IBM Spectrum Protect Plus
Versión 10.1.4

Guía de instalación y del usuario

Nota:

Antes de utilizar esta información y el producto al que da soporte, lea la información del apartado “Avisos” en la página 325.

Esta edición se aplica a la versión 10, release 1, modificación 4 de IBM Spectrum Protect Plus (número de producto 5737-F11) y a todos los releases y modificaciones posteriores, hasta que se indique lo contrario en nuevas ediciones.

Contenido

Acerca de esta publicación

Esta publicación proporciona una visión general, información de planificación e instalación, e instrucciones de usuario para IBM Spectrum Protect Plus.

A quién va dirigida esta publicación

Esta publicación está especialmente indicada para administradores y usuarios que son responsables de implementar una solución de copia de seguridad y recuperación con IBM Spectrum Protect Plus en uno de los entornos soportados.

En esta publicación, se supone que tiene un buen conocimiento de las aplicaciones que dan soporte a IBM Spectrum Protect Plus, tal como se describe en “Requisitos del sistema ” en la página 13.

Publicaciones

La familia de productos de IBM Spectrum Protect incluye IBM Spectrum Protect Plus, IBM Spectrum Protect for Virtual Environments, IBM Spectrum Protect for Databases y otros productos de gestión de almacenamiento de IBM®.

Para ver la documentación de IBM, consulte IBM Knowledge Center.

Novedades de la Versión 10.1.4

IBM Spectrum Protect Plus Versión 10.1.4 introduce nuevas características y actualizaciones.

Para ver una lista de las nuevas características y actualizaciones de este release y los releases anteriores de la versión 10, consulte actualizaciones de IBM Spectrum Protect Plus.

La información nueva y modificada incluida en esta documentación del producto se indica mediante una barra vertical (|) a la izquierda de la modificación.

Cómo implicarse en el desarrollo del producto

Puede influir en el futuro de los productos de IBM Storage compartiendo sus conocimientos con los equipos de diseño y desarrollo. Para implicarse, únase al programa de usuario patrocinador o al programa beta.

Programa de usuario patrocinador

El programa de usuario patrocinador de IBM Storage le permite trabajar directamente con los diseñadores y desarrolladores, a fin de influir en la orientación de los productos que utiliza.

IBM le invita a compartir su experiencia y sus conocimientos. Si se une al programa, podrá ayudarnos a explorar, y posiblemente a implementar, nuevas características de productos importantes para usted y para su empresa.

¿Utiliza un producto de software de IBM Storage, como, por ejemplo, IBM Spectrum Protect Plus?

¿Está preparado para compartir su perspectiva?

Si es así, regístrese en el programa de usuario patrocinador para participar en el proceso de innovación del producto. Además, como usuario patrocinador, podrá obtener una vista previa de los próximos releases de almacenamiento y participar en programas beta para probar las nuevas características del producto.

Si quiere unirse al programa de usuario patrocinador o recibir más información, complete este formulario:

Usuario patrocinador de IBM Storage

Su información se almacenará respetando su privacidad y será utilizada por los equipos de desarrollo y de diseño de IBM solo con fines de desarrollo de productos.

Programa beta

El programa beta de IBM Spectrum Protect Plus le permite ver las características de los próximos productos y le da la oportunidad de influir en los cambios de diseño. Puede probar el nuevo software en el entorno y dar su opinión en el proceso de desarrollo del producto.

El programa beta cuenta con un amplio abanico de participantes, incluidos clientes, Business Partners de IBM y empleados de IBM.

El programa ofrece las ventajas siguientes:

Obtenga acceso al código inicial y evalúe las nuevas características y mejoras del producto
Obtendrá acceso al código beta antes de que el release del producto esté disponible al público general y podrá determinar si las nuevas características y mejoras son adecuadas para su empresa. Una vez descargado el código, podrá ejecutar y validar el nuevo software en su entorno. A continuación, podrá identificar y solucionar los posibles problemas antes de que el código esté disponible, lo que le permitirá ahorrar tiempo y le ayudará a evitar problemas en la posterior fase de producción. Cuando el código esté disponible, podrá instalarlo y aprovechar sus prestaciones.

Interactúe con los equipos de diseño y desarrollo
Los diseñadores, arquitectos, desarrolladores y probadores del producto ayudan a planificar el release beta y dan soporte a sus participantes. Estos expertos pueden ayudarle a solucionar los problemas que puedan surgir.

Conviértase en un cliente de referencia de IBM
Tras una experiencia positiva como usuario beta, IBM le invitará a participar en el programa de referencia. El equipo de marketing de IBM le ayudará a crear un mensaje para notificar a otros posibles probadores beta que ha conseguir adoptar y utilizar el código inicial correctamente.

Información de contacto e inscripción

Para obtener más información sobre el programa beta, póngase en contacto con Mary Anne Filosa utilizando la dirección mailto:mfilosa@us.ibm.com.

Para inscribirse, complete el Formulario de registro en el programa beta de IBM Spectrum Protect Plus.

Capítulo 1. Visión general de IBM Spectrum Protect Plus

IBM Spectrum Protect Plus es una solución de protección y disponibilidad de datos para entornos virtuales y aplicaciones de base de datos que se puede desplegar en minutos y proteger su entorno en una hora.

IBM Spectrum Protect Plus se puede implementar como una solución autónoma o integrarse con un almacenamiento en la nube o un servidor de repositorio como, por ejemplo, un servidor IBM Spectrum Protect para descargar copias para almacenamiento a largo plazo.

Componentes del producto

La solución IBM Spectrum Protect Plus se proporciona como un dispositivo virtual autocontenido que incluye componentes de almacenamiento y movimiento de datos.

Requisitos de dimensionamiento de componentes: Es posible que algunos entornos requieran más instancias de estos componentes para dar soporte a mayores cargas de trabajo. Para obtener instrucciones sobre el dimensionamiento, la creación y la integración de componentes en el entorno de IBM Spectrum Protect Plus, consulte Blueprints de IBM Spectrum Protect Plus.

A continuación se indican los componentes base de IBM Spectrum Protect Plus:

Servidor de IBM Spectrum Protect Plus
Este componente gestiona todo el sistema. El servidor consta de varios catálogos que realizan un seguimiento de varios aspectos del sistema como, por ejemplo, los puntos de restauración, la configuración, los permisos y las personalizaciones. Normalmente, hay un dispositivo de IBM Spectrum Protect Plus en un despliegue, incluso si el despliegue se extiende por varias ubicaciones.

El servidor de IBM Spectrum Protect Plus contiene un servidor vSnap incorporado y el servidor proxy VADP (vStorage API for Data Protection) de VMware. Para entornos de copia de seguridad más pequeños, estos servidores pueden ser suficientes. Sin embargo, para entornos más grandes, es posible que se necesiten más servidores.

El servidor vSnap incorporado se puede utilizar para realizar una copia de seguridad de un número pequeño de máquinas virtuales y restaurarlas, así como evaluar operaciones de IBM Spectrum Protect Plus. A medida que crecen los requisitos de copia de seguridad y restauración de los datos, el almacenamiento de vSnap se puede ampliar añadiendo servidores vSnap externos. Al añadir servidores vSnap externos al entorno, puede reducir la carga en el dispositivo de IBM Spectrum Protect Plus.

Sitio
Este componente es una construcción de política de IBM Spectrum Protect Plus que se utiliza para gestionar la ubicación de datos en el entorno. Un sitio puede ser físico, por ejemplo, un centro de datos; o lógico, por ejemplo, un departamento o una organización. Los componentes de IBM Spectrum Protect Plus se asignan a los sitios para localizar y optimizar las vías de acceso de datos. Un despliegue siempre tiene al menos un sitio por ubicación física. El método preferido es localizar el movimiento de datos a sitios colocando servidores vSnap y proxies VADP juntos en un solo sitio. La colocación de datos de copia de seguridad en un sitio se rige por las políticas de acuerdo de nivel de servicio (SLA).

servidor vSnap
Este componente es una agrupación de almacenamiento de disco que recibe datos de sistemas de producción a los efectos de protección o reutilización de datos. El servidor vSnap consta de uno o más discos y se puede aumentar (añadir discos para aumentar la capacidad) o reducir (introducir varios servidores vSnap para aumentar el rendimiento global). Cada sitio puede incluir uno o más servidores vSnap.

Agrupación de vSnap
Este componente es la organización lógica de los discos en una agrupación de espacio de almacenamiento, que utiliza el componente de servidor vSnap. este componente también se conoce como una agrupación de almacenamiento.

proxy VADP
Este componente es responsable de mover datos de almacenes de datos de vSphere para proporcionar protección a las máquinas virtuales VMware y solo es necesario para la protección de recursos de VMware. Cada sitio puede incluir uno o más proxies VADP.

Interfaces de usuario

IBM Spectrum Protect Plus proporciona las siguientes interfaces para las tareas de configuración, administrativas y de supervisión:

interfaz de usuario de IBM Spectrum Protect Plus
La interfaz de usuario de IBM Spectrum Protect Plus es la interfaz principal para configurar, administrar y supervisar operaciones de protección de datos.

Un componente clave de la interfaz es el panel de instrumentos, que proporciona información de resumen sobre el estado del entorno. Para obtener más información sobre el panel de instrumentos, consulte “Panel de instrumentos del producto” en la página 3.

La barra de menús de la interfaz de usuario contiene los elementos siguientes:

Icono de alertas 	Este icono abre la ventana **Alertas**. Para obtener más información sobre las alertas, consulte “Alertas” en la página 4.
Icono de ayuda 	Este icono abre el sistema de ayuda en línea.
Menú de usuario	Este menú muestra el nombre del usuario que ha iniciado la sesión. El menú proporciona acceso a la información del producto y a la documentación, los registros y la opción de cierre de sesión del usuario.

Interfaz de línea de mandatos vSnap
La interfaz de línea de mandatos vSnap es una interfaz secundaria para la administración de algunas tareas de protección de datos. Ejecute el mandato **vsnap** para acceder a la interfaz de línea de mandatos. El mandato se puede invocar mediante el ID de usuario `serveradmin` o cualquier otro usuario de sistema operativo que tenga privilegios de administración de vSnap.

Consola de administración
La consola de administración se utiliza para instalar parches y actualizaciones de software y para completar otras tareas administrativas como, por ejemplo, gestionar certificados de seguridad, iniciar y detener IBM Spectrum Protect Plus y cambiar el huso horario de la aplicación.

Ejemplo de despliegue

La siguiente figura muestra IBM Spectrum Protect Plus desplegado en dos ubicaciones activas. Cada ubicación tiene un inventario que requiere protección. La ubicación 1 tiene un servidor vCenter y dos centros de datos de vSphere (y un inventario de máquinas virtuales) y la ubicación 2 tiene un único centro de datos (y un inventario más pequeño de máquinas virtuales).

El servidor de IBM Spectrum Protect Plus se despliega en solo uno de los sitios. Los proxies VADP y los servidores vSnap (con sus discos correspondientes) se despliegan en cada sitio para localizar el movimiento de datos en el contexto de los recursos de vSphere protegidos.

La réplica bidireccional está configurada para que tenga lugar entre los servidores vSnap en los dos sitios.

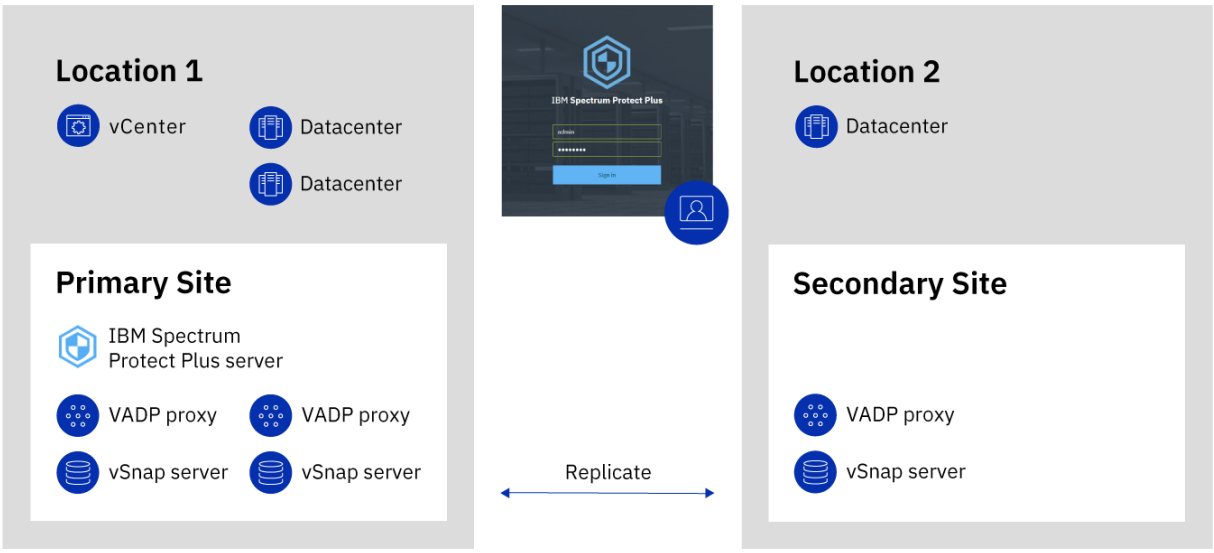


Figura 1. Despliegue de IBM Spectrum Protect Plus en dos ubicaciones geográficas

Panel de instrumentos del producto

El panel de instrumentos de IBM Spectrum Protect Plus resume el estado de su entorno virtual en tres secciones: **Trabajos y operaciones**, **Destinos** y **Cobertura**.

