivos comprimidos de acuerdo con las operaciones programadas. Utilice el botón **Actualizar** para actualizar la lista de archivos comprimidos.

3. Nombrar un archivo comprimido nuevo

De manera predeterminada, el archivo comprimido exportado hereda el nombre del archivo original. Debido a que tener varios archivos con el mismo nombre en la misma ubicación no es conveniente, las siguientes acciones están desactivadas en el nombre de archivo comprimido predeterminado:

- exportación de parte de un archivo comprimido a la misma ubicación
- exportación de un archivo comprimido o parte de un archivo comprimido a una ubicación donde existe un archivo comprimido con el mismo nombre
- exportación de un archivo comprimido o parte de un archivo comprimido a la misma ubicación dos veces

En cualquiera de los casos anteriores, proporcione un nombre de archivo comprimido que sea único en la carpeta o bóveda de destino. Si debe rehacer la exportación utilizando el mismo nombre de archivo comprimido, elimine primero el archivo comprimido que resultó de la operación de exportación anterior.

6.7.6 Credenciales de acceso para el destino

Especifique las credenciales necesarias para acceder a la ubicación donde se almacenará el archivo comprimido resultante. El usuario cuyo nombre se especifique se considerará el propietario del archivo comprimido.

Para especificar las credenciales

1. Seleccione una de las siguientes opciones:
   - **Utilizar las credenciales de la tarea**

     El programa accederá a la ubicación utilizando las credenciales de la cuenta de la tarea especificada en la sección General.
   - **Utilizar las siguientes credenciales**

     El programa accederá a la ubicación utilizando las credenciales que especifique. Utilice esta opción si la cuenta de la tarea no dispone de permisos de acceso a la ubicación. Quizás necesite atribuir credenciales especiales para una red compartida o para una bóveda de nodo de almacenamiento.

     Especifique:
     - **Nombre de usuario**. Cuando introduzca el nombre de una cuenta de usuario de Active Directory, asegúrese de especificar también el nombre del dominio (DOMINIO\NombreDeUsuario o NombreDeUsuario@dominio)
     - **Contraseña**. La contraseña de la cuenta.
2. Haga clic en **Aceptar**.

Como se muestra en la especificación FTP original, los credenciales necesarios para acceder a los servidores FTP se transfieren a través de la red como texto sin formato. Esto significa que una persona no deseada puede interceptar el nombre de usuario y la contraseña utilizando un comprobador de paquetes.

6.8 Acronis Secure Zone

Acronis Secure Zone es una partición segura que permite mantener archivos de copia de seguridad en el espacio de disco de un equipo gestionado y, por lo tanto, recuperar un disco del mismo disco donde reside la copia de seguridad.

Ciertas aplicaciones de Windows, como las herramientas de gestión de discos de Acronis pueden acceder a la zona.

Para obtener más información sobre las ventajas y limitaciones de Acronis Secure Zone, consulte el apartado Acronis Secure Zone (pág. 41) en la sección "Tecnologías patentadas de Acronis".

6.8.1 Creación de Acronis Secure Zone

Puede crear una Acronis Secure Zone cuando el sistema operativo se está ejecutando o cuando está utilizando un dispositivo de arranque.

Para crear una Acronis Secure Zone, lleve a cabo los siguientes pasos.

Espacio

Disco (pág. 168)

Escoja un disco duro (si hay más de uno) donde creará la zona. Acronis Secure Zone se crea utilizando un espacio no asignado, si hay espacio disponible, o a partir del espacio libre del volumen.

Tamaño (pág. 169)

Especifique el tamaño exacto de la zona. Mover o cambiar de tamaño de volúmenes bloqueados, tales como el volumen del actual sistema operativo activo, requiere reiniciar el sistema.

Configuraciones

Contraseña (pág. 169)

[Opcional] Proteja Acronis Secure Zone de accesos no autorizados mediante una contraseña. Se solicitará la contraseña para cualquier operación relacionada con la zona.

Después de configurar los ajustes requeridos, haga clic en Aceptar. En la ventana Confirmación de resultado (pág. 169), revise la distribución especificada y haga clic en Aceptar para comenzar a crear la zona.

Disco de Acronis Secure Zone

Acronis Secure Zone puede ubicarse en cualquier disco duro fijo. Acronis Secure Zone siempre se crea al final del disco duro. Un equipo puede tener solo una Acronis Secure Zone. Acronis Secure Zone se crea utilizando un espacio no asignado, si hay espacio disponible, o a partir del espacio libre del volumen.

Acronis Secure Zone no se puede organizar en un disco dinámico o disco que utiliza el estilo de partición GPT.

Para asignar espacio a Acronis Secure Zone

1. Escoja un disco duro (si hay más de uno) donde creará la zona. El espacio no asignado se selecciona de manera predeterminada. El programa muestra la totalidad de espacio disponible para Acronis Secure Zone.

2. Si necesita asignar más espacio a la zona, puede seleccionar volúmenes desde donde se pueda obtener espacio libre. Nuevamente, el programa muestra la totalidad de espacio disponible para Acronis Secure Zone según su selección. Podrá configurar el tamaño exacto de la zona en la ventana **Tamaño de Acronis Secure Zone.** (pág. 169)
3. Haga clic en **Aceptar**.

Tamaño de Acronis Secure Zone

Introduzca el tamaño de Acronis Secure Zone o arrastre el deslizador para seleccionar cualquier tamaño entre los mínimos y los máximos. El tamaño mínimo es aproximadamente de 50 MB, de acuerdo con la geometría del disco duro. El tamaño máximo es igual al espacio no asignado del disco más el espacio libre total de todos los volúmenes que haya seleccionado en el paso anterior.

Si tiene que sacar espacio del volumen de inicio o del sistema, tenga en cuenta lo siguiente:

- Para mover o cambiar el tamaño del volumen desde el cual se arranca actualmente el sistema, será necesario reiniciar.
- Sacar todo el espacio libre de un volumen del sistema puede hacer que el sistema operativo funcione de forma inestable e incluso que no pueda iniciarse. No configure el tamaño máximo de la zona si está seleccionado el volumen de inicio o del sistema.

Contraseña para Acronis Secure Zone

Configurar una contraseña protege a Acronis Secure Zone contra accesos no autorizados. El programa solicitará la contraseña para cualquier operación relacionada con la zona y los archivos comprimidos que se encuentren en ella, como realización de copias de seguridad y recuperación de datos, validación de archivos comprimidos, modificación de tamaño y eliminación de la zona.

Configurar una contraseña

1. Seleccione **Utilizar contraseña**.
2. En el campo **Introducir contraseña**, escriba una nueva contraseña.
3. En el campo **Confirmar contraseña**, vuelva a escribir la contraseña.
4. Haga clic en **Aceptar**.

Para deshabilitar la contraseña

1. Seleccione **No utilizar**.
2. Haga clic en **Aceptar**.

Confirmación del resultado

La ventana **Confirmación del resultado** muestra la distribución esperada de la partición de acuerdo con los ajustes que haya elegido. Haga clic en **Aceptar** si está de acuerdo con la distribución y se iniciará la creación de Acronis Secure Zone.

Cómo se procesarán los ajustes que realiza

Esto le ayudará a comprender cómo la creación de Acronis Secure Zone transformará un disco que contenga varios volúmenes.

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

tamaño de los volúmenes. Para modificar el tamaño de los volúmenes bloqueados, es necesario reiniciar el sistema.

- Sin embargo, debería haber espacio libre en un volumen para que el sistema operativo y las aplicaciones puedan funcionar; por ejemplo, para crear archivos temporales. El programa no reducirá un volumen en el que el espacio libre ocupe o quede en un nivel inferior al 25% del tamaño total del mismo. El programa 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 lo mencionado previamente, no es recomendable configurar el máximo posible para el tamaño de la zona. 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.

6.8.2 Gestión de Acronis Secure Zone

Acronis Secure Zone se considera una bóveda (pág. 186) personal. Una vez que se crea en un equipo gestionado, la zona está presente siempre en la lista de **Bóvedas personales**. Los planes de copias de seguridad centralizados pueden utilizar Acronis Secure Zone al igual que los planes locales.

Si ha utilizado Acronis Secure Zone anteriormente, tenga en cuenta que se ha producido un cambio radical en su funcionamiento. La zona ya no realiza limpiezas automáticas, es decir, ya no elimina archivos comprimidos antiguos. Utilice esquemas de copia de seguridad con limpieza automática para realizar copias de seguridad en la zona o elimine manualmente archivos comprimidos desactualizados mediante la función de gestión de la bóveda.

Con el nuevo comportamiento de Acronis Secure Zone, puede conseguir:

- elaborar una lista de los archivos comprimidos ubicados en la zona y de las copias de seguridad en cada archivo comprimido
- examinar el contenido de una copia de seguridad,
- montar la copia de seguridad de un volumen para copiar archivos desde la copia de seguridad a un disco físico,
- eliminar de manera segura los archivos comprimidos y las copias de seguridad de los archivos comprimidos.

Para obtener más información acerca de las operaciones con bóvedas, consulte la sección Bóvedas (pág. 77).

Aumento de Acronis Secure Zone

Para aumentar Acronis Secure Zone

1. En la página **Gestionar Acronis Secure Zone**, haga clic en **Aumentar**.
2. Seleccione los volúmenes que dispongan del espacio libre que se utilizará para aumentar Acronis Secure Zone.
3. Especifique el nuevo tamaño de la zona al:
   - arrastrar el deslizador y seleccionar cualquier tamaño entre los valores actuales y máximos. El máximo tamaño equivale al espacio no asignado del disco más el espacio libre total de las particiones seleccionadas;
   - escribir un valor exacto en el campo Tamaño de Acronis Secure Zone.

Al aumentar el tamaño de la zona, el programa actuará de la siguiente manera:

- en primer lugar, utilizará el espacio no asignado. De ser necesario, los volúmenes se moverán, pero no aumentarán su tamaño. Mover los volúmenes bloqueados requiere reiniciar el equipo.
- Si no existe suficiente espacio no asignado, el programa obtendrá espacio libre de los volúmenes seleccionados, reduciendo proporcionalmente el tamaño de estos. Para modificar el tamaño de las particiones bloqueadas es necesario reiniciar el sistema.