Trabajos y operaciones

En la sección **Trabajos y operaciones** se muestra un resumen de las actividades de trabajo para un periodo de tiempo seleccionado. Seleccione el periodo de tiempo de la lista desplegable. En esta sección se muestra la información siguiente:

Actualmente en ejecución

En la sección **Actualmente en ejecución** se muestra el número total de trabajos que se están ejecutando y el porcentaje de uso de la unidad de procesador central (CPU) en el dispositivo virtual de IBM Spectrum Protect Plus. Este porcentaje se renueva cada 10 segundos.

Para ver información detallada sobre la ejecución de trabajos, pulse **Ver**.

Historial

En la sección **Historial** se muestra el número total de trabajos que se han completado en el periodo de tiempo seleccionado. Este número no incluye los trabajos en ejecución.

En esta sección también se muestra la tasa de correctos de los trabajos durante el período de tiempo seleccionado. La tasa de correctos se calcula utilizando la fórmula siguiente:

100 x trabajos satisfactorios/Trabajos totales = Tasa de correctos

Los trabajos completados se muestran por estado de trabajo:

Satisfactorio
El número de trabajos que se han completado sin avisos o errores críticos.

Ha fallado
El número de trabajos que ha fallado con errores críticos o que no han logrado completarse.

Aviso
El número de trabajos que se han completado parcialmente, se ha omitido o ha resultado en avisos.

Para ver información detallada sobre el historial de trabajos de información, pulse **Ver**.

Destinos

En la sección **Destino** se muestra un resumen de los dispositivos que se utilizan para operaciones de copia de seguridad. En esta sección se muestra la información siguiente:

Resumen de capacidad
En la sección **Resumen de capacidad** se muestra el uso actual y la disponibilidad de los servidores vSnap que están disponibles en IBM Spectrum Protect Plus.

Para ver información sobre servidores vSnap, pulse **Ver**.

Estado del dispositivo
En la sección **Estado del dispositivo**, se muestra el número total de dispositivos que están disponibles para su uso.

El número de dispositivos que están fuera de línea o que no están disponibles se muestra en el campo **Inactivo**.

El número de dispositivos que tienen la capacidad completa se muestra en el campo **Completa**.

Reducción de datos
En la sección **Reducción de datos** se muestran las proporciones de deduplicación de datos y compresión de datos.

La proporción de deduplicación de datos es la cantidad de datos que se protegen con el espacio físico necesario para almacenar los datos después de eliminar los duplicados. Esta proporción representa un ahorro de espacio adicional que se logra sobre la proporción de compresión. Si la deduplicación está inhabilitada, esta proporción es 1.

Cobertura

En la sección **Cobertura** se muestra un resumen de los recursos inventariados por IBM Spectrum Protect Plus y las políticas de acuerdo de nivel de servicio (SLA) que se asignan a los recursos. En esta sección se muestra la información siguiente:

Protección de origen
En la sección **Protección de origen** se muestra el número total de recursos de origen, tales como máquinas virtuales y servidores de aplicaciones, que están inventariados en el catálogo de IBM Spectrum Protect Plus. Se muestra el número de recursos protegidos y no protegidos.

En esta sección también se muestra la proporción de recursos que están protegidos en IBM Spectrum Protect Plus respecto a los recursos totales, expresados como porcentaje.

Políticas
En la sección **Políticas** se muestra el número total de políticas de SLA con trabajos de protección asociados.

Esta sección también muestra las tres políticas de SLA que tienen el número más alto de recursos asignados.

Para ver información detallada sobre todas las políticas de SLA, pulse **Ver**.

Alertas

El menú **Alertas** muestra los avisos actuales y recientes y los errores del entorno de IBM Spectrum Protect Plus. El número de alertas se muestra en un círculo rojo, lo que indica que las alertas están disponibles para visualizarse.

Pulse el menú **Alertas** para ver la lista de alertas. Cada elemento de la lista incluye un icono de estado, un resumen de la alerta, la hora en la que se ha producido el aviso o el error asociado y un enlace para ver los registros asociados.

La lista de alertas puede incluir los tipos de alertas siguientes:

Tipos de alerta

Error de trabajo
Se visualiza cuando un trabajo falla.

Trabajo realizado con éxito parcialmente
Se visualiza cuando un trabajo se ejecuta con éxito parcialmente.

Espacio en disco del sistema bajo
Se visualiza cuando la cantidad de espacio libre de disco es igual o menor al 10%.

Espacio de almacenamiento vSnap bajo
Se visualiza cuando la cantidad de espacio libre de disco es igual o menor al 10%.

Memoria del sistema baja
Se visualiza cuando el uso de memoria excede el 95%.

Uso de CPU del sistema alto
Se visualiza cuando el uso de procesador excede el 95%.

Máquina virtual de hipervisor no encontrada
Se visualiza cuando no se encuentra la máquina virtual.

Excepción de instantánea de almacenamiento de réplicas bloqueada
Se visualiza cuando se bloquea la instantánea de almacenamiento de réplicas. Aumente la retención de las réplicas o la política de frecuencia de réplicas.

Excepción de instantánea de almacenamiento de descarga bloqueada
Se visualiza cuando se bloquea la instantánea de almacenamiento descargada más recientemente. Aumente la retención de las descargas o la política de frecuencia de descargas.

Error de copia de seguridad del registro SQL
Se visualiza cuando falla una copia de seguridad del registro para una base de datos.

Error de copia de seguridad de SMO del registro SQL
Se visualiza cuando se produce un error de copia de seguridad del registro de transacciones de Objeto de gestión de servidor.

Tamaño de registro SQL demasiado grande
Se visualiza cuando el tamaño del registro de transacciones es mayor que el espacio disponible en el disco.

Poco espacio restante en el registro SQL
Se visualiza cuando el directorio intermedio de copia de seguridad del registro de transacciones tiene poco espacio de disco y muestra la cantidad de espacio restante.

Control de acceso basado en roles

El control de acceso basado en roles define los recursos y los permisos que están disponibles para las cuentas de usuario de IBM Spectrum Protect Plus.

El acceso basado en roles proporciona a los usuarios acceso sólo a las características y los recursos que necesitan. Por ejemplo, un rol puede permitir que un usuario ejecute trabajos de copia de seguridad y restauración para recursos del hipervisor, pero permite que el usuario complete tareas administrativas tales como modificar cuentas de usuario.

Para completar las tareas que se describen en esta documentación, el usuario debe pertenecer a un rol que tenga los permisos necesarios. Asegúrese de que la cuenta de usuario pertenece a un rol que tiene los permisos necesarios antes de iniciar la tarea.

Para configurar y gestionar el acceso de usuario, consulte Capítulo 13, “Gestión del acceso de usuarios”, en la página 303.

Replicar datos de almacenamiento de copia de seguridad

Cuando habilite la réplica de datos de copia de seguridad, los datos de un servidor vSnap se replican de forma asíncrona en otro servidor vSnap. Por ejemplo, puede replicar los datos de copia de seguridad de un servidor vSnap en un sitio primario en un servidor vSnap en un sitio secundario.

Habilitación de la réplica de datos de almacenamiento de copia de seguridad.

Habilite la réplica de datos de almacenamiento de copia de seguridad realizando las acciones siguientes:

1. Establezca una asociación de réplica entre servidores vSnap. Las asociaciones de réplica se establecen en el panel Gestionar de un servidor vSnap registrado. En la sección **Configurar socios de almacenamiento**, seleccione otro servidor vSnap registrado como socio de almacenamiento para que sirva como destino de las operaciones de réplica.

   Asegúrese de que la agrupación en el servidor de socio sea suficientemente grande para que contenga datos replicados de la agrupación del servidor primario.
2. Habilite la réplica de datos de almacenamiento de copia de seguridad. La característica de réplica está habilitada utilizando políticas de copia de seguridad, que también se conocen como políticas de acuerdo de nivel de servicio (SLA). Estas políticas definen parámetros que se aplican a trabajos de copia de seguridad, incluida la frecuencia de operaciones de copia de seguridad y la política de retención para las copias de seguridad. Para obtener más información sobre las políticas de SLA, consulte Capítulo 6, “Gestión de políticas de SLA para operaciones de copia de seguridad”, en la página 93.

   Puede definir las opciones de réplica de almacenamiento de copia de seguridad en la sección **Protección operativa** > **Política de réplica** de una política de SLA. Las opciones incluyen la frecuencia de la réplica, el sitio de destino y la retención de la réplica.

Consideraciones sobre la habilitación de la réplica de datos de almacenamiento de copia de seguridad

Revise las consideraciones para habilitar la réplica de los datos de almacenamiento de copia de seguridad:

- Si el entorno incluye una combinación de servidores vSnap cifrados y no cifrados, **Utilice únicamente el almacenamiento de disco cifrado** para replicar datos a servidores vSnap cifrados. Si se selecciona esta opción y no hay disponibles servidores vSnap cifrados, el trabajo asociado fallará.
- Para crear escenarios de réplicas de uno a varios, en los que un solo conjunto de datos de copia de seguridad se duplica en varios servidores vSnap, cree varias políticas de SLA para cada sitio de réplica.

Descargar en almacenamiento de copia de seguridad secundario

El servidor vSnap es la ubicación de copia de seguridad primaria para las instantáneas. Todos los entornos de IBM Spectrum Protect Plus tienen al menos un servidor vSnap. Opcionalmente, puede descargar instantáneas de un servidor vSnap en un almacenamiento de copias de seguridad secundario.

Los siguientes destinos de almacenamiento de copias de seguridad secundarios están disponibles para las operaciones de descarga:

- IBM Cloud Object Storage (incluido IBM Cloud Object Storage Systems)
- Amazon Simple Storage Service (Amazon S3)
- Microsoft Azure
- Servidores de repositorio (para el release actual de IBM Spectrum Protect Plus, el servidor de repositorio debe ser un servidor IBM Spectrum Protect)

Estos destinos dan soporte a los siguientes tipos de almacenamiento. El tipo de almacenamiento que utiliza depende de factores como, por ejemplo, el tiempo de recuperación y los objetivos de seguridad.

Almacenamiento de objetos

El almacenamiento de objetos es un método para almacenar datos donde los datos se almacenan como unidades discretas u objetos en una agrupación de almacenamiento o un repositorio que no utiliza una jerarquía de archivos, sino que almacena todos los objetos en el mismo nivel.

El almacenamiento de objetos es una opción cuando descarga datos en un servidor IBM Spectrum Protect o un sistema de almacenamiento en la nube. Cuando los datos de instantánea se descargan en el almacenamiento de objetos, se crea una copia completa durante la primera operación de descarga. Las copias posteriores son incrementales y capturan los cambios acumulativos desde la última descarga.

La descarga de instantáneas en el almacenamiento de objetos es muy útil si desea tiempos de copia de seguridad y recuperación relativamente rápidos, y no requiere las ventajas de protección, coste y seguridad a más largo plazo que ofrece el almacenamiento de cinta o de archivado de nube.

Almacenamiento de cinta o de archivado de nube

El almacenamiento de cinta significa que los datos se almacenan en un soporte de cinta física o en una biblioteca de cintas virtual. El almacenamiento de cintas es una opción cuando descarga datos en un servidor IBM Spectrum Protect. Al almacenar los volúmenes de cinta en una ubicación segura y externa que no está conectada a Internet, puede ayudar a proteger los datos de amenazas en línea como, por ejemplo, malware y hackers.

El almacenamiento de archivado de nube es un método de almacenamiento a largo plazo que copia datos en uno de los siguientes servicios de almacenamiento: Amazon Glacier, IBM Cloud Object Storage Archive Tier o Microsoft Azure Archive.

Cuando descarga datos en cinta o en un sistema de almacenamiento en la nube, se crea una copia completa de los datos.

La descarga de instantáneas en almacenamiento de cinta o de archivado de nube ofrece ventajas adicionales de coste y seguridad. Sin embargo, como la descarga en estos tipos de almacenamiento requiere una copia de datos completa, el tiempo necesario para copiar los datos aumenta. Asimismo, el tiempo de recuperación puede ser impredecible y los datos pueden tardar más tiempo en procesarse antes de que se puedan utilizar.

Para obtener información sobre cómo se copian los datos de instantánea en el almacenamiento de objetos y el almacenamiento de archivado para cada sistema de almacenamiento en la nube, consulte "Requisitos de nube" en la página 23.

Añadir almacenamiento de copia de seguridad secundario y crear políticas de copia de seguridad

Para descargar datos en el almacenamiento secundario, son necesarias las acciones siguientes:

Acción	Procedimiento
Para descargar datos en un servidor de repositorio • Configure IBM Spectrum Protect Plus como un cliente objeto en el entorno del servidor IBM Spectrum Protect. • Añada el almacenamiento a IBM Spectrum Protect Plus.	Consulte "Configuración de un servidor IBM Spectrum Protect como destino de descarga" en la página 268 y "Adición de un servidor de repositorio como proveedor de almacenamiento de copias de seguridad" en la página 272.

Acción	Procedimiento
Para descargar datos en el almacenamiento en la nube, añada el almacenamiento a IBM Spectrum Protect Plus.	Siga las instrucciones para el tipo de almacenamiento seleccionado: • “Adición del almacenamiento en la nube Amazon S3 como proveedor de almacenamiento de copias de seguridad” en la página 263 • “Adición de IBM Cloud Object Storage como proveedor de almacenamiento de copias de seguridad” en la página 264 • “Adición del almacenamiento en la nube de Microsoft Azure como proveedor de almacenamiento de copias de seguridad” en la página 266 • “Adición de un servidor de repositorio como proveedor de almacenamiento de copias de seguridad” en la página 272
Crear una política de copia de seguridad que incluya el almacenamiento.	Consulte “Crear políticas de copia de seguridad” en la página 77.

Despliegues de ejemplo

La siguiente figura muestra IBM Spectrum Protect Plus desplegado en dos ubicaciones activas. Cada ubicación tiene un inventario que requiere protección. La ubicación 1 tiene un servidor vCenter y dos centros de datos de vSphere (y un inventario de máquinas virtuales) y la ubicación 2 tiene un único centro de datos (y un inventario más pequeño de máquinas virtuales).