Reducir el volumen del sistema al tamaño mínimo puede impedir el arranque del sistema operativo.

4. Haga clic en **Aceptar**.

Disminución de Acronis Secure Zone

Para disminuir Acronis Secure Zone

1. En la página **Gestión de Acronis Secure Zone**, haga clic en **Disminuir**.
2. Seleccione los volúmenes a los que se destinarán los espacios libres después de que se disminuya la zona.
3. Especifique el nuevo tamaño de la zona al:
   - arrastrar el deslizador y seleccionar cualquier tamaño entre los valores actuales y máximos. El tamaño mínimo es de aproximadamente 50 MB, de acuerdo con la geometría del disco duro;
   - escribir un valor exacto en el campo Tamaño de **Acronis Secure Zone.**
4. Haga clic en **Aceptar**.

Eliminación de Acronis Secure Zone

Para eliminar Acronis Secure Zone

1. En la barra **Acciones de Acronis Secure Zone** (en el panel **Acciones y herramientas**), seleccione **Eliminar**.
2. En la ventana **Eliminar Acronis Secure Zone**, seleccione los volúmenes a los cuales quiere añadir el espacio liberado de la zona y haga clic en **Aceptar**.

   Si selecciona varios volúmenes, el espacio se distribuirá de manera proporcional para cada partición. Si no selecciona un volumen, el espacio liberado se convertirá en espacio no asignado.

Tras hacer clic en **Aceptar**, Acronis Backup & Recovery 10 comenzará a eliminar la zona.

6.9 Acronis Startup Recovery Manager

Acronis Startup Recovery Manager es una modificación del agente de arranque (pág. 186) que reside en el disco del sistema en Windows o en la partición /boot en Linux y está configurado para iniciarse en el tiempo de arranque al pulsar F11. Elimina la necesidad disponer de un dispositivo o conexión de red para ejecutar la utilidad de rescate de inicio.

Activar

Habilita el mensaje de tiempo de inicio "Pulse F11 para Acronis Startup Recovery Manager..." (si no tiene el cargador de inicio GRUB) o añade el elemento "Acronis Startup Recovery Manager" al menú de GRUB (si tiene GRUB). Si el sistema no arranca, podrá ejecutar la utilidad de rescate de inicio al pulsar F11 o al seleccionarlo en el menú, respectivamente.

El disco del sistema (o la partición /boot en Linux) debe tener por lo menos 70 MB de espacio libre para activar Acronis Startup Recovery Manager.

A menos que use el cargador de inicio GRUB y este esté instalado en el registro de inicio maestro (MBR), la activación de Acronis Startup Recovery Manager sobrescribirá el registro de inicio maestro con su propio código de inicio. Por lo tanto, necesitará activar nuevamente cargadores de inicio de terceros, si están instalados.

En Linux, cuando se utiliza un cargador de inicio que no sea GRUB (como LILO), considere instalarlo en un registro de inicio de partición de raíz (o inicio) de Linux en lugar de MBR antes de activar. De lo contrario, vuelva a configurar este cargador de inicio manualmente después de la activación.

No activar

Deshabilita el mensaje de tiempo de inicio "Pulse F11 para Acronis Startup Recovery Manager..." (o el elemento del menú en GRUB). Si Acronis Startup Recovery Manager no está activado, necesitará realizar algunas de las siguientes acciones para recuperar el sistema cuando el arranque falle:

- arranque el equipo desde un dispositivo de rescate de arranque diferente
- realice el inicio de red desde Acronis PXE Server o Microsoft Remote Installation Services (RIS).

Consulte la sección Dispositivo de arranque (pág. 172) para obtener más información.

6.10 Dispositivo de arranque

Dispositivo de arranque

Los dispositivos de arranque son un dispositivo físico (CD, DVD, unidad USB u otro dispositivo compatible con el BIOS de un equipo como dispositivo de arranque) que inicia en cualquier equipo compatible con PC y permite que ejecute el agente Acronis Backup & Recovery 10 tanto en un entorno basado en Linux como un entorno de preinstalación de Windows (WinPE), sin la ayuda de un sistema operativo. Los dispositivos de arranque se usan con frecuencia para:

- recuperar de un sistema operativo que no puede iniciar
- acceder a los datos que sobrevivieron en un sistema dañado y realizar copias de seguridad de éstos
- implementar un sistema operativo desde cero
- crear volúmenes básicos o dinámicos desde cero
- realizar copias de seguridad "sector por sector" de un disco con un sistema de archivos incompatible
- realizar copias de seguridad fuera de línea de cualquier dato que no se puede incluir en la copia de seguridad en línea por acceso restricto, con un bloqueo permanente por las aplicaciones en ejecución o por cualquier otra razón.

Se puede iniciar un equipo en los entornos anteriores, ya sea con los dispositivos físicos o desde la red con el servidor PXE de Acronis, Windows Deployment Services (WDS) o Servicios de Instalación Remota (RIS). Estos servidores con componentes de arranque cargados también puede considerarse un tipo de dispositivo de arranque. Puede crear dispositivos de arranque o configurar el servidor PXE o WDS/RIS con el mismo asistente.

Dispositivo de arranque basado en Linux

Los dispositivos de arranque basados en Linux contienen el agente de arranque Acronis Backup & Recovery 10 basado en un núcleo Linux. El agente puede iniciar y realizar las operaciones en cualquier hardware compatible con PC, incluyendo desde cero y los equipo con sistemas de archivos corruptos o incompatibles. Se puede configurar y controlar las operaciones tanto a nivel local como remoto con la consola de administración.

Dispositivo de arranque basado en PE

Los dispositivos de arranque basados en PE contienen un sistema Windows mínimo llamado Windows Preinstallation Environment (WinPE) y el complemento para WinPE de Acronis, es decir, una modificación del Agente de Acronis Backup & Recovery 10 que se puede ejecutar en el entorno de preinstalación.

Se comprobó que WinPE es la solución de arranque más conveniente en entornos grandes con hardware heterogéneo.

Ventajas:

- El uso de Acronis Backup & Recovery 10 con el entorno de preinstalación de Windows proporciona más funcionalidad que el uso de dispositivos de arranque basados en Linux. Como se inició un hardware compatible con PC en WinPE, no sólo puede utilizar el Agente de Acronis Backup & Recovery 10, sino también los comandos y secuencias de comando y otros complementos de PE que haya agregado.
- Los dispositivos de arranque basados en PE ayudan a superar los problemas de los dispositivos de arranque basados en Linux compatibles con ciertos controladores RAID de ciertos niveles de conjuntos de RAID solos. Los dispositivos basados en PE 2.x, es decir los núcleos de Windows Vista o Windows Server 2008, permiten la carga dinámica de controladores de dispositivos necesarios.

6.10.1 Medios de inicio basados en Linux

Cuando use el generador de dispositivos, debe especificar:

1. [opcional] Los parámetros del kernel de Linux. Separe los diferentes parámetros con espacios.

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

   Para obtener una lista de parámetros, consulte Parámetros del kernel (pág. 174).
2. Los componentes de arranque de Acronis se ubicarán en el dispositivo.
   - Se puede habilitar Universal Restore de Acronis Backup & Recovery 10 si se instaló Universal Restore en el equipo donde se creó el dispositivo.
3. [opcional] El intervalo de tiempo de espera para el menú de inicio además del componente que se iniciará automáticamente en el tiempo de espera.
   - Si no se configura, el cargador de Acronis espera que alguien seleccione si iniciar desde el sistema operativo (de estar presente) o desde el componente de Acronis.
   - Si configura, por ejemplo, **10 seg** para el agente de inicio, el agente se iniciará 10 segundos después de que se muestre el menú. Esto permite la operación desatendida del sitio cuando inicie desde un servidor PXE o WDS/RIS.
4. [opcional] Configuraciones de inicio de sesión remota:
   - el nombre de usuario y contraseña que se ingresarán del lado de la consola cuando se conecte con el agente. Si deja estos campos en blanco, se habilitará la conexión para ingresar cualquier símbolo en la ventana de línea de comandos.
5. [opcional] Configuración de red (pág. 175):
   - La configuración TCP/IP que será asignada a los adaptadores de red del equipo.
6. [opcional] Puerto del red (pág. 176):
   - el puerto TCP que el agente de inicio escucha para las conexiones entrantes.

7. El tipo de dispositivo que desea crear. Puede:
   - crear CD, DVD u otros dispositivos de arranque como una unidad de memoria flash USB si la BIOS del hardware permite el inicio desde tal dispositivo
   - crear una imagen ISO de un disco de arranque para grabar más tarde en un disco en blanco
   - cargar los componentes seleccionados en el servidor PXE de Acronis
   - cargar los componentes seleccionados A WDS/RIS.
8. [opcional] los controladores del sistema Windows que usará Universal Restore de Acronis. La ventana aparece sólo si está instalado el complemento para Universal Restore de Acronis y si selecciona otro dispositivo que no sea PXE o WDS/RIS.
9. La ruta del archivo ISO o el nombre o dirección IP y las credenciales para PXE o WDS/RIS.

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.

Configuraciones de red

Mientras crea el dispositivo de arranque Acronis, usted tiene la opción de preconfigurar las conexiones de red que serán usadas por el agente de inicio. Se pueden preconfigurar los siguientes parámetros:

- Dirección IP
- Máscara de subred

- Puertas de enlace
- Servidor DNS
- Servidor WINS.

Una vez que se inicia el agente de arranque en un equipo, se aplica la configuración en la tarjeta de interfaz de red (NIC) del equipo. Si no se preconfiguran las configuraciones, el agente usa la configuración automática del servidor DHCP. También tienen la capacidad de establecer manualmente la configuración de red cuando se ejecuta el agente de inicio en el equipo.

Preconfiguración de múltiples conexiones de red

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

Puede cambiar la configuración, excepto por la dirección MAC, o establecer la configuración para una NIC no existente, de ser necesario.

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

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

Puede personalizar los dispositivos de arranque para cualquier equipo, y no sólo para el equipo en donde se crea el dispositivo. Para hacerlo, configure las NIC de acuerdo con el orden de ranuras del equipo. Nic1 ocupa la ranura más cercana al procesador, NIC2 es la siguiente ranura. Cuando el agente de inicio se ejecuta en el equipo, no encontrará NIC con direcciones MAC conocidas y configurará las NIC en el mismo orden que usted.

Ejemplo

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

Puerto de red

Cuando cree dispositivos de arranque, tiene la opción de preconfigurar el puerto de red que el agente de inicio escuchará para la conexión entrante. La opción disponible entre:

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

Si no se preconfiguró el puerto, el agente usa el número de puerto predeterminado (9876.) Este puerto que se usa predeterminado por la consola de administración de Acronis Backup & Recovery 10. La configuración temporal del puerto está disponible. Mientras se conecta la consola al agente, especifique el puerto para dicha sesión en la dirección URL <Agent-IP>:<port>.

6.10.2 Conexión a un equipo que se inició desde un dispositivo

Una vez que un equipo inicia desde un dispositivo de inicio, la terminal del equipo muestra una ventana de inicio con la dirección IP que el servidor DHCP proporcionó o la establecida de acuerdo a los valores preconfigurados.

Conexión remota

Para conectar el equipo remotamente, seleccione **Conectar -> Administración de un equipo remoto** en la consola de menú y especifique una de las direcciones IP del equipo. Proporcione el nombre de usuario y contraseña si se establecieron cuando se creó el dispositivo de arranque.

Conexión Local

La consola de administración Acronis Backup & Recovery 10 está siempre presente en el dispositivo de arranque. Cualquiera que tenga acceso físico a la terminal del equipo puede ejecutar la consola y conectarse. Sólo haga clic en **Ejecutar la Consola de administración** en la ventana de inicio del agente de arranque.

6.10.3 Trabajo desde dispositivo de arranque

Las operaciones que se realizan en equipos que iniciaron desde dispositivo de arranque son muy parecidas a las copias de seguridad y la recuperación en el sistema operativo. La diferencia es la siguiente:

1. Las letras de los discos que se ven en los dispositivos de inicio de estilo Windows pueden diferir de la manera en que Windows identifica las unidades. Por ejemplo, la unidad D: en la utilidad de rescate puede corresponder a la unidad E: de Windows.

   ¡Tenga cuidado! Para estar seguro, se aconseja asignar nombres únicos a los volúmenes.

2. Los dispositivos de inicio de estilo Linux muestran los discos y volúmenes locales como desmontados (sda1, sda2...).
3. El dispositivo de arranque de estilo Linux no puede realizar copias de seguridad en un volumen formateado con NTFS. Si es necesario, cambie al estilo de Windows.
4. Puede cambiar el dispositivo de arranque entre el estilo de Windows y el de Linux al seleccionar **Herramientas** > **Cambiar la representación del volumen**.
5. Los medios de GUI no tienen un árbol de **Navegación**. Use el menú de **Navegación** para navegar entre las vistas.
6. No se pueden programar las tareas; de hecho, tampoco se pueden crear las tareas. Si necesita repetir la operación, configúrela desde cero.
7. La vida útil del registro se limita a la sesión actual. Puede guardar todo el registro o las entradas del registro filtradas a en un archivo.
8. Las bóvedas centralizadas no se muestran en el árbol de carpetas de la ventana de **Archivos**.

   Para acceder a una bóveda gestionada, escriba la siguiente cadena en el campo de **Ruta**:

   bsp://dirección_nodo/nombre_bóveda/

   Para acceder a una bóveda centralizada sin gestionar, escriba la ruta completa de la carpeta de la bóveda.

   Después de introducir las credenciales de acceso, verá una lista de los archivos comprimidos que se encuentran en la bóveda.

Configuración del modo de visualización

Para un equipo que se inicia desde un dispositivo, se detecta automáticamente un modo de vídeo de visualización basado en la configuración del hardware (especificaciones de la tarjeta del monitor y de los gráficos). Si, por alguna razón, el modo vídeo se detecta de manera incorrecta, realice lo siguiente:

1. Pulse F11 en el menú de inicio.
2. Añada el siguiente comando en la entrada de comandos: **vga=ask** y prosiga con el arranque.
3. En la lista de modos de vídeo compatibles, escoja el correcto al escribir su número (por ejemplo, **318**) y pulse INTRO.

Si no desea seguir este procedimiento cada vez que inicie desde un dispositivo en una configuración de hardware en concreto, cree de nuevo el dispositivo de arranque con el número de modo apropiado (en nuestro ejemplo, **vga=0x318**) escrito en la ventana **Parámetros del kernel** (consulte la sección Generador de dispositivos de arranque (pág. 173) para obtener más detalles).

Configuración de los dispositivos iSCSI y NDAS

Esta sección describe cómo configurar los dispositivos de la Internet Small Computer System Interface (iSCSI) y los de Network Direct Attached Storage (NDAS) mientras trabaja desde un dispositivo de arranque.

Estos dispositivos están conectados al equipo a través de una interfaz de red y aparecen como si fueran dispositivos asociados localmente. En la red, un dispositivo iSCSI se identifica mediante su dirección IP y un dispositivo NDAS mediante el ID del dispositivo.

Un dispositivo iSCSI a veces se denomina un objetivo iSCSI. Un componente hardware o software que proporciona interacción entre el equipo y el objetivo iSCSI se denomina un iniciador iSCSI. El nombre del iniciador iSCSI generalmente está definido por un administrador del servidor que aloja el dispositivo.

Para añadir un dispositivo iSCSI

1. En un dispositivo de arranque (basado en Linux o basado en PE), ejecute la consola de gestión.
2. Haga clic en **Configurar dispositivos iSCSI/NDAS** (en un medio basado en Linux) o **Ejecutar la configuración iSCSI** (en un medio basado en PE).
3. Especifique la dirección de IP y el puerto del servidor del dispositivo iSCSI y el nombre del iniciador iSCSI.
4. Si el servidor requiere autenticación, especifique el nombre de usuario y contraseña para el mismo.
5. Haga clic en **Aceptar**.
6. Seleccione el dispositivo iSCSI de la lista y después haga clic en **Conectar**.
7. Si se le solicita, especifique el nombre de usuario y la contraseña para acceder al dispositivo iSCSI.

Para añadir un dispositivo NDAS

1. En un dispositivo de arranque basado en Linux, ejecute la consola de gestión.
2. Haga clic en **Configurar dispositivos iSCSI/NDAS**.
3. En **Dispositivos NDAS**, haga clic en **Añadir dispositivo**.
4. Especifique el ID de 20 caracteres del dispositivo.
5. Para desea permitir datos de escritura en el dispositivo, especifique la clave de escritura de cinco caracteres. Sin esta clave, el dispositivo solo estará disponible en el modo de solo lectura.

6. Haga clic en **Aceptar**.

6.10.4 Lista de comandos y utilidades disponibles en los dispositivos de inicio basados en Linux

Los dispositivos de inicio basados en Linux contienen los siguientes comandos y utilidades de línea de comandos, que puede usar cuando se ejecuta un shell de comando. Para comenzar el shell de comandos, pulse CTRL+ALT+F2 mientras esté en la consola de gestión del dispositivo de inicio.

Utilidades de línea de comandos Acronis

- `acronis`
- `asamba`
- `lash`
- `restoreraids`
- `trueimagecmd`
- `trueimagemnt`

Comandos y utilidades de Linux

`busybox`	`ifconfig`	`rm`
`cat`	`init`	`rmmod`
`cdrecord`	`insmod`	`route`
`chmod`	`iscsiadm`	`scp`
`chown`	`kill`	`scsi_id`
`chroot`	`kpartx`	`sed`
`cp`	`ln`	`sg_map26`
`dd`	`ls`	`sh`
`df`	`lspci`	`apagar`
`dmesg`	`lvm`	`ssh`
`dmraid`	`mdadm`	`sshd`
`e2fsck`	`mkdir`	`strace`
`e2label`	`mke2fs`	`swapoff`
`echo`	`mknod`	`swapon`
`egrep`	`mkswap`	`sysinfo`
`fdisk`	`more`	`tar`
`fsck`	`montar`	`tune2fs`
`fxload`	`mtx`	`udev`
`gawk`	`mv`	`udevinfo`
`gpm`	`pccardctl`	`udevstart`

```
grep       ping         umount
growisofs  pktsetup     uuidgen
grub       poweroff     vconfig
gunzip     ps           vi
halt       raidautorun  zcat
hexdump    readcd
hotplug    reiniciar
```

6.10.5 Recuperación de los dispositivos MD y los volúmenes lógicos

Para recuperar los dispositivos MD, conocidos como Linux Software RAID, y/o dispositivos creados por el Administrador de volúmenes lógicos (LVM), conocidos como volúmenes lógicos, necesita crear la estructura del volumen correspondiente antes de comenzar la recuperación.

Puede crear la estructura del volumen de una de las siguientes maneras:

- Automáticamente, en dispositivos de arranque basados en Linux, utilizando la consola de gestión o una secuencia de comandos; consulte Creación de la estructura del volumen automáticamente (pág. 180).
- Manualmente utilizando las utilidades **mdadm** y **lvm** . Vea Creación de la estructura de volumen de forma manual (pág. 181).

Creación de la estructura del volumen automáticamente

Asumamos que usted ha guardado (pág. 36) la estructura de volumen en el directorio /etc/Acronis y que el volumen para este directorio está incluido en el archivo comprimido.

Para recrear la estructura del volumen en el dispositivo de arranque basado en Linux, utilice cualquiera de los métodos que se describen abajo.

Precaución: *Como resultado de los siguientes procedimientos, la estructura actual del volumen en el equipo se cambiará por una almacenada en el archivo comprimido. Esto destruirá los datos que se encuentran almacenados actualmente en alguno o todos los discos duros del equipo.*

Si ha cambiado la configuración del disco. Un dispositivo MD o volumen lógico reside en uno o más discos, cada uno con un tamaño propio. Si entre la realización de la copia de seguridad y la recuperación cambió cualquiera de estos discos o si está recuperando los volúmenes en equipos diferentes, asegúrese de que la configuración del disco nuevo incluye por lo menos una cantidad de discos de tamaños iguales a los de los originales.