El servidor de IBM Spectrum Protect Plus se despliega en solo uno de los sitios. Los proxies VADP y los servidores vSnap (con sus discos correspondientes) se despliegan en cada sitio para localizar el movimiento de datos en el contexto de los recursos de vSphere protegidos.

La réplica bidireccional está configurada para que tenga lugar entre los servidores vSnap en los dos sitios.

Las instantáneas se descargan del servidor vSnap en el sitio secundario en el almacenamiento en la nube para la protección de datos a largo plazo.

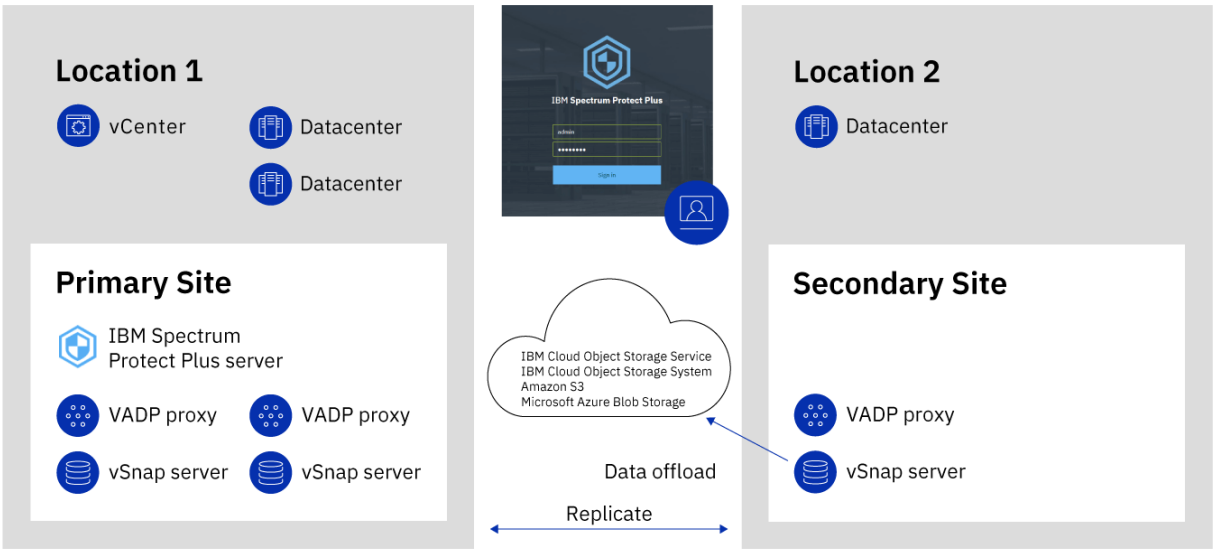


Figura 2. Despliegue de IBM Spectrum Protect Plus en dos ubicaciones geográficas con descarga en almacenamiento en la nube

La siguiente figura muestra el mismo despliegue que la anterior.

No obstante, en este despliegue, las instantáneas se descargan del servidor vSnap en el sitio secundario en IBM Spectrum Protect para protección de datos a largo plazo.

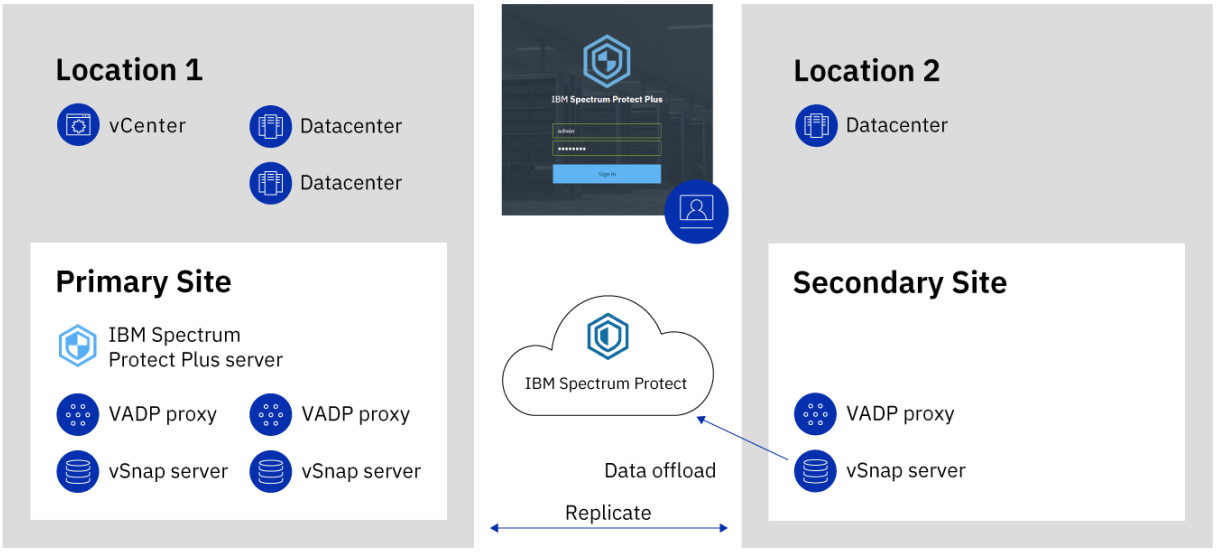


Figura 3. Despliegue de IBM Spectrum Protect Plus en dos ubicaciones geográficas con descarga en IBM Spectrum Protect

IBM Spectrum Protect Plus on IBM Cloud

IBM Spectrum Protect Plus está disponible como un servicio de Soluciones de IBM Cloud for VMware, IBM Spectrum Protect Plus on IBM Cloud.

Soluciones de IBM Cloud for VMware le permite integrar o migrar las cargas de trabajo de VMware locales a IBM Cloud utilizando la infraestructura de IBM Cloud escalable y la tecnología de virtualización híbrida de VMware.

Soluciones de IBM Cloud for VMware ofrece las principales ventajas siguientes:

Alcance global
Expanda su ocupación en la nube híbrida hasta un máximo de 30 centros de datos de IBM Cloud de nivel empresarial en todo el mundo.

Integración simplificada
Utilice el proceso simplificado para integrar la nube híbrida con la infraestructura de IBM Cloud.

Despliegue y configuración automatizados
Despliegue un entorno de VMware de clase empresarial con servidores de nivel básico y servidores virtuales bajo demanda de IBM Cloud utilizando el despliegue y la configuración automatizados del entorno de VMware.

Simplificación
Utilice una plataforma en la nube de VMware sin identificar, adquirir, desplegar y gestionar la infraestructura informática física, de almacenamiento y de red, así como las licencias de software subyacentes.

Flexibilidad en cuanto a ampliación y reducción
Expande y reduzca las cargas de trabajo de VMware de acuerdo con sus requisitos empresariales.

Consola única de gestión
Utilice una única consola para desplegar, acceder y gestionar los entornos de VMware en IBM Cloud.

Características disponibles en IBM Spectrum Protect Plus on IBM Cloud

IBM Spectrum Protect Plus da soporte a entornos de VMware y de Microsoft Hyper-V.

Sin embargo, IBM Spectrum Protect Plus on IBM Cloud solo da soporte a entornos de VMware.

En esta documentación se incluyen temas sobre las características específicas de Hyper-V. Estas características no están disponibles si utiliza IBM Spectrum Protect Plus on IBM Cloud.

Es posible que la versión actual de IBM Spectrum Protect Plus y de IBM Spectrum Protect Plus on IBM Cloud no sea la misma. Para encontrar la documentación de la versión de IBM Spectrum Protect Plus on IBM Cloud que utiliza, vaya a documentación del producto en línea y seleccione la versión del producto.

Información adicional

Para obtener información acerca de cómo solicitar, instalar y configurar IBM Spectrum Protect Plus on IBM Cloud, consulte la documentación siguiente. Es preciso un IBMid para acceder a la documentación.

- Iniciación a las soluciones de IBM Cloud for VMware
- Componentes y consideraciones para IBM Spectrum Protect Plus en IBM Cloud
- Gestión de IBM Spectrum Protect Plus en IBM Cloud

IBM Spectrum Protect Plus en la plataforma de nube de AWS

IBM Spectrum Protect Plus en la plataforma de nube de Amazon Web Services (AWS) es una solución para los usuarios que ejecutan IBM Spectrum Protect Plus de manera local, pero que desean proteger las bases de datos que se ejecutan en la nube de AWS.

IBM Spectrum Protect Plus on AWS es una solución híbrida donde el servidor de IBM Spectrum Protect Plus es local y el servidor vSnap está en AWS.

La política, la administración del sistema, el control de accesos y otras características de IBM Spectrum Protect Plus se gestionan y mantienen en el servidor de IBM Spectrum Protect Plus local. Los datos de las bases de datos que están en AWS se almacenan en el servidor vSnap que también está en AWS.

Despliegue de IBM Spectrum Protect Plus en AWS

Página IBM Spectrum Protect Plus en AWS Marketplace proporciona las plantillas de AWS CloudFormation necesarias para desplegar el servidor vSnap en AWS, así como la información de precios, uso y soporte. Siga las instrucciones de esta página y la Guía de despliegue de IBM Spectrum Protect Plus en AWS Cloud para configurar los entornos local y AWS.

El despliegue de IBM Spectrum Protect Plus on AWS incluye IBM Spectrum Protect Plus versión 10.1.3. Si quiere utilizar la versión actual de IBM Spectrum Protect Plus, siga las instrucciones en Capítulo 5, “Actualización de componentes de IBM Spectrum Protect Plus”, en la página 87 para completar la actualización.

Capítulo 2. Instalación de IBM Spectrum Protect Plus

Antes de instalar IBM Spectrum Protect Plus, revise los requisitos del sistema y los procedimientos de instalación.

Hoja de ruta de despliegue del producto

Siga la hoja de ruta para instalar, configurar y empezar a utilizar IBM Spectrum Protect Plus.

Acción	Procedimiento
Asegúrese de que el sistema cliente cumpla los requisitos de hardware y software mínimos.	Consulte “Requisitos del sistema ” en la página 13.
Determine cómo dimensionar, compilar y colocar los componentes en el entorno de IBM Spectrum Protect Plus.	Consulte el Blueprints de IBM Spectrum Protect Plus.
Instale IBM Spectrum Protect Plus.	Consulte Capítulo 2, “Instalación de IBM Spectrum Protect Plus”, en la página 13.
Si son necesarios servidores vSnap adicionales para dar soporte al entorno, instálelos y configúrelos.	Consulte Capítulo 3, “Instalación y configuración de servidores vSnap”, en la página 57.
Si se necesitan proxies VADP (vStorage API for Data Protection) de VMware adicionales para dar soporte al entorno, cree y configure los proxies.	Consulte “Gestión de proxies de copias de seguridad VADP” en la página 112.
Complete los pasos básicos para configurar y empezar a utilizar IBM Spectrum Protect Plus.	Consulte Capítulo 4, “Empezar con un inicio rápido”, en la página 73.

Requisitos del sistema

Antes de instalar IBM Spectrum Protect Plus, revise los requisitos de hardware y software para el producto y los demás componentes que tiene previsto instalar en el entorno de almacenamiento.

Para ayudarle a garantizar que las operaciones de copia de seguridad y restauración se pueden ejecutar correctamente, el sistema debe cumplir los requisitos de hardware y software. Utilice los requisitos siguientes como punto de partida. Para los requisitos más actuales, que pueden incluir actualizaciones, consulte nota técnica 2013790.

Para determinar cómo dimensionar, compilar y colocar los componentes que aparecen listados en las especificaciones del entorno de IBM Spectrum Protect Plus, consulte Blueprints de IBM Spectrum Protect Plus.

Requisitos de los componentes

Asegúrese de que dispone de la configuración del sistema necesaria y de un navegador soportado para desplegar y ejecutar IBM Spectrum Protect Plus.

Para ayudarle a garantizar que las operaciones de copia de seguridad y restauración se pueden ejecutar correctamente, el sistema debe cumplir los requisitos de hardware y software. Utilice los requisitos siguientes como punto de partida. Para los requisitos más actuales, que pueden incluir actualizaciones, consulte nota técnica 2013790.

El soporte de IBM Spectrum Protect Plus para plataformas de terceros, aplicaciones, servicios y hardware es paralelo al de los proveedores terceros. Cuando un producto o versión de proveedor de terceros

especifica soporte ampliado, el soporte de autoservicio o la finalización del ciclo de vida, IBM Spectrum Protect Plus lo soporta en el mismo nivel.

Instalación de la máquina virtual

IBM Spectrum Protect Plus está instalado como un dispositivo virtual. Antes de desplegar IBM Spectrum Protect Plus en el host, asegúrese de que se cumplan los requisitos siguientes:

- vSphere 5.5, 6.0, 6.5 o 6.7
- Microsoft Hyper-V Server 2016 o Hyper-V 2019.

Para el despliegue inicial, configure el dispositivo virtual para que cumpla los requisitos mínimos siguientes:

- Máquina de 8 núcleos de 64 bits
- 48 GB de memoria
- Almacenamiento de disco de 536 GB para la máquina virtual

Utilice un servidor NTP (Network Time Protocol) para sincronizar los husos horarios en los recursos de IBM Spectrum Protect Plus que hay en el entorno como, por ejemplo, el dispositivo virtual de IBM Spectrum Protect Plus, las matrices de almacenamiento, los hipervisores y los servidores de aplicaciones. Si los relojes de los distintos sistemas no están sincronizados, es posible que surjan errores durante el registro de aplicaciones, la catalogación de metadatos, el inventario, la copia de seguridad, la restauración o los trabajos de restauración de archivos. Para obtener más información sobre la identificación y la resolución de la desviación del temporizador, consulte el siguiente artículo de la base de conocimientos de VMware: Time in virtual machine drifts due to hardware timer drift.

Soporte de navegadores

Ejecute IBM Spectrum Protect Plus desde un sistema que tenga acceso al dispositivo virtual instalado. IBM Spectrum Protect Plus se ha probado en los navegadores web siguientes. Tenga en cuenta que las versiones posteriores del navegador también pueden estar soportadas.

- Firefox 55.0.3
- Google Chrome 60.0.3112 y posteriores
- Microsoft Edge 40.15063/Microsoft EdgeHTML 15.15063 y posteriores

Si la resolución de la pantalla es inferior a 1024 x 768 píxeles, es posible que algunos elementos no quepan en la ventana. Las ventanas emergentes deben estar habilitadas en el navegador para acceder al sistema de ayuda y a algunas operaciones de IBM Spectrum Protect Plus.

Requisitos de IBM Spectrum Protect

Si tiene previsto utilizar IBM Spectrum Protect como servidor de repositorio para las operaciones de descarga en la nube, asegúrese de utilizar IBM Spectrum Protect V8.1.8.

Puertos de IBM Spectrum Protect Plus

IBM Spectrum Protect Plus utiliza los puertos siguientes y los servicios asociados. Los puertos que se indican mediante "Aceptar" en la columna Regla de cortafuegos utilizan conexiones seguras (HTTPS o SSL).

Tabla 1. Conexiones de cortafuegos entrantes (dispositivo de IBM Spectrum Protect Plus)

Puerto	Protocolo	Cortafuegos	Servicio	Descripción
22	TCP	Accept	OpenSSH 5.3 (protocolo 2.0)	Se utiliza para la resolución de problemas de IBM Spectrum Protect Plus
443	TCP	Accept	Un microservicio que ejecuta un proxy inverso	Punto de entrada principal para las conexiones de cliente (SSL)
5671	TCP, AMQP	Accept	RabbitMQ	La infraestructura de mensajes utilizada para gestionar los mensajes producidos y consumidos por el proxy VADP y los Workers de gestión de trabajos de VMware. También facilita la gestión del registro de trabajos.
8090	TCP	Accept	Infraestructura de consola de administración (ACF)	Infraestructura ampliable para las funciones de administración del sistema. Da soporte a los plug-ins que ejecutan operaciones como, por ejemplo, las actualizaciones del sistema y las operaciones de copia de seguridad o restauración de catálogos
8761	TCP	Accept	Servidor de descubrimiento	Descubre automáticamente proxies VADP y se utiliza en operaciones de copia de seguridad de la máquina virtual de IBM Spectrum Protect Plus

Tabla 2. Conexiones de cortafuegos entrantes (servidor vSnap incorporado)

Puerto	Protocolo	Cortafuegos	Servicio	Descripción
111	TCP	Accept	Enlace de puerto RPC	Permite que los clientes descubran los puertos que los clientes de Open Network Computing (ONC) requieren para comunicarse con servidores ONC (internos)
2049	TCP	Accept	NFS	Se utiliza para la transferencia de datos NFS a y desde vSnap (internos)
3260	TCP	Accept	iSCSI	Se utiliza para la transferencia de datos iSCSI a y desde vSnap (internos)
20048	TCP	Accept	NFS	Se utiliza para la transferencia de datos NFS a y desde vSnap (internos)

Tabla 3. Conexiones de cortafuegos salientes (dispositivo de IBM Spectrum Protect Plus)

Puerto	Protocolo	Servicio	Descripción
22	TCP	OpenSSH 5.3 (protocolo 2.0)	Se utiliza para las comunicaciones SSH en servidores remotos que ejecutan componentes de aplicaciones invitados.
25	TCP	SMTP	Servicio de correo electrónico.
389	TCP	LDAP	Servicios de Active Directory.
443	TCP	Host de VMware ESXi	Puerto de host ESXi para operaciones de gestión.
443	TCP	VMware vCenter	Conexiones de cliente a vCenter.
636	TCP	LDAP	Servicios de Active Directory (SSL).

Tabla 3. Conexiones de cortafuegos salientes (dispositivo de IBM Spectrum Protect Plus) (continuación)			
Puerto	**Protocolo**	**Servicio**	**Descripción**
902	TCP	Servicio VMware NFC	La copia de archivo de red (NFC) proporciona un servicio FTP con reconocimiento de tipo de archivo para componentes de vSphere. De forma predeterminada, ESXi utiliza NFC para operaciones tales como copia y traslado de datos entre almacenes de datos.
5985	TCP	Windows Remote Management (WinRM)	Conexiones de cliente Hyper-V y aplicaciones invitado.
8098	TCP	proxy VADP	Proxy de protección de datos de máquina virtual.
8900	TCP	vSnap	Versión de OVA/Installer de la infraestructura de almacenamiento inteligente utilizada como destino para las operaciones de protección de datos.

Requisitos del servidor vSnap

Un servidor vSnap es el destino de copia de seguridad primario de IBM Spectrum Protect Plus. En un entorno de VMware o Hyper-V, un servidor vSnap con el nombre `localhost` se instala automáticamente en el momento en que se despliega inicialmente el dispositivo virtual de IBM Spectrum Protect Plus. En entornos de empresa de copia de seguridad más grandes, es posible que se necesiten más servidores vSnap.

Asigne memoria basándose en la capacidad de copia de seguridad para una deduplicación más eficiente. Para obtener más información y orientación de dimensionamiento, consulte Blueprints de IBM Spectrum Protect Plus.

Para el despliegue inicial, asegúrese de que la máquina virtual o la máquina física de Linux cumple los requisitos mínimos siguientes:

- Procesador de 8 núcleos de 64 bits
- 32 GB de memoria
- 16 GB de espacio libre en el sistema de archivos raíz
- 128 GB de espacio libre en un sistema de archivos independiente montado en la ubicación siguiente: `/opt/vsnap-data`

El servicio de gestión de red de Linux debe estar instalado y en ejecución.

Opcionalmente, una unidad de estado sólido (SSD) mejora el rendimiento de la copia de seguridad y la restauración.

- Para mejorar el rendimiento de la copia de seguridad, configure la agrupación para que utilice uno o más dispositivos de registro con copia de seguridad de una SSD. Especifique al menos dos dispositivos de registro para crear un registro duplicado para mejorar la redundancia.
- Para mejorar el rendimiento de la restauración, configure la agrupación para que utilice un dispositivo de memoria caché con copia de seguridad de una SSD.

Requisitos de instalación de la máquina virtual de servidor vSnap

Antes de desplegar el servidor vSnap en el host, asegúrese de que se cumplan los requisitos siguientes:

- vSphere 5.5, 6.0, 6.5. o 6.7
- Microsoft Hyper-V 2016 o Microsoft Hyper-V 2019.

Requisitos de instalación física del servidor vSnap

A partir de V10.1.3, IBM Spectrum Protect Plus proporciona la proporciona una funcionalidad que requiere los niveles de kernel soportados en RHEL 7.5 y CentOS 7.5. Si debe utilizar sistemas operativos anteriores a RHEL 7.5 y CentOS 7.5, utilice IBM Spectrum Protect Plus V10.1.2 para las instalaciones físicas de vSnap V10.1.2.

Los siguientes sistemas operativos Linux están soportados para las instalaciones de servidor vSnap físico de IBM Spectrum Protect Plus V10.1.4 o posteriores:

- CentOS 7.1804 (7.5) (x86_64)
- CentOS 7.1810 (7.6) (x86_64)
- RedHat Enterprise Linux 7.5 (x86_64)
- Red Hat Enterprise Linux 7.6 (x86_64)

Si utiliza los siguientes sistemas operativos, utilice IBM Spectrum Protect Plus V10.1.2 para instalaciones de servidor vSnap físico V10.1.2:

- CentOS Linux7.3.1611 (x86_64)
- CentOS Linux7.4.1708 (x86_64)
- Red Hat Enterprise Linux 7.3 (x86_64)
- Red Hat Enterprise Linux 7.4 (x86_64)

Puertos del servidor vSnap

Los servidores vSnap utilizan los puertos siguientes. Los puertos que se indican con Aceptar en la columna Regla de cortafuegos utilizan conexiones seguras (HTTPS/SSL).

Tabla 4. Conexiones de cortafuegos vSnap entrantes

Puerto	Protocolo	Cortafuegos	Servicio	Descripción
22	TCP	Accept	SSH	Se utiliza para la resolución de problemas de servidores vSnap

Tabla 4. Conexiones de cortafuegos vSnap entrantes (continuación)

Puerto	Protocolo	Cortafuegos	Servicio	Descripción
111	TCP	Accept	Enlace de puerto RPC	Permite que los clientes descubran los puertos que los clientes de Open Network Connectivity (ONC) requieren para comunicarse con servidores ONC (internos)
137	UDP	Accept	SMB/CIFS	Se utiliza para la transferencia de datos SMB o CIFS hacia y desde los servidores vSnap (internos)
138	UDP	Accept	SMB/CIFS	Se utiliza para la transferencia de datos SMB o CIFS hacia y desde los servidores vSnap (internos)
139	TCP	Accept	SMB/CIFS	Se utiliza para la transferencia de datos SMB o CIFS hacia y desde los servidores vSnap (internos)
445	TCP	Accept	SMB/CIFS	Se utiliza para la transferencia de datos SMB o CIFS hacia y desde los servidores vSnap (internos)
2049	TCP	Accept	NFS	Se utiliza para la transferencia de datos NFS hacia y desde los servidores vSnap (internos)
3260	TCP	Accept	iSCSI	Se utiliza para la transferencia de datos iSCSI hacia y desde los servidores vSnap (internos)
8900	TCP	Accept	HTTPS	API REST del servidor vSnap

Tabla 4. Conexiones de cortafuegos vSnap entrantes (continuación)				
Puerto	**Protocolo**	**Cortafuegos**	**Servicio**	**Descripción**
20048	TCP	Accept	NFS	Se utiliza para la transferencia de datos NFS hacia y desde los servidores vSnap (internos)

Requisitos del proxy VADP

En IBM Spectrum Protect Plus, la ejecución de trabajos de copia de seguridad de máquina virtual a través de VADP puede estar gravando los recursos del sistema. Al crear proxies de trabajo de copia de seguridad VADP, puede habilitar el uso compartido de carga y el equilibrio de carga para los trabajos de copia de seguridad de IBM Spectrum Protect Plus. Si existen proxies, toda la carga de proceso se desplaza desde el dispositivo IBM Spectrum Protect Plus a los proxies.

Esta dispositivo solo se ha probado para entornos de SUSE Linux Enterprise Server y Red Hat. La característica solo está soportada en las configuraciones de cuatro núcleos de 64 bits o superiores con un kernel mínimo de 2.6.32.

Los proxies VADP dan soporte a los modos de transporte de VMware siguientes: File, SAN, HotAdd, NBDSSL y NBD. Para obtener más información sobre las modalidades de transporte de VMware, consulte Métodos de transporte de disco virtual.

Esta característica solo está soportada en configuraciones de cuatro núcleos de 64 bits o superiores en los entornos de Linux siguientes:

- Niveles de mantenimiento y modificación de CentOS Linux 6.5 y posterior (empezando por 10.1.1 parche 1)
- Niveles de mantenimiento y modificación de CentOS Linux 7.0 y posterior (empezando por 10.1.1 parche 1)
- Niveles de mantenimiento y modificación de Red Hat Enterprise Linux 6, Fixpack 4 y posterior
- Niveles de mantenimiento y modificación de Red Hat Enterprise Linux 7 y posterior
- Niveles de mantenimiento y modificación de SUSE Linux Enterprise Server 12 y posterior

Para obtener más información y orientación de dimensionamiento, consulte Blueprints de IBM Spectrum Protect Plus.

Para el despliegue inicial de un servidor proxy VADP, asegúrese de que la máquina Linux cumple los requisitos mínimos siguientes:

- Procesador de 4 núcleos de 64 bits
- Se requieren 8 GB de RAM, se prefieren 16 GB
- 60 GB de espacio libre en disco

El aumento de las CPU utilizadas y la simultaneidad en el servidor proxy VADP requiere que se incremente la memoria asignada en el servidor proxy según corresponda.

El proxy debe ser capaz de montar sistemas de archivos NFS, que en muchos casos requieren que se instale un paquete de cliente NFS. Los detalles del paquete exacto varían en función de la distribución.

Cada proxy debe tener un nombre de dominio completo y debe ser capaz de resolver y llegar al vCenter. Los servidores vSnap deben ser accesibles desde el proxy. El puerto 8098 en el servidor proxy VADP debe estar abierto cuando el cortafuegos del servidor proxy está habilitado.

Puertos de proxy VADP

Los proxies VADP utilizan los puertos siguientes. Los puertos que se indican con "Aceptar" en la columna Regla de cortafuegos utilizan conexiones seguras (HTTPS o SSL).

Tabla 5. Conexiones de cortafuegos proxy VADP entrantes

Puerto	Protocolo	Cortafuegos	Servicio	Descripción
22	TCP	Accept	SSH	El puerto 22 se utiliza para enviar el proxy VADP al nodo de host.
8098	TCP	Accept	VADP	El puerto predeterminado para comunicaciones de API REST basadas en TLS entre el servidor de IBM Spectrum Protect Plus y el proxy VADP.

Tabla 6. Conexiones de cortafuegos proxy VADP salientes

Puerto	Protocolo	Servicio	Descripción
111	TCP	Enlace de puerto RPC vSnap	Permite que los clientes descubran los puertos que los clientes de ONC requieren comunicarse con los servidores ONC internos.
443	TCP	Host/vCenter de VMware ESXi	Conexiones de cliente a vCenter.
902	TCP	Host de VMware ESXi	La copia de archivo de red (NFC) proporciona un servicio FTP con reconocimiento de tipo de archivo para componentes de vSphere. ESXi utiliza NFC para operaciones tales como copia y traslado de datos entre almacenes de datos de forma predeterminada.
2049	TCP	NFS vSnap	Se utiliza para compartir archivos NFS utilizando el servidor vSnap.