Para crear la estructura del volumen utilizando la consola de gestión

1. Inicie el equipo desde una dispositivo de arranque basado en Linux.
2. Haga clic en **Acronis Bootable Agent**. Luego, haga clic en **Ejecutar la consola de administración**.
3. En la consola de gestión, haga clic en **Recuperar**.

   Bajo los contenidos del archivo comprimido, Acronis Backup & Recovery 10 mostrará un mensaje indicando que ha detectado información sobre la estructura del volumen.
4. Haga clic en **Detalles** en el área en la que se encuentra ese mensaje.
5. Revise la estructura del volumen y luego haga clic en **Aplicar RAID/LVM** para crearla.

Creación de la estructura del volumen con una secuencia de comandos

1. Inicie el equipo desde una dispositivo de arranque basado en Linux.
2. Haga clic en **Acronis Bootable Agent**. Luego, haga clic en **Ejecutar la consola de administración**.
3. En la barra de herramientas, haga clic en **Acciones** y luego haga clic en **Ejecutar shell**. O bien, puede pulsar CTRL+ALT+F2.
4. Ejecute la secuencia de comandos **restoreraids.sh**, especificando el nombre completo del archivo, por ejemplo:

   ```
   /bin/restoreraids.sh
   smb://server/backups/linux_machine_2010_01_02_12_00_00_123D.tib
   ```
5. Vuelva a la consola de administración presionando CTRL+ALT+F1, o ejecutando el comando: **/bin/product**
6. Haga clic en **Recuperar**, luego especifique la ruta al archivo comprimido y otros parámetros necesarios, y luego haga clic en **Aceptar.**

Si Acronis Backup & Recovery 10 no crease la estructura del volumen (o si no está presente en el archivo comprimido), cree la estructura de forma manual.

Creación de la estructura del volumen manualmente

A continuación se brinda un procedimiento general para la recuperación de dispositivos MD y volúmenes lógicos utilizando los dispositivos de arranque basados en Linux y un ejemplo de dicha recuperación. Puede utilizar un procedimiento parecido en Linux.

Para recuperar dispositivos MD y volúmenes lógicos.

1. Inicie el equipo desde una dispositivo de arranque basado en Linux.
2. Haga clic en **Acronis Bootable Agent**. Luego, haga clic en **Ejecutar la consola de administración**.
3. En la barra de herramientas, haga clic en **Acciones** y luego haga clic en **Ejecutar shell**. O bien, puede pulsar CTRL+ALT+F2.
4. De ser necesario, examine la estructura de volúmenes almacenados en el archivo comprimido, mediante la utilidad **trueimagecmd**. Además, puede usar la utilidad **trueimagemnt** para montar uno o más de estos volúmenes como si fueran volúmenes comunes (consulte "Montaje de volúmenes de copia de seguridad" que se desarrolla a continuación dentro de este tema).
5. Cree la estructura del volumen de acuerdo con el archivo comprimido, mediante la utilidad **mdadm** (para los dispositivos MD), la utilidad **lvm** (para volúmenes lógicos) o ambas.

   Nota: *Las utilidades frl Administrador de volúmenes lógico como* ***pvcreate*** *y* ***vgcreate****, que suelen estar disponibles en Linux, no están incluidas en el entorno de los dispositivos de inicio, por lo que necesita usar la utilidad* ***lvm*** *con un comando correspondiente:* ***lvm pvcreate****,* ***lvm vgcreate****, etc.*
6. Si montó previamente la copia de seguridad con la utilidad **trueimagemnt**, use esta utilidad de nuevo para desmontar la copia de seguridad (consulte "Montaje de volúmenes de copias de seguridad", más adelante).
7. Vuelva a la consola de administración presionando CTRL+ALT+F1, o ejecutando el comando: **/bin/product**

   (No reinicie el equipo en este momento. De otro modo, tendrá que crear la estructura del volumen de nuevo).
8. Haga clic en **Recuperar**, luego especifique la ruta al archivo comprimido y otros parámetros necesarios, y luego haga clic en **Aceptar.**

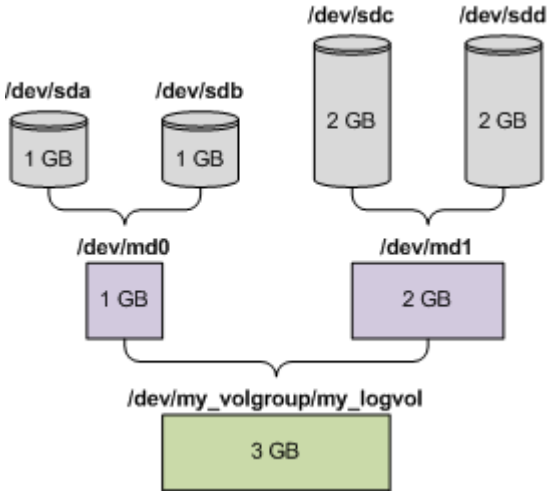
Nota: *Este procedimiento no funciona cuando se conecta remotamente a Acronis Backup & Recovery 10 Bootable Agent porque el shell del comando no está disponible en este caso.*

Ejemplo

Suponga que se realiza previamente una copia de seguridad del disco de un equipo con la siguiente configuración de disco:

- El equipo tiene dos discos duros SCSI: uno de 1 gigabyte y otro de 2 gigabytes, montados en **/dev/sda**, **/dev/sdb**, **/dev/sdc**, y **/dev/sdd,** respectivamente.
- El primer y el segundo par de discos duros están configurados como dos dispositivos MD, ambos en la configuración RAID-1, y están montados en **/dev/md0** y **/dev/md1**, respectivamente.
- Un volumen lógico está basado en dos dispositivos MD y está montado en **/dev/my_volgroup/my_logvol**.

La siguiente imagen ilustra esta configuración.



Haga lo siguiente para recuperar datos del archivo comprimido.

Paso 1: Creación de la estructura del volumen

1. Inicie el equipo desde una dispositivo de arranque basado en Linux.
2. En la consola de administración, presione CTRL+ALT+F2.
3. Ejecute los siguientes comandos para crear los dispositivos MD:

```
mdadm --create /dev/md0 --level=1 --raid-devices=2 /dev/sd[ab]
mdadm --create /dev/md1 --level=1 --raid-devices=2 /dev/sd[cd]
```

4. Ejecute los siguientes comandos para crear el volumen lógico del grupo:

Precaución: *El comando* ***pvcreate*** *destruye todos los datos en los dispositivos* ***/dev/md0*** *y* ***/dev/md1****.*

```
lvm pvcreate /dev/md0 /dev/md1
lvm vgcreate my_volgroup /dev/md0 /dev/md1
lvm vgdisplay
```

La salida del comando **lvm vgdisplay** será similar a:

```
--- Volume group ---
VG Name     my_volgroup
...
VG Access   read/write
VG Status   resizable
...
VG Size     1.99 GB
...
VG UUID     0qoQ4l-Vk7W-yDG3-uF1l-Q2AL-C0z0-vMeACu
```

5. Ejecute el siguiente comando para crear el volumen lógico, en el parámetro**-L**, y especifique el tamaño dado por **VG Size**:

```
lvm lvcreate -L1.99G --name my_logvol my_volgroup
```

6. Active el volumen del grupo al ejecutar el siguiente comando:

```
lvm vgchange -a y my_volgroup
```

7. Presione CTRL+ALT+F1 para volver a la consola de administración.

Paso 2: Comienzo de la recuperación

1. En la consola de gestión, haga clic en **Recuperar**.
2. En **Archivo comprimido**, haga clic en **Cambio** y luego especifique el nombre del archivo comprimido.
3. En **Copia de Seguridad**, haga clic en **Cambio** y luego selecciones la copia de seguridad de la que quiere recuperar datos.
4. En los **tipos de datos**, seleccione **Volúmene**s.
5. En **Elementos a recuperar**, seleccione la casilla de verificación que se encuentra junto a **my_volgroup-my_logvol**.
6. En **Dónde recuperar,** haga clic en **Cambio** y luego seleccione el volumen lógico que creó en el Paso 1. Haga clic en los botones para expandir la lista de discos.
7. Haga clic en **Aceptar** para comenzar la recuperación.

Para obtener una lista completa de comandos y utilidades que puede usar en el entorno de los dispositivos de arranque, consulte Lista de comandos y utilidades disponibles en dispositivos de arranque basados en Linux (pág. 179). Para obtener una descripción detallada de las utilidades **trueimagecmd** y **trueimagemnt**, consulte la referencia de línea de comandos Acronis Backup & Recovery 10.

Montaje de los volúmenes de copia de seguridad

Se recomienda a montar un volumen almacenado en una copia de seguridad del disco, por ejemplo, para ver algunos archivos antes de comenzar la recuperación.

Para montar un volumen de copia de seguridad

1. Use la lista de comandos **--list** para enumerar los volúmenes que están almacenados en la copia de seguridad. Por ejemplo:

```
trueimagecmd --list --filename:smb://server/backups/linux_machine.tib
```

La salida contendrá líneas similares a las siguientes:

```
Num  Idx Partition Flags Start Size      Type
---- --- --------- ----- ----- --------- ------
Disk 1:
         Table           0               Table
Disk 2:
         Table           0               Table
...
Dynamic & GPT Volumes:
DYN1 4   my_volgroup-my_logvol 12533760  Ext2
```

En el próximo paso, necesitará el índice del volumen, el cual se proporciona en la columna **idx**.

2. Use el comando **--mount** y especifique el índice del volumen en el parámetro **-i** Por ejemplo:

```
trueimagemnt --mount /mnt --filename smb://server/backups/linux_machine.tib -i
4
```

Este comando monta un volumen lógico DYN1 cuyo índice en la copia de seguridad es 4, en el punto de montaje /mnt.

Para montar un volumen de copia de seguridad

- Use el comando **--unmount** y especifique el punto de montaje del volumen como parámetro. Por ejemplo:

```
trueimagemnt --unmount /mnt
```

6.11 Recolección de información del sistema

La herramienta de recolección de información del sistema recopila información acerca del equipo al cual está conectada la consola de gestión y la guarda en un archivo. Es conveniente que proporcione este archivo cuando se ponga en contacto con la asistencia técnica de Acronis.