Tabla 6. Conexiones de cortafuegos proxy VADP salientes (continuación)

Puerto	Protocolo	Servicio	Descripción
5671	TCP	RabbitMQ	La infraestructura de mensajes utilizada para gestionar los mensajes producidos y consumidos por el proxy VADP y los Workers de gestión de trabajos de VMware. También facilita el registro de trabajo.
8761	TCP	Servidor de descubrimiento	Descubre automáticamente proxies VADP y se utiliza en operaciones de copia de seguridad de la máquina virtual de IBM Spectrum Protect Plus.
20048	TCP	Montaje de vSnap	Monta sistemas de archivos vSnap en clientes tales como proxy VADP, servidores de aplicaciones y almacenes de datos de virtualización.

Consejo: Los proxies VADP se pueden enviar e instalar en servidores basados en Linux sobre el puerto SSH 22.

Si el script de mandato de cortafuegos no está disponible en el sistema, edite el cortafuegos manualmente para añadir los puertos necesarios y reinicie el cortafuegos. Para obtener más información sobre la edición de reglas de cortafuegos, consulte "Edición de puertos de cortafuegos" en la página 54.

Proxy VADP en requisitos del servidor vSnap

Los proxies VADP se pueden instalar en servidores vSnap en el entorno de IBM Spectrum Protect Plus. Una combinación de proxy VADP y servidor vSnap debe cumplir los requisitos mínimos de ambos dispositivos. Consulte los requisitos del sistema de ambos dispositivos y añada los requisitos de núcleo y RAM para identificar los requisitos mínimos de la combinación de proxy y servidor vSnap VADP.

Asegúrese de que la combinación de proxy y servidor vSnap VADP cumple los siguientes requisitos mínimos recomendados, que es la suma de los requisitos para cada dispositivo.

Proxy VADP instalado en un servidor vSnap virtual:

- Procesador de 8 núcleos de 64 bits
- 48 GB RAM

Todos los puertos de proxy y servidor vSnap VADP necesarios deben estar abiertos en la combinación de servidor proxy y vSnap VADP. Para obtener más información, revise las secciones de proxy VADP y puertos vSnap de los requisitos del sistema.

Requisitos de nube

Para descargar los datos en el almacenamiento en la nube, asegúrese de que los entornos de IBM Spectrum Protect Plus y nube cumplan los requisitos siguientes.

Área de memoria caché de disco

Para todas las funciones relacionadas con la descarga o restauración desde la nube, el servidor vSnap requiere un área de memoria caché de disco en el servidor vSnap.

- Durante las operaciones de descarga, esta memoria caché se utiliza como un área intermedia temporal para los objetos que están pendientes de carga en el punto final de la nube.
- Durante las operaciones de restauración, el área de memoria caché de disco se utiliza para almacenar en memoria caché los objetos descargados, así como para almacenar cualquier dato temporal que se pueda escribir en el volumen de restauración.

Para obtener instrucciones sobre el dimensionamiento y la instalación de la memoria caché, consulte Configuración de descarga de nube o Blueprints de IBM Spectrum Protect Plus.

Requisitos de los certificados

- **Certificados autofirmados:** si el punto final de la nube o el servidor de repositorio utiliza un certificado autofirmado, el certificado se debe especificar (en formato de correo PEM (Privacy Enhanced Mail)) al registrar el servidor de nube o de repositorio en la interfaz de usuario de IBM Spectrum Protect Plus.
- **Certificados firmados por la entidad emisora de certificados privada:** si el punto final de la nube o el servidor de repositorio utiliza un certificado firmado por una entidad emisora de certificados (CA) privada, se debe especificar el certificado de punto final (en formato PEM) al registrar el servidor de nube o de repositorio en la interfaz de usuario de IBM Spectrum Protect Plus. Además, el certificado raíz/intermedio de la entidad emisora de certificados privada debe añadirse al almacén de certificados del sistema en cada servidor de vSnap utilizando el procedimiento siguiente:
  1. Inicie la sesión en la consola del servidor vSnap como usuario `serveradmin` y cargue los certificados de la entidad emisora de certificados privada (en formato PEM) en una ubicación temporal.
  2. Copie cada archivo de certificado en el directorio del almacén de certificados del sistema (`/etc/pki/ca trust/source/anchors/`) ejecutando el mandato siguiente:

     ```
     $ sudo cp /tmp/private-ca-cert.pem /etc/pki/ca-trust/source/anchors/
     ```

  3. Para incorporar el certificado personalizado que se acaba de añadir y actualizar el paquete de certificados del sistema, ejecute el mandato siguiente:

     ```
     $ sudo update-ca-trust
     ```

- **Certificados firmados por la autoridad de certificados públicos:** Si el punto final de la nube utiliza un certificado firmado por una entidad emisora de certificados pública, no se necesita ninguna acción especial. El servidor vSnap valida el certificado utilizando el almacén de certificados del sistema predeterminado.

Requisitos de red

Los puertos siguientes se utilizan para la comunicación entre servidores vSnap y puntos finales de la nube o del servidor de repositorio.

Tabla 7. Conexiones de cortafuegos del servidor vSnap salientes			
Puerto	**Protocolo**	**Servicio**	**Descripción**
443	TCP	HTTPS	Permite que vSnap se comunique con los puntos finales de Amazon S3, Azure o IBM Cloud Object Storage.
9000	TCP	HTTPS	Permite que vSnap se comunique con los puntos finales de IBM Spectrum Protect (servidor de repositorio).

Los cortafuegos o proxies de red que ejecutan la intercepción SSL o la inspección profunda de paquetes para tráfico entre servidores vSnap y puntos final de la nube pueden interferir con la validación de certificados SSL en los servidores vSnap. Esta interferencia puede provocar errores en el trabajo de descarga de la nube. Para impedir esta interferencia, los servidores vSnap deben estar exentos de la intercepción SSL y de la inspección en la configuración del cortafuegos o de proxy.

Requisitos del proveedor de la nube

La gestión de ciclo de vida nativa no está soportada. IBM Spectrum Protect Plus gestiona el ciclo de vida de los objetos subidos automáticamente utilizando un enfoque incremental para siempre en el que los objetos más antiguos todavía pueden ser utilizados por instantáneas más recientes. La caducidad automática o manual de los objetos fuera de IBM Spectrum Protect Plus dará lugar a la corrupción de datos.

Si el proveedor de nube utiliza un certificado SSL autofirmado o firmado por una entidad emisora de certificados privada, consulte Requisitos sobre certificados.

Requisitos de nube de Amazon S3

- **Descarga:** cuando se registra el proveedor de nube en IBM Spectrum Protect Plus, se debe especificar un grupo existente en uno de los niveles de almacenamiento soportados: S3 Standard, S3 Intelligent-Tiering, S3 Standard-Infrequent Access o S3 One Zone-Infrequent Access.
- **Archivado:** cuando se registra el proveedor de nube en IBM Spectrum Protect Plus, se debe especificar un grupo existente en uno de los niveles de almacenamiento soportados: S3 Standard, S3 Intelligent-Tiering, S3 Standard-Infrequent Access o S3 One Zone-Infrequent Access. IBM Spectrum Protect Plus cargará directamente los archivos de datos en el nivel Glacier. Algunos archivos de metadatos pequeños se almacenarán en el nivel predeterminado para el grupo. También se coloca una copia de estos archivos de metadatos en el nivel Glacier para fines de recuperación tras desastre.

Requisitos de IBM Cloud Object Storage

- **Descarga:** cuando se registra el proveedor de nube en IBM Spectrum Protect Plus, se debe especificar un grupo existente. Si el grupo especificado tiene una política WORM que bloquea los objetos durante un determinado periodo de tiempo, IBM Spectrum Protect Plus detecta automáticamente la configuración y suprime las instantáneas después de que la política WORM elimina el bloqueo.
- **Archivado:** cuando se registra el proveedor de nube en IBM Spectrum Protect Plus, se debe especificar un grupo existente. Si el grupo especificado tiene una política WORM que bloquea los objetos durante un determinado periodo de tiempo, IBM Spectrum Protect Plus detecta automáticamente la configuración y suprime las instantáneas después de que la política WORM elimina el bloqueo. IBM Spectrum Protect Plus crea una única regla de gestión del ciclo de vida en el grupo para migrar los archivos de datos al nivel de archivado.

Requisitos de Microsoft Azure

- **Descarga:** cuando el proveedor de nube se registra en IBM Spectrum Protect Plus, debe especificarse un contenedor existente en una cuenta de almacenamiento dinámica o en caliente.
- **Archivado:** cuando el proveedor de nube se registra en IBM Spectrum Protect Plus, debe especificarse un contenedor existente en una cuenta de almacenamiento dinámica o en caliente. IBM Spectrum Protect Plus mueve los archivos entre niveles bajo demanda. Los archivos de datos se trasladarán inmediatamente al nivel de archivado y se devolverán temporalmente al nivel dinámico solo durante una operación de restauración. Algunos archivos de metadatos pequeños se almacenarán en el nivel predeterminado para el contenedor. También se coloca una copia de estos archivos de metadatos en el nivel de archivado para fines de recuperación tras desastre.

Requisitos de IBM Spectrum Protect (servidor de repositorio)

- **Descarga:** cuando el proveedor de nube se registra en IBM Spectrum Protect Plus, no puede utilizar un grupo existente. IBM Spectrum Protect Plus crea un grupo de nombre exclusivo para su propio uso.
- **Archivado:** cuando el proveedor de nube se registra en IBM Spectrum Protect Plus, no puede utilizar un grupo existente. IBM Spectrum Protect Plus crea un grupo de nombre exclusivo para su propio uso. IBM Spectrum Protect Plus cargará directamente los archivos de datos en el almacenamiento de cintas de IBM Spectrum Protect. Algunos archivos de metadatos pequeños se almacenarán en el almacenamiento de objetos de IBM Spectrum Protect. También se coloca una copia de estos archivos de metadatos en el almacenamiento de cintas de IBM Spectrum Protect para fines de recuperación tras desastre.

Tabla 8. Requisitos de descarga y archivado para los proveedores de nube

Operación	**Proveedor**	**Requisitos**
Traspaso de datos	Amazon S3	Se debe especificar un grupo existente de uno de los niveles de almacenamiento soportados.
Traspaso de datos	IBM Cloud Storage	Se debe especificar un grupo existente.
Traspaso de datos	Microsoft Azure	Se debe especificar un contenedor existente del nivel de almacenamiento dinámico o en caliente.
Traspaso de datos	IBM Spectrum Protect	IBM Spectrum Protect Plus crea su propio grupo exclusivo.
Archivado.	Amazon S3	Permite que vSnap se comunique con los puntos finales de IBM Spectrum Protect (servidor de repositorio).
Archivado.	IBM Cloud Storage	Se debe especificar un grupo existente del nivel de archivado.
Archivado.	Microsoft Azure	Se debe especificar un contenedor existente del nivel de almacenamiento dinámico y del nivel de archivado.

Tabla 8. Requisitos de descarga y archivado para los proveedores de nube (continuación)		
Operación	**Proveedor**	**Requisitos**
Archivado.	IBM Spectrum Protect	IBM Spectrum Protect Plus crea su propio grupo exclusivo para copiarlo en el almacenamiento de cintas de IBM Spectrum Protect.

Para obtener información de inicio rápido que le ayude a configurar y descargar los datos en proveedores de nube específicos, consulte: Descarga de datos en almacenamiento de objetos en la nube con IBM Spectrum Protect Plus.

Requisitos del hipervisor

Revise los requisitos del hipervisor para IBM Spectrum Protect Plus.

Para ayudarle a garantizar que las operaciones de copia de seguridad y restauración se pueden ejecutar correctamente, el sistema debe cumplir los requisitos de hardware y software. Utilice los requisitos siguientes como punto de partida. Para los requisitos más actuales, que pueden incluir actualizaciones, consulte nota técnica 2013790.

Requisitos de Hyper-V

El servidor Hyper-V de Microsoft debe cumplir los requisitos mínimos siguientes:

- Hyper-V Server 2016 o Microsoft Hyper-V en Windows Server 2016
- Microsoft Hyper-V en Windows Server 2019

La copia de seguridad y la restauración de discos duros virtuales compartidos (VHDX compartido) no está soportada. Para conocer los problemas y las limitaciones, consulte https://www.ibm.com/support/docview.wss?uid=ibm10884592.

IBM Spectrum Protect Plus no protege los entornos en los que se ha habilitado Hyper-V Replica.

El servicio del iniciador iSCSI de Microsoft debe estar en ejecución en todos los servidores Hyper-V, incluidos los nodos de clúster. En la ventana **Servicios**, establezca el tipo de inicio para el servicio del iniciador iSCSI de Microsoft en **Automático**, para que el servicio esté disponible cuando se inicie el servidor Hyper-V o el nodo de clúster.

El parámetro automount de **DiskPart** debe estar habilitado en el servidor Hyper-V. Para obtener más información sobre la habilitación del parámetro automount, consulte el tema Automount en el sitio web de Microsoft.

Los servidores Hyper-V se pueden registrar utilizando un nombre DNS (Sistema de nombres de dominio) o una dirección IP. IBM Spectrum Protect Plus debe poder resolver los nombres de DNS. Si el servidor Hyper-V forma parte de un clúster, todos los nodos del clúster deben poder resolverse a través de DNS. Si el DNS no está disponible, debe añadir el servidor al archivo `/etc/hosts` en el dispositivo de IBM Spectrum Protect Plus utilizando la línea de mandatos. Si se ha configurado más de un servidor Hyper-V en un entorno de clúster, debe añadir todos los servidores al archivo `/etc/hosts`. Cuando se registra el clúster en IBM Spectrum Protect Plus, registre el gestor de clústeres de migración tras error. .

Requisitos de VMware

Se da soporte a las siguientes versiones de VMware vSphere :

- vSphere 5.5, incluidas todas las actualizaciones y todos los niveles de parche
- vSphere 6.0, incluidas todas las actualizaciones y todos los niveles de parche
- vSphere 6.5, incluidas todas las actualizaciones y todos los niveles de parche
- vSphere 6.7, incluidas todas las actualizaciones y todos los niveles de parche

Asegúrese de que la versión más reciente de las herramientas de VMware esté instalada en el entorno. IBM Spectrum Protect Plus se ha probado con las herramientas de VMware 9.10.0 instaladas.

Los volúmenes RDM físicos (pRDM) no dan soporte a las instantáneas. Las máquinas virtuales que contengan uno o más volúmenes RDM (correlación de dispositivos en bruto) proporcionados en modalidad de compatibilidad física (pRDM) se incluirán en la copia de seguridad. Sin embargo, los volúmenes pRDM no se procesan como parte de la operación de copia de seguridad de máquina virtual.

Requisitos de indexación y restauración de archivos

Revise los requisitos de indexación y restauración de archivos para IBM Spectrum Protect Plus.

Para ayudarle a garantizar que las operaciones de copia de seguridad y restauración se pueden ejecutar correctamente, el sistema debe cumplir los requisitos de hardware y software. Utilice los requisitos siguientes como punto de partida. Para los requisitos más actuales, que pueden incluir actualizaciones, consulte nota técnica 2013790.

Los discos iSCSI que se correlacionan directamente con el sistema operativo invitado no se indexarán. Los volúmenes soportados incluyen volúmenes VMDK o VHD que se montan a través de la configuración de la máquina virtual asociada.

La cantidad de espacio libre necesario para los metadatos en el catálogo, depende del número total de archivos presentes en el entorno. Para catalogar un millón de archivos, el volumen de catálogo en el dispositivo IBM Spectrum Protect Plus necesita aproximadamente 350 MB de espacio libre por versión retenida. El espacio utilizado por los metadatos de indexación de archivos se reclama cuando caducan las instancias de copia de seguridad correspondientes.

Requisitos de VMware

En los valores de la máquina virtual bajo Configuración avanzada, el valor disk.enableUUID debe estar presente y establecido en true.

Requisitos de Windows

Sistemas operativos admitidos	• Windows Server 2008 R2 • Windows Server 2012 R2 y Windows Server 2012 R2 Core • Windows Server 2016 y Windows Server 2016 Core • Windows Server 2019 y Windows Server 2019 Core
Sistemas de archivos soportados	• NTFS • ReFS • CsvFS
Tipos de almacenamiento de disco soportados	Discos básicos con • Particiones MBR • Particiones GPT **Restricción:** La copia de seguridad o la restauración de archivos en discos dinámicos no está soportada.

- IBM Spectrum Protect Plus solo soporta los sistemas operativos disponibles para los hipervisores. Revise la documentación del hipervisor para obtener información sobre los sistemas operativos soportados.

- Las operaciones de indexación y restauración de archivos soportan discos SCSI en un entorno Hyper-V. Los discos IDE (Integrated Drive Electronics) no están soportados. Tenga en cuenta que las máquinas virtuales de Generación 1 requieren discos de arranque IDE; no obstante, si hay disponibles discos SCSI adicionales, las operaciones de indexación y restauración de archivos se soportará en estos discos.
- Se debe habilitar el shell remoto de Windows (WinRM).

  Importante: IBM Spectrum Protect Plus puede proteger y restaurar máquinas virtuales con otros sistemas de archivos, pero solo los sistemas de archivos listados previamente son elegibles para la indexación y la restauración de archivos.
- Cuando se ejecuta la indexación de archivos en un entorno Windows, se omiten los directorios siguientes en el recurso:

  ```
  \Drivers
  \Archivos de programa
  \Archivos de programa (x86)
  \Windows
  \winnt
  ```

  Nota: Los archivos de estos directorios no se añaden al inventario de IBM Spectrum Protect Plus y no están disponibles para la recuperación de archivos.
- Asegúrese de que la versión más reciente de VMware Tools esté instalada en máquinas virtuales VMware y que esté instalado Hyper-V Integration Services en sus máquinas virtuales Hyper-V.

Requisitos de espacio

- La unidad `C:\` debe tener suficiente espacio temporal para guardar los resultados de indexación de archivos.
- Cuando los sistemas de archivos están indexados, los archivos de metadatos temporales se generan en el directorio `/tmp` y después se suprimen en cuanto se completa la indexación. La cantidad de espacio libre necesario para los metadatos depende del número total de archivos presentes en el sistema. Asegúrese de que hay aproximadamente 350 MB de espacio libre por 1 millón de archivos.

Requisitos de conectividad

- El nombre de host del dispositivo de IBM Spectrum Protect Plus se debe poder resolver desde la máquina virtual de Windows.
- La dirección IP de la máquina virtual seleccionada para la indexación debe ser visible para el cliente de vSphere o Hyper-V Manager.
- La máquina virtual de Windows seleccionada para la indexación debe permitir conexiones salientes al puerto 22 (SSH) en el dispositivo de IBM Spectrum Protect Plus.
- Todos los cortafuegos deben estar configurados para permitir que IBM Spectrum Protect Plus se conecte al servidor a través de WinRM.

Requisitos de autenticación y privilegios

Las credenciales que se especifican para la máquina virtual deben incluir a un usuario con los privilegios siguientes:

- La identidad de usuario debe tener el derecho "Iniciar sesión como servicio", que se asigna a través del panel de control de herramientas administrativas en la máquina local (**Política de seguridad local** > **Políticas locales** > **Asignación de derechos de usuario** > **Iniciar sesión como servicio**).

  Para obtener más información sobre el derecho "Iniciar sesión como servicio", consulte Añadir el inicio de sesión como servicio de derecho a una cuenta.
- La política de seguridad predeterminada utiliza el protocolo NTLM de Windows y la identidad de usuario sigue el formato `dominio\Nombre` predeterminado si la máquina virtual Hyper-V está conectada a un dominio. El formato `<administrador local>` se utiliza si el usuario es un administrador local. Tenga en cuenta que las credenciales deben establecerse para la máquina

virtual asociada mediante la opción **Nombre de usuario de SO invitado** y **Contraseña de SO invitado** en la definición de trabajo de copia de seguridad asociada.

- La credencial de inicio de sesión del sistema debe tener los permisos del administrador local.

Requisitos de Kerberos

- La autenticación basada en Kerberos se puede habilitar a través de un archivo de configuración en el dispositivo de IBM Spectrum Protect Plus. Este valor alterará temporalmente el protocolo NTLM predeterminado de Windows. Tenga en cuenta que Kerberos no permite que se utilicen cuentas de usuario locales y solo es adecuado para entornos en los que todas las máquinas están en un solo dominio.
- Solo para la autenticación basada en Kerberos, la identidad de usuario se debe especificar en el formato `username@FQDN`. El usuario especificado debe poder autenticarse utilizando la contraseña registrada para obtener un tíquet de otorgamiento de tíquet (TGT) desde el centro de distribución de claves (KDC) en el dominio especificado por el nombre de dominio completo.
- La autenticación de Kerberos también requiere que el desfase horario entre el controlador de dominio y el dispositivo de IBM Spectrum Protect Plus sea inferior a 5 minutos. Tenga en cuenta que el protocolo NTLM de Windows predeterminado no depende del tiempo.

Requisitos de Linux

Sistemas operativos admitidos	• Niveles de mantenimiento y modificación de Red Hat Enterprise Linux 6.4 y posterior • Niveles de mantenimiento y modificación de CentOS 6.4 y posterior • Niveles de mantenimiento y modificación de Red Hat Enterprise Linux 7.0 y posterior • Niveles de mantenimiento y modificación de CentOS 7.0 y posterior • Niveles de mantenimiento y modificación de SUSE Linux Enterprise Server 12.0 y posterior
Sistemas de archivos soportados	• ext2 • ext3 • ext4 • XFS

- Es posible que un sistema de archivos creado en una versión de kernel más reciente no se pueda montar en un sistema con un kernel más antiguo, en cuyo caso restaurar archivos desde el sistema de archivos más antiguo no está soportado.

  IBM Spectrum Protect Plus solo soporta los sistemas operativos disponibles para los hipervisores. Revise la documentación del hipervisor para obtener información sobre los sistemas operativos soportados.

  Nota: IBM Spectrum Protect Plus puede proteger y restaurar máquinas virtuales con otros sistemas de archivos, pero solo los sistemas de archivos listados previamente son elegibles para la indexación y la restauración de archivos.
- Cuando se ejecuta la indexación de archivos en un entorno Linux, se omiten los directorios siguientes en el recurso:

  ```
  /tmp
  /usr/bin
  /Drivers
  ```

/bin
/sbin

- Los archivos en los sistemas de archivos virtuales como /proc, /sys y /dev también se pasan por alto. Los archivos de estos directorios no se añaden al inventario de IBM Spectrum Protect Plus y no están disponibles para la recuperación de archivos.

Requisitos de espacio

- El disco de sistema debe tener suficiente espacio temporal para guardar los resultados de indexación de archivos.
- Cuando los sistemas de archivos están indexados, los archivos de metadatos temporales se generan en el directorio /tmp y después se suprimen en cuanto se completa la indexación. La cantidad de espacio libre necesario para los metadatos depende del número total de archivos presentes en el sistema. Asegúrese de que hay aproximadamente 350 MB de espacio libre por 1 millón de archivos.

Requisitos de software

- Python versión 2.6 (cualquier nivel) o 2.7 (cualquier nivel) debe estar instalado.
- Red Hat Enterprise Linux/CentOS 6.x únicamente: asegúrese de que el paquete util-linux-ng esté actualizado ejecutando **yum update util-linux-ng**. En función de su versión o distribución, el paquete se puede denominar util-linux.
- Si los datos residen en volúmenes LVM, asegúrese de que la versión de LVM sea 2.0.2.118 o posterior. Ejecute **lvm version** para comprobar la versión y ejecute **yum update lvm2** para actualizar el paquete si es necesario.
- Si los datos residen en volúmenes LVM, el servicio **lvm2-lvmetad** debe estar inhabilitado, porque puede interferir con la posibilidad de que IBM Spectrum Protect Plus monte y vuelva a firmar instantáneas de grupo de volúmenes o clones. Para inhabilitar el servicio, complete los pasos siguientes:

  1. Ejecute los mandatos siguientes:

     ```
     systemctl stop lvm2-lvmetad
     systemctl disable lvm2-lvmetad
     ```

  2. Edite /etc/lvm/lvm.conf y especifique el valor siguiente:

     ```
     use_lvmetad = 0
     ```

     Para obtener información detallada sobre el servicio **lvmetad**, consulte Daemon de metadatos (lvmetad).

- Si los datos residen en sistemas de archivos XFS y la versión de **xfsprogs** está entre 3.2.0 y 4.1.9, la restauración de archivos puede fallar por un problema conocido en **xfsprogs** que produce daños en un clon o un sistema de archivos de instantánea cuando se modifica su UUID. Para resolver este problema, actualice **xfsprogs** a la versión 4.2.0 o superior.

  Para obtener más información, consulte Registros de informes de error Debian.

Requisitos de conectividad

El servicio SSH debe estar en ejecución en el puerto 22 en el servidor y cualquier cortafuegos debe estar configurado para permitir que IBM Spectrum Protect Plus se conecte al servidor mediante SSH. El subsistema SFTP para SSH también debe estar habilitado.

Requisitos de autenticación y privilegios

Las credenciales que se especifican para la máquina virtual deben especificar un usuario que tenga los privilegios **sudo** siguientes:

- La configuración de sudoers debe permitir que el usuario ejecute mandatos sin una contraseña.
- Se debe establecer el valor !requiretty.

El método recomendado consiste en crear un usuario agente de IBM Spectrum Protect Plus dedicado con los privilegios siguientes. Configuración de ejemplo:

- Cree el usuario: `useradd -m sppagent`

  donde **sppagent** especifica el usuario agente de IBM Spectrum Protect Plus
- Establezca una contraseña: `passwd <sppagent>`

Coloque las líneas siguientes en el final del archivo de configuración de `sudoers`, normalmente `/etc/sudoers`. Si el archivo de `sudoers` existente está configurado para importar las configuraciones desde otro directorio (por ejemplo, `/etc/sudoers.d`), también puede colocar las líneas en un archivo nuevo en dicho directorio:

```
Defaults: sppagent !requiretty
sppagent ALL=(root) NOPASSWD:ALL
```

Requisitos de Microsoft Exchange Server

Antes de instalar IBM Spectrum Protect Plus, revise los requisitos de hardware y software para el producto y otros componentes.

Para ayudarle a garantizar que las operaciones de copia de seguridad y restauración se pueden ejecutar correctamente, el sistema debe cumplir los requisitos de hardware y software. Utilice los requisitos siguientes como punto de partida. Para los requisitos más actuales, que pueden incluir actualizaciones, consulte nota técnica 2013790.

Los requisitos de copia y seguridad de base de datos de Exchange para IBM Spectrum Protect Plus son los siguientes.

Configuración

Asegúrese de que la versión de Microsoft Exchange Server que está utilizando está soportada en el sistema operativo.

Versiones de aplicación

- Niveles de mantenimiento de Microsoft Exchange Server 2013 CU16 y CU posterior
- Niveles de mantenimiento de Microsoft Exchange Server 2016 CU 5 y CU posterior: Ediciones Standard y Enterprise.
- Niveles de mantenimiento de Microsoft Exchange Server 2019 y posterior: Ediciones Standard y Enterprise.

Nota: Los grupos de disponibilidad de base de datos de Microsoft Exchange (DAG) están soportados.