Esta opción está disponible en los dispositivos de inicios y para equipos donde Agente para Windows, Agente para Linux o Acronis Backup & Recovery 10 Management Server esté instalado.

Para recolectar la información del sistema

1. Seleccione **Ayuda** > **Recopilar información del sistema desde** 'nombre del equipo' en el menú superior de la consola de gestión.
2. Especifique dónde guardar al archivo con la información de sistema.

7 Glosario

A

Acronis Active Restore

La tecnología propietaria de Acronis que pone un sistema en línea inmediatamente después de que comience la recuperación del sistema. El sistema se inicia desde la copia de seguridad (pág. 189) y el equipo queda funcional y listo para proporcionar los servicios necesarios. Se recupera con la más alta prioridad a los datos requeridos para que se utilizarán para las solicitudes entrantes; todo lo demás se recupera en segundo plano. Limitaciones:

- La copia de seguridad se ubica en la unidad local (cualquier dispositivo disponible a través de BIOS, a excepción del inicio de red)
- No funciona con imágenes de Linux.

Acronis Secure Zone

Un volumen seguro para almacenar archivos comprimidos (pág. 186) de copias de seguridad dentro de un equipo gestionado (pág. 190). Ventajas:

- Permite la recuperación de un disco en el mismo disco en donde se encuentra la copia de seguridad del disco
- Ofrece un método rentable y útil para la protección de datos por fallos del software, virus, ataques o errores del operador
- Elimina la necesidad de medios o conexión de red diferentes para realizar copias de seguridad o recuperar los datos. Es especialmente útil para los usuarios móviles
- Puede utilizarse como la ubicación primaria para copias de seguridad de destino doble.

Limitaciones: Acronis Secure Zone no se puede organizar en un disco dinámico (pág. 189) o un disco que utilice el estilo de partición GPT.

Acronis Secure Zone se considera una bóveda personal (pág. 188).

Acronis Startup Recovery Manager (ASRM)

Una modificación del agente reiniciable (pág. 186), que reside en el disco del sistema y está configurado para iniciarse al momento del inicio al presionarse F11. Acronis Startup Recovery Manager elimina la necesidad de un dispositivo de rescate o conexión de red para iniciar la utilidad de rescate de inicio.

Acronis Startup Recovery Manager es muy útil para los usuarios móviles. En caso de fallo, el usuario reinicia el equipo, pulsa F11 cuando aparezca el aviso "Press F11 for Acronis Startup Recovery Manager..." y realiza recuperación de datos en la misma manera que con un medio de inicio común.

Limitación: requiere la reactivación de cargadores que no sean los de Windows ni GRUB.

Agente (Agente Acronis Backup & Recovery 10)

Una aplicación que realiza copias de seguridad de datos y recuperación, y que permite otras operaciones de gestión en el equipo (pág. 190), como gestión de tareas y operaciones con discos duros.

El tipo de datos con los que se puede realizar una copia de seguridad depende del tipo de agente. Acronis Backup & Recovery 10 incluye los agentes para realizar copias de seguridad de discos y archivos, y los agentes para copias de seguridad para máquinas virtuales que se encuentran en los servidores de virtualización.

Agente de inicio

Es una herramienta de rescate de inicio que incluye la mayor parte de la funcionalidad del agente Acronis Backup & Recovery 10 (pág. 185). El agente de inicio está basado en un núcleo de Linux. Se puede iniciar un equipo (pág. 190) desde un agente de inicio utilizando medios de inicio (pág. 195) o Acronis PXE Server. Las operaciones se pueden configurar y controlar tanto de manera local, por medio de una interfaz de usuario, como de manera remota, por medio de la consola (pág. 188).

Archivo comprimido

Consulte el archivo de copia de seguridad (pág. 186).

Archivo comprimido cifrado

Es un archivo cifrado de copias de seguridad (pág. 186) de acuerdo con Advanced Encryption Standard (AES). Cuando se establece la opción de cifrado y contraseña del archivo en las opciones de copia de seguridad (pág. 195), el agente (pág. 185) cifra cada copia de seguridad que pertenece al archivo antes de guardar la copia de seguridad a su destino.

El algoritmo criptográfico AES funciona en el modo Cipher-block chaining (CBC) y utiliza una clave generada de manera aleatoria con un tamaño definido por el usuario de 128, 192 ó 256 bits. Entonces se cifra la clave de cifrado con AES-256 con un hash SHA-256 de la contraseña como clave. No se almacena la contraseña en el disco o en el archivo de copia de seguridad, el hash de la contraseña se usa para verificación. Con esta seguridad con dos niveles, los datos de copia de seguridad están protegidos contra el acceso no autorizado.

Archivo de copia de seguridad (Archivo)

Un conjunto de copias de seguridad (pág. 189) creadas y gestionadas por un plan de copias de seguridad (pág. 196). Un archivo puede tener varias copias de seguridad completas (pág. 188), como también copias de seguridad diferenciales (pág. 189) e incrementales. (pág. 189) Las copias de seguridad que pertenecen al mismo archivo se guardan siempre en la misma ubicación. Los planes de copias de seguridad múltiples pueden copiar la misma ubicación en el mismo archivo, pero el modelo dominante es "un plan, un archivo".

Las copias de seguridad en un archivo son manejadas por completo por el plan de copia de seguridad. Las operaciones manuales con archivos (validación (pág. 199), visualización de contenidos, montaje y eliminación de copias de seguridad) se debería realizar con Acronis Backup & Recovery 10. No modifique sus archivos con herramientas incompatibles con Acronis, como Windows Explorer o gestores de terceros.

B

Bóveda

Es un lugar para almacenar archivos de copia de seguridad (pág. 186). Se puede organizar una bóveda en una unidad o medio extraíble local o de red, como una unidad USB externa. No hay configuración para el límite del tamaño de la bóveda o el número de copias de seguridad en una

bóveda. Puede limitar el tamaño de cada archivo con una limpieza (pág. 193), pero el tamaño total de los archivos almacenados en la bóveda sólo está limitado por el tamaño de almacenamiento.

Bóveda centralizada

Es una ubicación de red asignada por el administrador de management server (pág. 194) para que funcione como almacenamiento de archivos de copias de seguridad (pág. 186). Una bóveda centralizada puede ser gestionada por el nodo de almacenamiento (pág. 195) o quedar sin gestión. El tamaño y cantidad total de archivos almacenados en una bóveda centralizada están limitados solamente por el tamaño de almacenamiento.

Tan pronto como el administrador del management server crea una bóveda centralizada, el nombre y la ruta de la bóveda se distribuyen por todos los equipos registrados (pág. 190) en el servidor. El vínculo a la bóveda aparece en los equipos en la lista de bóvedas centralizadas. Cualquier plan de copia de seguridad (pág. 196) existente en los equipos, incluidos los planes locales, puede usar la bóveda centralizada.

En un equipo que no está registrado en el servidor de administración, un usuario que tiene privilegios para realizar copias de seguridad en la bóveda centralizada puede hacerlo al especificar la ruta completa a la bóveda. Si es una bóveda gestionada, los archivos del usuario serán gestionados por el nodo de almacenamiento como también los archivos almacenados en la bóveda.

Bóveda cifrada

Es una bóveda gestionada (pág. 187) en la que se cifra todo lo que se guarda y en donde el nodo de almacenamiento (pág. 195) descifra de modo claro todo lo que se lee, por medio de una clave de cifrado específica de la bóveda guardada en el nodo. En el caso de robo o acceso por una persona no autorizada, el malhechor no podrá descifrar los contenidos de la bóveda si no tiene acceso al nodo de almacenamiento. Los archivos cifrados (pág. 186) serán cifrados por encima de lo cifrado por el agente (pág. 185).

Bóveda de deduplicación

Es una bóveda gestionada (pág. 187) en la que se habilita la deduplicación (pág. 189).

Bóveda gestionada

Es una bóveda centralizada (pág. 187) gestionada por un nodo de almacenamiento (pág. 195). Se puede acceder a los archivos (pág. 186) en una bóveda gestionada de la siguiente manera:

bsp://node_address/vault_name/archive_name/

Físicamente, las bóvedas gestionadas pueden residir en una red compartida, SAN, NAS, en un disco duro local conectado al nodo de almacenamiento, o en una biblioteca de cintas conectada de manera local al nodo de almacenamiento. El nodo de almacenamiento realiza limpieza del lado del nodo de almacenamiento (pág. 194) y validación del lado del nodo de almacenamiento (pág. 199) por cada archivo almacenado en la bóveda gestionada. El administrador puede especificar las operaciones adicionales que el nodo de almacenamiento realizará (cifrado, deduplicación (pág. 189)).

Todas las bóvedas administradas son autónomas, es decir, contienen todos los metadatos que el nodo de almacenamiento necesita para administrar la bóveda. En caso de pérdida del nodo de almacenamiento o de daño de su base de datos, el nuevo nodo de almacenamiento recupera los metadatos y crea nuevamente la base de datos. Cuando la bóveda está conectada a otro nodo de almacenamiento, se realiza el mismo proceso.

Bóveda personal

Es una bóveda (pág. 186) local o de red creada por gestión directa (pág. 191). Una vez que se crea una bóveda personal, aparece un vínculo debajo del elemento **Bóvedas personales** del panel de **Navegación**. Varios equipos pueden usar la ubicación física, por ejemplo, una red compartida como una bóveda personal.

Bóveda sin gestionar

Es cualquier bóveda (pág. 186) que no esté gestionada (pág. 187).

C

Complemento de Acronis para WinPE

Una modificación del agente para Windows de Acronis Backup & Recovery 10 que puede ejecutarse en el entorno de preinstalación. Es posible añadir el complemento a una imagen WinPE (pág. 200) con el generador de dispositivos de inicio. El medio de inicio (pág. 195) resultante se puede usar para iniciar cualquier equipo compatible con PC y realizar,con ciertas limitaciones, la mayoría de las operaciones de gestión directa (pág. 191) sin la ayuda de un sistema operativo. Las operaciones se pueden configurar y controlar tanto de manera local, por medio de una interfaz de usuario, como de manera remota, por medio de la consola (pág. 188).