Sistemas operativos

- Niveles de mantenimiento de Windows Server 2012R2 y posterior (kernel de 64 bits): Ediciones Standard y Datacenter editions
- Niveles de mantenimiento de Windows Server 2016 y posterior (kernel de 64 bits): Ediciones Standard y Datacenter editions
- Niveles de mantenimiento de Windows Server 2019 y posterior (kernel de 64 bits): Ediciones Standard y Datacenter editions

Nota: La instalación principal de Windows Server 2019 está soportada. No obstante, la característica de restauración granular no está soportada en una instalación principal.

Notas adicionales

Instale los parches y actualizaciones de Microsoft Exchange Server más recientes en el entorno.

Para obtener información sobre el soporte de virtualización para Exchange Server, consulte “Requisitos previos para Microsoft Exchange Server ” en la página 165.

Software

Asegúrese de que se haya instalado una versión soportada de un sistema operativo Windows de 64 bits.

Los siguientes requisitos previos de Microsoft son necesarios y se deben instalar antes de utilizar IBM Spectrum Protect Plus:

- Windows PowerShell 4 o posterior
- Framework de gestión de Windows 4 o posterior

Al utilizar Microsoft Exchange Server 2013 y la característica de restauración granular, el nivel mínimo soportado para el cliente Microsoft Exchange Messaging API (MAPI) y Collaboration Data Objects (MAPI/CDO) es la versión 6.5.8320.0.

Nota: MAPI/CDO solo es necesario para Microsoft Exchange Server 2013. No es necesario si está ejecutando Microsoft Exchange Server 2016 o Exchange Server 2019.

Cuando se utiliza la función de restauración granular con Microsoft Exchange Server 2016 o Microsoft Exchange Server 2019, se necesita Microsoft Outlook 2016 de 32 bits o Microsoft Outlook 2019 de 32 bits.

Los requisitos previos siguientes de Microsoft son necesarios y los instala automáticamente la característica granular de IBM Spectrum Protect Plus, si todavía no está presente en la máquina virtual.

- Paquete redistribuible Microsoft Visual C++ 2012 de 32 bits
- Paquete redistribuible Microsoft Visual C++ 2012 de 64 bits
- Paquete redistribuible Microsoft Visual C++ 2017 de 32 bits
- Paquete redistribuible Microsoft Visual C++ 2017 de 64 bits
- Microsoft .NET Framework 4.5
- Microsoft ReportViewer 2012 SP1 Redistribuible
- Tipos de CLR del sistema de Microsoft SQL Server 2012
- Tipos de CLR del sistema de Microsoft SQL Server 2014
- Tipos de CLR del sistema de Microsoft SQL Server 2016

Consejo: Es posible que la instalación de estos requisitos previos requiera un reinicio del sistema. Para evitar un reinicio del sistema, asegúrese de que estos requisitos previos estén instalados antes de iniciar la función de restauración granular de IBM Spectrum Protect Plus.

Privilegios

Los usuarios agentes de IBM Spectrum Protect Plus tienen los privilegios siguientes:

Microsoft Exchange Server está protegido por la autenticación basada en roles. Para poder conseguir que el agente de Microsoft Exchange funcione en el entorno de IBM Spectrum Protect Plus, debe configurar los privilegios adecuados. Para obtener más información, consulte “Privilegios ” en la página 165.

Puertos

Los agentes de usuario de IBM Spectrum Protect Plus utilizan los puertos siguientes. Los puertos que se indican con "Aceptar" en la columna Regla de cortafuegos utilizan conexiones seguras (HTTPS o SSL).

Tabla 9. Conexiones de cortafuegos de agentes de IBM Spectrum Protect Plus entrantes

Puerto	Protocolo	Regla de cortafuegos	Servicio	Descripción
5985	TCP	Accept	WinRM	Servicio de administración remota de Windows
5986	TCP	Accept	WinRM	Servicio de administración remota segura de Windows

Tabla 10. Conexiones de cortafuegos de agentes de IBM Spectrum Protect Plus salientes

Puerto	Protocolo	Servicio	Descripción
3260*	TCP	iSCSI vSnap	Puerto de destino iSCSI vSnap utilizado para montar LUNS para copia de seguridad y recuperación
137	UDP	vSnap SMB/CIFS	Puerto de destino de vSnap SMB o CIFS utilizado para montar unidades compartidas de sistemas de archivo para copia de seguridad y restauración de registro de transacciones
138	UDP	vSnap SMB/CIFS	Puerto de destino de vSnap SMB o CIFS utilizado para montar unidades compartidas de sistemas de archivo para copia de seguridad y restauración de registro de transacciones
139	TCP	vSnap SMB/CIFS	Puerto de destino de vSnap SMB o CIFS utilizado para montar unidades compartidas de sistemas de archivo para copia de seguridad y restauración de registro de transacciones

Tabla 10. Conexiones de cortafuegos de agentes de IBM Spectrum Protect Plus salientes (continuación)			
Puerto	**Protocolo**	**Servicio**	**Descripción**
445	TCP	vSnap SMB/CIFS	Puerto de destino de vSnap SMB o CIFS utilizado para montar unidades compartidas de sistemas de archivo para copia de seguridad y restauración de registro de transacciones

*El iniciador de iSCSI es necesario en este nodo.

Hardware

Sistema	**Espacio en disco**	**Espacio de disco para operaciones de restauración granular**
x64: hardware compatible soportado por el sistema operativo y Microsoft Exchange Server	Se instalará un mínimo de 200 MB de espacio en disco para el producto que se va a instalar	Por lo menos 2.1 GB de espacio de disco para "Requisitos previos de Microsoft adicionales", que se instalará automáticamente si no lo están

Requisitos de Db2

Antes de registrar Db2 con IBM Spectrum Protect Plus, asegúrese de que el entorno cumpla los requisitos que se describen.

Para ayudarle a garantizar que las operaciones de copia de seguridad y restauración se pueden ejecutar correctamente, el sistema debe cumplir los requisitos de hardware y software. Utilice los requisitos siguientes como punto de partida. Para los requisitos más actuales, que pueden incluir actualizaciones, consulte nota técnica 2013790.

Los requisitos de copia de seguridad y restauración de base de datos de IBM Db2 para IBM Spectrum Protect Plus son los siguientes.

Requisitos de configuración

Se da soporte a las siguientes bases de datos de IBM Db2:

- Niveles de mantenimiento y modificación de IBM Db2 Versión 10.5 y posterior: Enterprise Server Edition.
- Niveles de mantenimiento y modificación de IBM Db2 Versión 11.1 y posterior: Enterprise Server Edition.

Sistemas operativos

Están soportados los sistemas operativos siguientes:

- En PowerPC:
  - Niveles de modificación y de fixpack de AIX 7.1 y posterior (kernel de 64 bits).
  - Niveles de modificación y de fixpack de AIX 7.2 y posterior (kernel de 64 bits).
- En Linux x86_x64:
  - Niveles de mantenimiento y niveles de modificación de Red Hat Enterprise Linux 6.8 y posterior.

  - Niveles de mantenimiento y niveles de modificación de Red Hat Enterprise Linux 7 y posterior.
  - Niveles de mantenimiento y modificación de SUSE Linux Enterprise Server 11.0 SP4 y posterior.
  - Niveles de mantenimiento y niveles de modificación de SUSE Linux Enterprise Server 12.0 SP1 y posterior.
- En Linux on Power System (little endian)
  - Niveles de mantenimiento y modificación de Red Hat Enterprise Linux 7.1 y posterior.
  - Niveles de mantenimiento y modificación de SUSE Linux Enterprise Server 12.0 SP1 y posterior.

Notas adicionales

Instale los últimos parches y actualizaciones de IBM Db2 en el entorno.

IBM Db2 pureScale no está soportada

Asegúrese de que el entorno de Db2 esté configurado para cumplir los criterios siguientes:

- El registro de archivado de Db2 se ha activado y Db2 está en modalidad recuperable.
- Los volúmenes lógicos que contienen espacios de tablas de Db2 (espacios de tablas de datos y temporales), el directorio de bases de datos local y archivos de registro de Db2 que gestiona LVM2 (gestor de volúmenes lógicos) en Linux y JFS2 en AIX, respectivamente. LVM2 en Linux y JFS2 en AIX se utilizan para crear instantáneas de volúmenes temporales. El volumen lógico crece en tamaño con los datos a medida que cambia en el volumen de origen mientras existe la instantánea. Para obtener más información, consulte “LVM2 y JFS2” en la página 144.
- Db2 debe estar en modalidad de copia de seguridad paralela si se deben proteger varias particiones. La modalidad de copia de seguridad paralela se puede habilitar utilizando las variables de registro de Db2. Para obtener más información, consulte el apartado “Requisitos previos para Db2” en la página 141.

Software

Revise los requisitos de software siguientes:

- Los paquetes bash y sudo deben estar instalados. Sudo debe ser la versión 1.7.6p2 o superior. Ejecute sudo -V para comprobar la versión.

  Nota: Los paquetes bash y sudo necesarios se incluyen en los sistemas operativos Linux86_64 y LinuxPower Sytems (little endian) con soporte.
- Python versión 2.6 (cualquier nivel) o 2.7 (cualquier nivel) debe estar instalado en Linux.
- Python versión 2.7.x debe estar instalado en AIX.
- Asegúrese de que esté instalada la versión soportada de Linux x86_64, LinuxPower Systems (little endian) o AIX.

Conectividad

Asegúrese de que los siguientes criterios de conectividad están en vigor:

- El servicio SSH se está ejecutando en el puerto 22 en el servidor.
- Los cortafuegos deben configurarse para permitir que IBM Spectrum Protect Plus se conecte al servidor utilizando SSH.
- El subsistema SFTP para SSH está habilitado.
- El servidor se puede registrar utilizando un nombre de DNS o una dirección IP. IBM Spectrum Protect Plus debe poder resolver los nombres de DNS.
- En AIX, asegúrese de que la comunicación de NFS está configurada con puertos reservados utilizando el mandato: **`nfso -p -o nfs_use_reserved_port=1`**.

Autenticación y privilegios

El servidor de Db2 debe estar registrado en IBM Spectrum Protect Plus utilizando un usuario del sistema operativo que exista en el servidor Db2 (denominado usuario de agente de IBM Spectrum Protect Plus).

Asegúrese de que la contraseña está configurada correctamente y que el usuario puede iniciar la sesión sin enfrentarse a ninguna otra solicitud como, por ejemplo, las solicitudes para restablecer la contraseña.

El usuario del agente de IBM Spectrum Protect Plus deben tener los privilegios siguientes:

- Privilegios para ejecutar mandatos como usuario raíz y como propietario de software de Db2 utilizando sudo. IBM Spectrum Protect Plus requiere esto para varias tareas tales como el descubrimiento de diseños de almacenamiento, el montaje y desmontaje de discos y la gestión de bases de datos.
  - La configuración de sudoers debe permitir que el usuario agente de IBM Spectrum Protect Plus ejecute mandatos sin una contraseña.
  - Se debe establecer el valor `!requiretty`.
- Privilegios para leer el inventario de Db2 utilizando `/usr/local/bin/db2ls`. IBM Spectrum Protect Plus requiere este privilegio para descubrir y recopilar información sobre instancias y bases de datos de IBM Db2.

Puertos

Los agentes de IBM Spectrum Protect Plus utilizan los puertos siguientes. Los puertos que están marcados como Accept utilizan conexiones seguras (HTTPS/SSL).

Tabla 11. Conexiones de cortafuegos de agentes de IBM Spectrum Protect Plus entrantes

Puerto	Protocolo	Cortafuegos	Servicio	Descripción
22	TCP	Accept	SSH	Se utiliza para transferencia de datos SSH a y desde el servidor vSnap interno.

Tabla 12. Conexiones de cortafuegos de agentes de IBM Spectrum Protect Plus salientes

Puerto	Protocolo	Servicio	Descripción
111	TCP	Enlace de puerto RPC vSnap	Permite que los clientes descubran los puertos que los clientes de Open Network Computing (ONC) requieren para comunicarse con servidores ONC.
2049	TCP	NFS vSnap	Se utiliza para compartir archivos NFS a través de vSnap.
20048	TCP	Montaje NFS de vSnap	Monta sistemas de archivos vSnap en clientes tales como proxy VADP, servidores de aplicaciones y almacenes de datos de virtualización.

Requisitos de MongoDB

Antes de registrar MongoDB con IBM Spectrum Protect Plus, asegúrese de que el entorno cumpla los requisitos que se describen.

Para ayudarle a garantizar que las operaciones de copia de seguridad y restauración se pueden ejecutar correctamente, el sistema debe cumplir los requisitos de hardware y software. Utilice los requisitos siguientes como punto de partida. Para los requisitos más actuales, que pueden incluir actualizaciones, consulte nota técnica 2013790.

Los requisitos de copia de seguridad y restauración de la base de datos de MongoDB para IBM Spectrum Protect Plus son los siguientes

Requisitos de configuración

Están soportadas las versiones de base de datos de MongoDB siguientes:

- Niveles de mantenimiento y niveles de modificación de MongoDB Versión 3.6: Ediciones Community Server y Enterprise Server.
- Niveles de mantenimiento y niveles de modificación de MongoDB Versión 4.0: Ediciones Community Server y Enterprise Server.

Sistemas operativos

Están soportados los sistemas operativos siguientes:

- En Linux x86_x64:
  - Niveles de mantenimiento y niveles de modificación de Red Hat Enterprise Linux 6.8 y posterior
  - Niveles de mantenimiento y modificación de CentOS 6.8 y posterior
  - Niveles de mantenimiento y niveles de modificación de Red Hat Enterprise Linux 7 y posterior
  - Niveles de mantenimiento y modificación de CentOS 7 y posterior
  - Niveles de mantenimiento y modificación de SUSE Linux Enterprise Server 12.0 SP1 y posterior
- En Power Systems de Linux (little endian):
  - Niveles de mantenimiento y modificación de Red Hat Enterprise Linux 7.1 y posterior
  - Niveles de mantenimiento y modificación de CentOS 7 y posterior

Nota: en Power Systems de Linux, solo se da soporte a la edición de servidor de empresa de MongoDB.