Consola (Acronis Backup & Recovery 10 Management Console)

Una herramienta para el acceso local o remoto de agentes Acronis (pág. 185) y Acronis Backup & Recovery 10 Management Server (pág. 194).

Una vez que se establece la conexión de la consola con el management server, el administrador establece y gestiona las políticas de copias de seguridad (pág. 197) y acceder a otra funcionalidad del servidor de gestión, es decir, realiza la gestión centralizada (pág. 191). El uso de la conexión directa de la consola y el agente, el administrador realiza gestión directa (pág. 191).

Consolidación

La combinación de dos o más copias de seguridad (pág. 189) subsecuentes que pertenecen al mismo archivo comprimido (pág. 186) en una sola copia de seguridad.

Se puede necesitar la consolidación cuando se elimina copias de seguridad, tanto de manera manual o durante la limpieza (pág. 193). Por ejemplo, las reglas de retención requiere la eliminación de una copia de seguridad completa (pág. 188) que caducó pero guarda la siguiente copia incremental (pág. 189). Las copias de seguridad serán combinadas en una sola copia de seguridad que tendrá la fecha del copia de seguridad incremental. Debido a que mover los archivos puede demorar mucho tiempo e implicar el uso de recursos del sistema, las reglas de retención proporcionan una opción para no eliminar las copias de seguridad con dependencias. En nuestro ejemplo, se conservará la copia de seguridad completa hasta que la copia incremental también sea obsoleta. Después, se eliminarán las copias de seguridad.

Copia de seguridad completa

Es una copia de seguridad (pág. 189) 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 del disco (Imagen)

Una copia de seguridad (pág. 189) que contiene una copia basada en un sector del disco o un volumen en una forma compacta. Por lo general, se copian sólo los sectores que contienen datos. Acronis Backup & Recovery 10 proporciona la opción de tomar una imagen sin procesar, es decir, copia todo los sectores del disco, lo que permite imágenes de sistemas de archivos no compatibles.

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. 188). 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 (pág. 189). Necesita tener acceso a otras copias de seguridad del mismo archivo (pág. 186) para restaurar los datos de una copia de seguridad incremental.

Crear copia de seguridad

Una copia de seguridad es el resultado de una única operación de copia de seguridad (pág. 196). Físicamente, es un archivo o un registro de cinta que contiene una copia de los datos en una fecha y hora específica. Los archivos de copia de seguridad creados con Acronis Backup & Recovery 10 tienen la extensión TIB. Los archivos TIB que son el resultado de una exportación (pág. 191) o consolidación (pág. 188) de una copia de seguridad también se denominan copias de seguridad.

D

Deduplicación

Es un método diferente de almacenamiento que duplica la misma información sólo una vez.

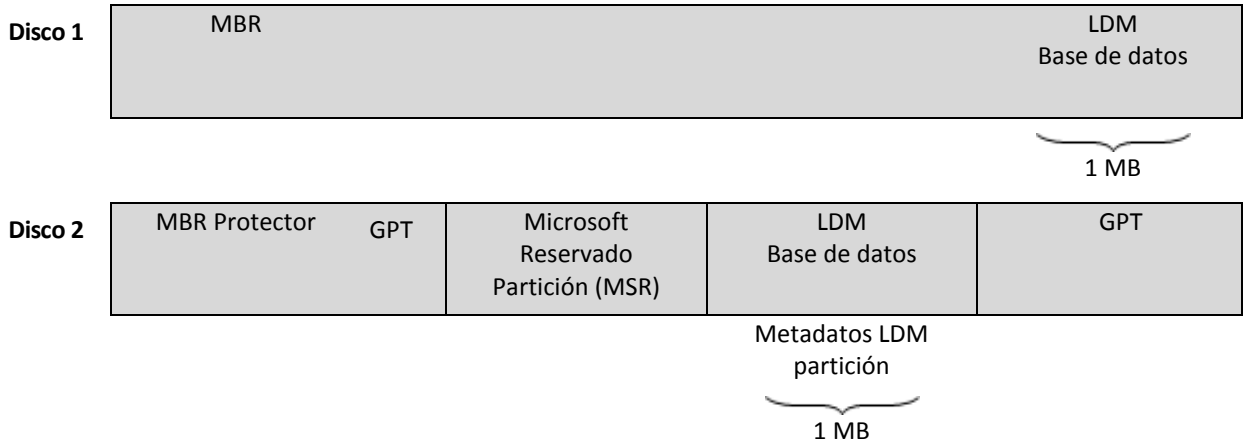
Acronis Backup & Recovery 10 puede aplicar la tecnología de desduplicación a los archivos de copia de seguridad (pág. 186) almacenados en los nodos de almacenamiento (pág. 195). Esto minimiza el espacio de almacenamiento de los archivos, el tráfico de copias de seguridad y el uso de la red durante las copias de seguridad.

Disco dinámico

Los discos duros gestionados con el Administrador de discos lógicos (LDM) disponible en Windows desde Windows 2000. LDM ayuda a asignar flexiblemente los volúmenes en un dispositivo de almacenamiento para una mejor tolerancia a fallos, mejor rendimiento o mayor tamaño de volumen.

Un disco dinámico puede usar tanto el estilo de partición Registro de inicio maestro (MBR) o Tabla de partición GUID (GPT). Además de MBR o GPT, cada disco dinámico tiene una base de datos oculta en donde LDM almacena la configuración de volúmenes dinámicos. Cada disco dinámico retiene toda la

información sobre los volúmenes dinámicos existentes en el grupo de discos, lo que mejora la confiabilidad del almacenamiento. La base de datos ocupa al menos 1 MB de un disco MBR. En un disco GPT, Windows crea una partición dedicada de metadatos LDM, lo que toma espacio de la partición reservada de Microsoft (MSR).



Los discos dinámicos organizados con discos MBR (Disco 1) y GPT (Disco 2).

Para obtener más información sobre los grupos de discos dinámicos, consulte el siguiente artículo de la Base de Conocimiento de Microsoft:

Gestión del disco (Windows XP Professional Resource Kit) http://technet.microsoft.com/es-es/library/bb457110.aspx.

816307 Mejores prácticas para el uso de los discos dinámicos en equipos con Windows Server 2003 http://support.microsoft.com/kb/816307/es.

E

Equipo

Es un equipo físico o virtual identificado por la instalación del sistema operativo. Los equipos con varios sistemas operativos (sistemas con múltiples inicios) son considerados como equipos múltiples.

Equipo físico

En el Acronis Backup & Recovery 10 Management Server, un equipo físico es lo mismo al equipo registrado (pág. 190). Se considera que una máquina virtual es física si hay un agente de Acronis Backup & Recovery 10 instalado en el equipo y el equipo está registrado en el management server.

Equipo gestionado

Es un equipo (pág. 190), tanto físico como virtual cuando al menos tiene un agente instalado de Acronis Backup & Recovery 10. (pág. 185)

Equipo registrado

Un equipo (pág. 190) gestionado por el management server (pág. 194). Se puede registrar un solo equipo a la vez en un management server. Un equipo se encuentra registrado como resultado del proceso de registro (pág. 197).

Equipo virtual

En el Acronis Backup & Recovery 10 Management Server, se considera que es una máquina (pág. 190) es virtual si se puede realizar una copia de seguridad del servidor de virtualización sin instalar un agente (pág. 185) en el equipo. Una máquina virtual aparece en el management server después del registro del servidor de virtualización que alberga el equipo, ya que el agente Acronis Backup & Recovery 10 para máquinas virtuales está instalado en dicho servidor.

Esquema de copias de seguridad

Una parte del plan de copia de seguridad (pág. 196) que incluye el programa de copia de seguridad y (de manera opcional) las reglas de retención del programa de limpieza (pág. 193). Por ejemplo, realice una copia de seguridad completa (pág. 188) mensualmente en el último día del mes a las 10:00 h y una copia de seguridad incremental (pág. 189) los domingos a las 22:00 h. Elimina copias de seguridad que tienen más de tres meses. Verifica dichas copias de seguridad cada vez que se completa una operación de respaldo.

Acronis Backup & Recovery 10 ofrece la capacidad de usar programas conocidos y optimizados para copias de seguridad, como GFS y Torre de Hanói, para crear un esquema de copias de seguridad personalizado o hacer copias de seguridad solo una vez.

Exportar

Una operación que crea una copia de un archivo comprimido (pág. 186) o una copia parcial de un archivo comprimido en la ubicación especificada. La operación de exportación se puede aplicar a un único archivo comprimido, una única copia de seguridad (pág. 189) o a su selección de copias de seguridad que pertenecen al mismo archivo comprimido. Se puede exportar una bóveda (pág. 186) completa utilizando la interfaz de línea de comandos.

G

Generador de dispositivos

Es una herramienta dedicada a la creación de medios de inicio (pág. 195).

Gestión centralizada

La gestión de la infraestructura Acronis Backup & Recovery 10 por medio de una unidad de gestión central conocida como Acronis Backup & Recovery 10 Management Server (pág. 194). Las operaciones de gestión centralizada incluyen:

- Creación, aplicación y gestión de políticas de copias de seguridad (pág. 197)
- Creación y gestión de grupos dinámicos (pág. 193) y estáticos (pág. 193) de equipos (pág. 190)
- Gestión de las tareas (pág. 198) existentes en los equipos
- Creación y gestión de las bóvedas centralizadas (pág. 187) para el almacenamiento de archivos
- Gestión de nodos de almacenamiento (pág. 195)
- Actividades de supervisión de componentes de Acronis Backup & Recovery 10 , visualización del registro centralizado y más.

Gestión directa

Cualquier operación de gestión que se realice en un equipo gestionado (pág. 190) por medio de la conexión entre consola (pág. 188) y agente (pág. 185) (a diferencia de la gestión centralizada (pág. 191) en donde se configura las operaciones en el management server (pág. 194) y se propaga por el servidor de los equipos gestionados).

Las operaciones de gestión directa incluyen:

- La creación y gestión de planes de copias de seguridad locales (pág. 197)
- La creación y gestión de tareas locales (pág. 198), como tareas de recuperación
- La creación y gestión de la bóveda personal (pág. 188) y los archivos almacenados allí
- La visualización del estado, progreso y propiedades de las tareas centralizadas (pág. 198) que existen en el equipo
- Visualización y gestión del registro de las operaciones del agente
- Operaciones de gestión de disco, como la clonación del disco, creación del volumen, conversión de volumen.

Se realiza un tipo de gestión directa cuando se usa medios de inicio (pág. 195). También se pueden realizar algunas de las operaciones de gestión directa por medio de la interfaz del management server. Sin embargo, esto implica tanto una conexión explícita como implícita del equipo seleccionado.

GFS (Abuelo-padre-hijo)

Un popular esquema de copia de seguridad (pág. 191) que permite el mantenimiento de un equilibrio óptimo entre el tamaño del archivo de copia de seguridad (pág. 186) y el número de los puntos de recuperación (pág. 197) disponibles del archivo. GFS permite la recuperación con resolución diaria para los últimos días, una resolución semanal por las últimas semanas y una resolución mensual para cualquier momento en el pasado.

Para más información, consulte esquema de copias de seguridad GFS (pág. 25).

Grupo de disco

Es una variedad de discos dinámicos (pág. 189) que almacenan los datos comunes de configuración en sus bases de datos LDM y por lo tanto se pueden gestionar como uno solo. Por lo general, todos los discos dinámicos creados dentro del mismo equipo (pág. 190) son miembros del mismo grupo de discos.

Tan pronto como se cree el primer disco dinámico con LDM u otra herramienta de gestión de discos, el nombre del grupo de discos se encuentra en la clave del registro HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\dmio\Boot Info\Primary Disk Group\Name.

Los discos creados o importados a continuación son agregados al mismo grupo de discos. El grupo existe siempre que exista al menos uno de sus miembros. Una vez que se desconecta el último disco dinámico o se lo convierte a básico, el grupo queda suspendido, si bien su nombre queda en la clave de registro que se nombró antes. En el caso de que se conecte o se cree de nuevo un disco, se crea un grupo de discos con un nombre incremental.

Cuando se mueva un grupo de discos a otro equipo, se lo considerará como "externo" y no se podrá usar hasta que se lo importe al grupo de discos existentes. El proceso de importación actualiza los datos de configuración tanto de los discos locales como externos para que puedan formar una sola

entidad. Los grupos externos se importan tal como están (tendrán el nombre original) si no existe el grupo de discos en el equipo.

Para obtener más información sobre los grupos de discos, consulte el siguiente artículo de la Base de Conocimiento de Microsoft:

222189 Descripción de Grupos de Discos en Administrador de discos de Windows http://support.microsoft.com/kb/222189/es.

Grupo dinámico

Es un grupo de equipos (pág. 190) que el management server (pág. 194) completa automáticamente de acuerdo a los criterios de pertenencia que especifica el administrador. Acronis Backup & Recovery 10 ofrece los siguientes criterios de pertenencia:

- Sistema operativo
- Unidad organizativa de Active Directory
- Rango de dirección IP.

Un equipo sigue siendo parte de un grupo dinámico siempre que el equipo cumpla con los criterio del grupo. Se elimina automáticamente al equipo del grupo tan pronto como

- las propiedades del equipo cambian para que el equipo deje de cumplir con los criterios ó
- el administrador cambia los criterios para que el equipo deje de cumplir con los criterios.

No hay manera de eliminar manualmente un equipo de una grupo dinámico, excepto por la eliminación del equipo del management server.

Grupo estático

Es un grupo de equipos que el administrador del management server (pág. 194) poblará manualmente al cargar los equipos al grupo. Un equipo permanece en un grupo estático hasta que el administrador elimina del grupo o del management server.

Grupo incorporado

Es un grupo de equipos que siempre existe en un management server (pág. 194).

Un management server tiene dos grupos integrados que contienen dos equipos de cada tipo: Todos los equipos físicos (pág. 190), todas las máquinas virtuales (pág. 190).

No se pueden eliminar, ni mover a otros grupos o modificar manualmente a los grupos integrados. Los grupos personalizados no pueden ser creados dentro de grupos integrados. No hay manera de quitar un equipo físico del grupo integrado, salvo por la eliminación del equipo del management server. Las máquinas virtuales son eliminadas como resultado de la eliminación del servidor.

Se puede aplicar una política de copia de seguridad (pág. 197) en un grupo integrado.

I

Imagen

El mismo que en Copia de seguridad del disco (pág. 189).

L

Limpieza

Es la eliminación de copias de seguridad (pág. 189) de un archivo de copia de seguridad (pág. 186) para eliminar las copias de seguridad desactualizadas o prevenir que el archivo exceda el tamaño deseado.

La limpieza incluye la aplicación a un archivo de reglas de retención establecidas por el plan de copia de seguridad (pág. 196) que produce el archivo. Esta operación verifica si el archivo excede su tamaño máximo o para las copias de seguridad caducadas. Esto puede eliminar las copias de seguridad, dependiendo de si se exceden las reglas de retención.

Para obtener más información, consulte: Reglas de retención (pág. 32).

Limpieza del lado del agente

La limpieza (pág. 193) realizada por un agente (pág. 185) de acuerdo al plan de copia de seguridad (pág. 196) que produce el archivo (pág. 186). La limpieza del lado del agente la realizan las bóvedas sin gestionar (pág. 188).

Limpieza del lado del nodo de almacenamiento

La limpieza (pág. 193) realizada por un nodo de almacenamient (pág. 195)o de acuerdo a los planes de copias de seguridad (pág. 196) que guarda los archivos (pág. 186) en una bóveda gestionada (pág. 187). Como es una alternativa a la limpieza del lado del agente (pág. 194), la limpieza del lado del nodo de almacenamiento evita la carga innecesaria de la CPU de los servidores de producción.

Puesto que el programa de limpieza existe en el equipo (pág. 190) en donde está el agente (pág. 185), y por lo tanto usa la hora y sucesos del equipo, el agente debe iniciar la limpieza del lado del nodo de almacenamiento cada vez que sucede el momento o suceso programado. Para hacerlo, el agente debe estar en línea.

La siguiente tabla resume los tipos de limpieza usados en Acronis Backup & Recovery 10.

	Limpieza	
	Del lado del agente	**Almacenamiento del lado del nodo**
Se aplica a:	Archivo comprimido	Archivo comprimido
Iniciado por:	Agente	Agente
Realizado por:	Agente	Nodo de almacenamiento
Programación establecida por:	Plan de copia de seguridad	Plan de copia de seguridad
Reglas de retención establecidas por:	Plan de copia de seguridad	Plan de copia de seguridad

M

Management server (Acronis Backup & Recovery 10 Management Server)

Es un servidor central que gestiona la protección de datos dentro de la red empresarial. Acronis Backup & Recovery 10 Management Server le proporciona al administrador lo siguiente:

- un punto de acceso a la infraestructura Acronis Backup & Recovery 10
- Una manera fácil de proteger los datos en varios equipos (pág. 190) con políticas de copia de seguridad (pág. 197) y agrupación
- Funcionalidad de supervisión en toda la empresa
- La capacidad de crear bóvedas centralizadas (pág. 187) para guardar los archivos de copias de seguridad (pág. 186) de la empresa.
- La capacidad de gestionar los nodos de almacenamiento (pág. 195).

Si hay varios management server en la red, funcionan independientemente, gestionan diferentes equipos y utilizan las bóvedas centralizadas para almacenamiento de archivos.

Medio de inicio

Es un medio físico (CD, DVD, unidad de memoria flash USB u otros medios admitidos por el BIOS del equipo (pág. 190) que se usa como dispositivo de inicio) que contienen el agente de inicio (pág. 186) o en el entorno de preinstalación de Windows (WinPE) (pág. 200) con el complemento Acronis para WinPE (pág. 188). Se puede iniciar un equipo en los entornos antedichos que se usan el inicio por red de Acronis PXE Server o Servicio de Instalación Remota (RIS). Estos servidores con componentes de inicio cargados también pueden ser medios de inicio.

Los dispositivos de arranque se usan con frecuencia para:

- recuperar de un sistema operativo que no puede iniciar
- acceder a los datos que sobrevivieron en un sistema dañado y realizar copias de seguridad de éstos
- implementar un sistema operativo desde cero
- Creación completa de volúmenes básicos o dinámicos (pág. 199)
- Copia de seguridad sector por sector de un disco que tiene un sistema de archivos incompatible.
- realizar copias de seguridad fuera de línea de cualquier dato que no se puede incluir en la copia de seguridad en línea por acceso restricto, con un bloqueo permanente por las aplicaciones en ejecución o por cualquier otra razón.

N

Nodo de almacenamiento (Acronis Backup & Recovery 10 Nodo de almacenamiento)

Es un servidor que permite optimizar el uso de diversos recursos necesarios para la protección de los datos de una empresa. Este objetivo se logra al organizar las bóvedas gestionadas (pág. 187). El nodo de almacenamiento le permite al administrador:

- Evita la carga innecesaria de la CPU de los equipos gestionados (pág. 190) al usar la limpieza del lado de los nodos de almacenamiento (pág. 194) y la validación del lado del nodo de almacenamiento (pág. 199)
- Reduce drásticamente el tráfico de la copia de seguridad y el espacio de almacenamiento que ocupan los archivos (pág. 186) al usar la deduplicación (pág. 189)
- Previene que malhechores tengan acceso a los archivos de copias de seguridad, incluso en caso de robo del medio de almacenamiento, al usar bóvedas cifradas (pág. 187).

O

Opciones de copia de seguridad

Son los parámetros de configuración de una operación de copia de seguridad (pág. 196) como comandos pre/post de copia de seguridad, asignación del máximo ancho de banda de la red para el flujo de la copia de seguridad o del nivel de compresión de datos. Las opciones de copia de seguridad son parte del plan de copia de seguridad (pág. 196).

Operación de copia de seguridad

Es una operación que crea una copia de los datos que existen en el disco duro del equipo (pág. 190) para la recuperación o reversión de los datos a una fecha y hora específicos.

P

Plan

Consulte el plan de copia de seguridad (pág. 196).

Plan de copia de seguridad (Plan)

Es un conjunto de reglas que especifican como se protegerán los datos en algún equipo. Un plan de copia de seguridad especifica:

- Los datos para incluir en la copia de seguridad
- La ubicación en donde se almacenará el archivo de copia de seguridad (pág. 186) (el nombre y ubicación del archivo de copia de seguridad)
- El esquema de copia de seguridad (pág. 191) incluye el programa de copia de seguridad y de manera opcional las reglas de retención
- De manera opcional, el archivo de validación de reglas (pág. 198)
- Las opciones de copia de seguridad (pág. 195).

Por ejemplo, un plan de copia de seguridad puede contener la siguiente información:

- Copia de seguridad del volumen C: **(estos son los datos que el plan protegerá)**
- Nombre al archivo como MySystemVolume y ubíquelo en \\server\backups\ (**es el nombre y la ubicación del archivo**)
- Realiza una copia de seguridad completa por mes en el último día del mes a las 10:00 y copias de seguridad incrementales los domingos a las 22:00. Elimina la copias de seguridad que tienen más de tres meses **(es el esquema de copia de seguridad)**
- Valida la última copia de seguridad inmediatamente después de su creación **(es una regla de validación)**
- Protege el archivo con una contraseña **(es una opción).**

Físicamente, un plan de copia de seguridad es un paquete de tareas (pág. 198) configuradas para la ejecución en un equipo gestionado (pág. 190).

Se puede crear un plan de copia de seguridad directamente en el equipo (plan local) o puede aparecer en el equipo como resultado de la implementación de una política de copia de seguridad (pág. 197) (plan centralizado (pág. 196)).

Plan de copia de seguridad centralizado

Un plan de copia de seguridad (pág. 196) que parece en el equipo gestionado (pág. 190) como resultado de la implementación de la política de la copia de seguridad (pág. 197) del management server (pág. 194). Dicho plan se puede modificar sólo al editar la política de copia de seguridad.

Plan de copia de seguridad local

Es un plan de copia de seguridad (pág. 196) creado en un equipo gestionado (pág. 190) por medio de la gestión directa (pág. 191).

Política

Consulte la política de copias de seguridad (pág. 197).

Política de copia de seguridad (Política)

El administrador de Management server (pág. 194) crea las plantillas del plan de copia de seguridad y las almacena en el management server. Una política de copias de seguridad tiene las mismas reglas que un plan de copias de seguridad, pero no se pueden especificar los datos a respaldar explícitamente. En cambio, se pueden usar las reglas de selección (pág. 198), como las variables de entorno. Debido a la flexibilidad de la selección, una política de copias de seguridad se puede aplicar centralmente a varios equipos. Si se especifica explícitamente un elemento de datos (p. ej. /dev/sda o C:\Windows), la política realizará copias de seguridad del elemento en cada equipo en donde existe la ruta exacta.

Al aplicar la política a un grupo de equipos, el administrador implementa varios planes de copias de seguridad con una sola acción.

El flujo de trabajo cuando se usan políticas es las siguiente:

1. El administrador crea la política de seguridad.
2. El administrador aplica la política a un grupo de equipos o a un solo equipo (pág. 190).
3. El management server implementa la política en los equipos.
4. En cada equipo, el agente (pág. 185) instalado en el equipo encuentra los elementos de datos por medio de las reglas de selección. Por ejemplo, si la regla de selección es [Todos los volúmenes], se hará una copia de seguridad de todo el equipo.
5. En cada equipo, el agente instalado crea un plan de copias de seguridad (pág. 196) por medio de otras reglas especificadas por la política. A este plan de copia de seguridad se lo denomina plan centralizado (pág. 196).
6. En cada equipo, el agente instalado crea un conjunto de tareas centralizadas (pág. 198) que lleva a cabo el plan.

Punto de recuperación

Es la hora y fecha a la que se puede revertir los datos de la copia de seguridad.

R

Registro

Es un proceso que agrega un equipo gestionado (pág. 190) a un management server (pág. 194).

El registro establece una relación de confianza entre el agente (pág. 185) del equipo y el servidor. Durante el registro, la consola recupera el certificado del cliente de management server y lo pasa al agente que lo usa después para autenticar los clientes que intentan establecer una conexión. Esto evita intentos de ataques a la red que consisten en establecer una conexión falsa de parte de un miembro de confianza (management server).

Regla de selección

Es una parte de la política de copias de seguridad (pág. 197). Le permite al administrador del management server (pág. 194) la selección de los datos a respaldar dentro de un equipo.

Reglas de validación

Es una parte de la política de copias de seguridad (pág. 196). Las reglas que definen cómo y la asiduidad para realizar la validación y si la validación (pág. 199) de todo el archivo (pág. 186) o la última copia de seguridad del archivo.

T

Tarea

En AcronisBackup & Recovery 10, una tarea es un conjunto de acciones secuenciales que deben realizarse en un equipo gestionado (pág. 190) cuando se llega a un tiempo o sucede cierto suceso. Las acciones se describen en un archivo de secuencia de comandos xml. La condición de inicio (programa) existe en las claves protegidas del registro.

Tarea centralizada

Es una tarea (pág. 198) que pertenece a un plan de copia de seguridad centralizada (pág. 196). Dicha tarea aparece en el equipo gestionado (pág. 190) como resultado de la implementación de la política de copia de seguridad (pág. 197) del management server (pág. 194) y se puede modificar sólo por la edición de la política de copia de edición.

Tarea local

Es una tarea (pág. 198) que pertenece al plan local de copias de seguridad (pág. 197) o tarea que no pertenece a un plan, como una tarea de recuperación. Sólo se puede modificar una tarea local que pertenece a una plan de copia de seguridad al editar el plan; otras tareas locales se pueden modificar directamente.

Torres de Hanói

Un popular esquema de copia de seguridad (pág. 191) que permite el mantenimiento de un equilibrio óptimo entre el tamaño del archivo de copia de seguridad (pág. 186) y el número de los puntos de recuperación (pág. 197) disponibles del archivo comprimido. A diferencia del esquema GFS (pág. 192) que posee solo tres niveles de resolución de recuperación (resolución diaria, semanal y mensual), el esquema Torres de Hanói reduce continuamente el intervalo de tiempo entre los puntos de recuperación a medida que incrementa la antigüedad de la copia de seguridad. Esto permite un uso muy eficaz del almacenamiento de las copias de seguridad.

Para obtener más información, consulte "Esquema de copias de seguridad Torres de Hanói" (pág. 29).

U

Universal Restore (Acronis Backup & Recovery 10 Universal Restore)

La tecnología propia de Acronis ayuda a iniciar Windows en hardware diferente o una máquina virtual. Universal Restore maneja diferentes dispositivos que son críticos para el inicio del sistema operativo, como controladores de almacenamiento, placa madre o conjunto de chips.

Universal Restore no está disponible:

- Cuando se inicia el equipo con Acronis Startup Recovery Manager (pág. 185) (con F11) o
- la imagen que se recupera se encuentra en Acronis Secure Zone (pág. 185) o
- Cuando se usa Acronis Active Restore (pág. 185),

debido a que estas funciones fueron especialmente diseñadas para la recuperación instantánea de datos en el mismo equipo.

Universal Restore no está disponible cuando se recupera Linux.

V

Validación

Una operación que verifica la posibilidad de recuperación de datos en una copia de seguridad (pág. 189).

La validación de la copia de seguridad de un archivo imita la recuperación de todos los archivos de la copia de seguridad a un destino Las versiones previas del producto consideraban que la copa de seguridad de un archivo era válida cuando los metadatos del encabezado era consistente. El método actual lleva tiempo pero es mucho más confiable. La validación de la copia de seguridad del volumen calcula la suma de comprobación por cada bloque de datos guardados en la copia de seguridad. Este proceso también usa más recursos.

Si bien la validación satisfactoria significa una gran probabilidad de tener una recuperación exitosa, no verifica todos los factores que influencian el proceso de recuperación. Si realiza una copia de seguridad del sistema operativo, sólo se podrá garantizar una recuperación exitosa con una recuperación de prueba del medio de inicio a un disco duro libre.

Validación del lado del agente

Es la validación (pág. 199) realizada por un agente (pág. 185) de acuerdo al plan de copia de seguridad (pág. 196) que produce el archivo (pág. 186). La validación del lado del agente la realiza las bóvedas sin gestionar (pág. 188).

Validación del lado del nodo de almacenamiento

La validación (pág. 199) realizada por un nodo de almacenamient (pág. 195)o de acuerdo a los planes de copias de seguridad (pág. 196) que guarda los archivos (pág. 186) en una ubicación gestionada (pág. 187). Como es una alternativa a la validación del lado del agente (pág. 199), la validación del lado del nodo de almacenamiento evita la carga innecesaria de la CPU de los servidores de producción.

Volumen dinámico

Es cualquier volumen ubicado en discos dinámicos (pág. 189), o más precisamente, en un grupo de discos (pág. 192). Los volúmenes dinámicos pueden abarcar múltiples discos. Los volúmenes dinámicos se configuran dependiendo del objetivo:

- Aumento del tamaño del volumen (volumen extendido).
- Reducción del tiempo de acceso (un volumen segmentado).
- Logra la tolerancia a fallos al incluir redundancia (volúmenes replicados y RAID-5).

W

WinPE (Entorno de preinstalación de Windows)

Es un sistema Windows reducido basado en alguno de los siguientes núcleos:

- Windows XP Professional con Service Pack 2 (PE 1.5)
- Windows Server 2003 con Service Pack 1 (PE 1.6)
- Windows Vista (PE 2.0)
- Windows Vista SP1 y Windows Server 2008 (PE 2.1).

Win PE suele utilizarse por fabricantes de equipos originales (OEM) y corporaciones para implementar, probar, diagnosticar y reparar sistemas. Se puede iniciar un equipo con WinPE mediante PXE, CD-ROM, unidad de memoria flash USB o disco duro. Complemento de Acronis para WinPE (pág. 188) permite la ejecución del agente Acronis Backup & Recovery 10 (pág. 185) entorno de preinstalación.