Notas adicionales

Para ayudar a optimizar el rendimiento, instale los parches y actualizaciones de MongoDB más recientes disponibles para su entorno.

Asegúrese de que el entorno de MongoDB esté configurado para cumplir los criterios siguientes:

- MongoDB está configurado como una instancia autónoma o un conjunto de réplicas. No se da soporte a operaciones de copia de seguridad de instancias de clúster con particiones de MongoDB. Una copia de seguridad siempre incluye todas las bases de datos en la instancia.
- La instancia de MongoDB está configurada para utilizar el motor de almacenamiento WiredTiger.
- El usuario en el registro del servidor de aplicaciones de MongoDB en IBM Spectrum Protect Plus debe poder recuperar información y estado del servidor de la base de datos de administración de MongoDB.
- Los volúmenes lógicos de datos y vías de acceso de registro de MongoDB están gestionados por el Gestor de volúmenes lógicos de Linux (LVM2). LVM2 se utiliza para crear instantáneas de volúmenes temporales. Los archivos de base de datos y el diario deben estar ubicados en un único volumen. El volumen lógico crece en tamaño con los datos a medida que cambia en el volumen de origen mientras existe la instantánea. Para obtener más información, consulte “LVM2 de Linux ” en la página 203.

Software

Revise los requisitos de software siguientes:

- Python versión V2.6 (cualquier nivel) o V2.7 (cualquier nivel) debe estar instalado.
- Cuando el servidor de aplicaciones de MongoDB ejecuta RHEL 6 o CentOS 6, asegúrese de que el paquete `openssl` se encuentre en la versión 1.0.1e-57 o superior. Ejecute `"yum update openssl"` para actualizar este requisito.
- Asegúrese de que está instalada la versión soportada de Linux x86_64 o Linux Power Little Endian.

Conectividad

Asegúrese de que los siguientes criterios de conectividad están en vigor:

- El servicio SSH se está ejecutando en el puerto 22 en el servidor.
- Los cortafuegos deben configurarse para permitir que IBM Spectrum Protect Plus se conecte al servidor utilizando SSH.
- El subsistema SFTP para SSH está habilitado.
- El servidor de aplicaciones se puede registrar en IBM Spectrum Protect Plus utilizando un nombre DNS o una dirección IP. IBM Spectrum Protect Plus debe poder resolver los nombres de DNS.

Autenticación y privilegios

El servidor de MongoDB debe registrarse en IBM Spectrum Protect Plus utilizando un usuario del sistema operativo que exista en el servidor de MongoDB (denominado usuario agente de *IBM Spectrum Protect Plus* en el resto de este tema).

Asegúrese de que la contraseña está configurada correctamente y que el usuario puede iniciar la sesión sin enfrentarse a ninguna otra solicitud como, por ejemplo, las solicitudes para restablecer la contraseña.

En MongoDB, el cifrado basado en SSL y la autenticación basada en certificados no están soportados.

En MongoDB Enterprise Server Editions, solo se da soporte al cifrado en almacenamiento.

El usuario agente de IBM Spectrum Protect Plus deben tener los privilegios siguientes:

- Privilegios para ejecutar mandatos como usuario raíz y como propietario de software de MongoDB utilizando sudo. IBM Spectrum Protect Plus requiere este privilegio para tareas tales como descubrir diseños de almacenamiento y desmontaje de discos y gestión de bases de datos.
  - La configuración de sudoers debe permitir que el usuario agente de IBM Spectrum Protect Plus ejecute mandatos sin una contraseña.
  - Se debe establecer el valor `!requiretty`.
- Privilegios para ejecutar el módulo del servidor estándar de MongoDB `/usr/local/bin/mongodb`. IBM Spectrum Protect Plus requiere que este privilegio utilice la API `pymongo` para conectarse a los servidores de MongoDB utilizando el nombre DNS/IP asignado y el puerto de la instancia. Este mecanismo se utiliza para recopilar información sobre las instancias y bases de datos de MongoDB.
- Si el servidor de MongoDB está protegido mediante autenticación basada en roles, para conseguir que el agente de MongoDB funcione en el entorno de IBM Spectrum Protect Plus, debe configurar los privilegios adecuados. Para obtener más información, consulte el apartado Capítulo 13, “Gestión del acceso de usuarios”, en la página 303. .

Puertos

Los agentes de usuario de IBM Spectrum Protect Plus utilizan los puertos siguientes. Los puertos que se indican con Aceptar en la columna Regla de cortafuegos utilizan conexiones seguras (HTTPS/SSL).

Tabla 13. Conexiones de cortafuegos de agentes de IBM Spectrum Protect Plus entrantes				
Puerto	**Protocolo**	**Regla de cortafuegos**	**Servicio**	**Descripción**
22	TCP	Accept	SSH	Se utiliza para transferencia de datos SSH a y desde el servidor vSnap interno

Tabla 14. Conexiones de cortafuegos de agentes de IBM Spectrum Protect Plus salientes			
Puerto	**Protocolo**	**Servicio**	**Descripción**
111	TCP	Enlace de puerto RPC vSnap	Permite que los clientes descubran los puertos que los clientes de Open Network Computing (ONC) requieren para comunicarse con servidores ONC
2049	TCP	NFS vSnap	Se utiliza para compartir archivos NFS a través de vSnap
20048	TCP	Montaje NFS de vSnap	Monta sistemas de archivos vSnap en clientes tales como proxy VADP, servidores de aplicaciones y almacenes de datos de virtualización

Requisitos de Oracle

Revise los requisitos de copia de seguridad y restauración de la base de datos Oracle para IBM Spectrum Protect Plus.

Para ayudarle a garantizar que las operaciones de copia de seguridad y restauración se pueden ejecutar correctamente, el sistema debe cumplir los requisitos de hardware y software. Utilice los requisitos siguientes como punto de partida. Para los requisitos más actuales, que pueden incluir actualizaciones, consulte nota técnica 2013790.

Requisitos de configuración

Versiones de base de datos

- Oracle 11g R2
- Oracle 12c R1
- Oracle 12c R2
- Oracle 18c

Nota: Para bases de datos de varios arrendatarios en Oracle 12c y posteriores, IBM Spectrum Protect Plus da soporte a la protección y recuperación de la base de datos del contenedor, incluidas todas las bases de datos conectables (PDB) bajo ella. La recuperación granular de PDB específicas se puede realizar a través de la recuperación restauración de disco instantánea combinada con RMAN.

Sistemas operativos

- Niveles de mantenimiento y modificación de AIX 6.1 TL9 y posterior
- Niveles de mantenimiento y modificación de AIX 7.1 y posterior
- Niveles de mantenimiento y modificación de Red Hat Enterprise Linux / CentOS 6.5 y posterior
- Niveles de mantenimiento y modificación de Red Hat Enterprise Linux / CentOS 7.0 y posterior
- Niveles de mantenimiento y modificación de SUSE Linux Enterprise Server 11.0 SP4 y posterior
- Niveles de mantenimiento y modificación de SUSE Linux Enterprise Server 12.0 SP1 y posterior
- Niveles de mantenimiento y modificación de SUSE Linux Enterprise Server 15.0 y posterior

Notas adicionales

- Oracle DataGuard no está soportado.
- Las bases de datos deben estar en modalidad ARCHIVELOG. IBM Spectrum Protect Plus no puede proteger bases de datos que se ejecutan en modalidad NOARCHIVELOG.
- Las recuperaciones de bases de datos Real Application Cluster (RAC) no tienen reconocimiento de agrupación de servidores. IBM Spectrum Protect Plus puede recuperar bases de datos en RAC, pero no en agrupaciones de servidores específicas.
- Las bases de datos RAC se deben configurar de forma que la ubicación del archivo de control de instantáneas de RMAN apunte al almacenamiento compartido accesible para todas las instancias de clúster.
- Cuando se restaura una base de datos de Oracle que se ha configurado para la multihebra en el momento de la copia de seguridad, la base de datos de restauración no es multihebra. La base de datos restaurada se debe volver a configurar manualmente para que utilice la configuración multihebra.

Software

- Los paquetes **bash** y **sudo** deben estar instalados. **sudo** debe tener la versión 1.7.6p2 o superior. Ejecute **sudo -V** para comprobar la versión.
- Python versión 2.6.x o 2.7.x debe estar instalado.
- **Solo RHEL/CentOS 6.x:**

  Para asegurarse de que el paquete `util-linux-ng` esté actualizado, ejecute: **`yum update util-linux-ng`**.

  En función de su versión o distribución, el paquete se puede denominar `util-linux`.

Conectividad

- El servicio SSH debe estar en ejecución en el puerto 22 en el servidor y cualquier cortafuegos debe estar configurado para permitir que IBM Spectrum Protect Plus se conecte al servidor utilizando SSH. El subsistema SFTP para SSH también debe estar habilitado.
- El servidor se puede registrar utilizando un nombre DNS o una dirección IP. IBM Spectrum Protect Plus debe poder resolver los nombres de DNS.
- Si el DNS no está disponible, debe añadir el servidor al archivo `/etc/hosts` en el dispositivo de IBM Spectrum Protect Plus utilizando la línea de mandatos.
- Al registrar nodos RAC de Oracle, registre cada nodo utilizando su IP o nombre físico. No utilice un nombre virtual o un nombre de acceso de cliente único (SCAN).

Autenticación y privilegios

- El servidor de Oracle debe estar registrado en IBM Spectrum Protect Plus utilizando un usuario de sistema operativo que exista en el servidor de Oracle. En adelante, el usuario se denominará el usuario agente de IBM Spectrum Protect Plus.

- Asegúrese de que la contraseña está configurada correctamente y que el usuario puede iniciar la sesión sin otras solicitudes como, por ejemplo, las solicitudes para restablecer la contraseña.

El usuario del agente de IBM Spectrum Protect Plus deben tener los privilegios siguientes:

- Privilegios para ejecutar mandatos como usuario root y como usuarios de propietario de software de Oracle (por ejemplo, `oracle`, `grid`) utilizando **sudo**. Estos privilegios son necesarios para tareas como, por ejemplo, el descubrimiento de diseños de almacenamiento, el montaje y desmontaje de discos y la gestión de bases de datos y ASM.
  - La configuración de `sudoers` debe permitir que el usuario agente de IBM Spectrum Protect Plus ejecute mandatos sin una contraseña.
  - Se debe establecer el valor !requiretty.
  - El valor ENV_KEEP debe permitir que se conserven las variables de entorno ORACLE_HOME y ORACLE_SID.
- Privilegios para leer el inventario de Oracle. Estos privilegios son necesarios para tareas como, por ejemplo, el descubrimiento y la recopilación de información sobre bases de datos y ubicaciones de Oracle.

  Para conseguir esto, el usuario agente de IBM Spectrum Protect Plus debe pertenecer al grupo de inventario de Oracle, normalmente denominado `oinstall`.

Para obtener información sobre la creación de un nuevo usuario con los privilegios necesarios, consulte "Configuración de ejemplo de un usuario agente de IBM Spectrum Protect Plus" en la página 42

NFS

El servidor Oracle debe tener instalado el cliente NFS de Linux o AIX nativo. IBM Spectrum Protect Plus utiliza NFS para montar volúmenes de almacenamiento para operaciones de copia de seguridad y restauración.

Durante la restauración de la base de datos, se necesita la característica Oracle Direct NFS. IBM Spectrum Protect Plus habilita automáticamente Direct NFS si todavía no está habilitado.

Para que Direct NFS funcione correctamente, el ejecutable `<ORACLE_HOME>/bin/oradism` en cada inicio de Oracle debe ser propiedad del usuario raíz y tener privilegios setuid. Normalmente, esto está preconfigurado por el instalador de Oracle, pero en determinados sistemas, es posible que el binario no tenga los privilegios necesarios. Para obtener más información, consulte el documento El inicio de la base de datos ha fallado con Direct NFS en el sitio web de soporte de Oracle.

Ejecute los mandatos siguientes para establecer los privilegios correctos:

- `chown root:oinstall <ORACLE_HOME>/bin/oradism`
- `chmod 750 <ORACLE_HOME>/bin/oradism`

donde `oinstall` especifica el grupo que es propietario de la instalación.

Descubrimiento de bases de datos

IBM Spectrum Protect Plus descubre instalaciones y bases de datos de Oracle examinando los archivos `/etc/oraInst.loc` y `/etc/oratab`, así como la lista de los procesos de Oracle en ejecución. Si los archivos no están presentes en su ubicación predeterminada, el programa de utilidad "locate" debe estar instalado en el sistema para que IBM Spectrum Protect Plus pueda buscar los archivos.

IBM Spectrum Protect Plus descubre bases de datos y sus diseños de almacenamiento conectándose a las instancias en ejecución y consultando las ubicaciones de sus archivos de datos, archivos de registro, etc. Para que IBM Spectrum Protect Plus pueda descubrir correctamente las bases de datos durante las operaciones de catalogación y copia, las bases de datos deben tener una modalidad "MOUNTED", "READ ONLY" o "READ WRITE". IBM Spectrum Protect Plus no puede descubrir ni proteger las instancias de base de datos que se han cerrado.

Seguimiento de cambios de bloque

IBM Spectrum Protect Plus requiere que Oracle Block Change Tracking esté habilitado en bases de datos protegidas con objeto de realizar de forma eficaz copias de seguridad incrementales. Si Block Change Tracking todavía no está habilitado, IBM Spectrum Protect Plus habilítelo automáticamente durante el trabajo de copia de seguridad.

Para personalizar la ubicación del archivo Block Change Tracking, debe habilitar manualmente la característica Block Change Tracking antes de ejecutar un trabajo de copia de seguridad asociado. Si la característica se habilita automáticamente mediante IBM Spectrum Protect Plus, se utilizan las reglas siguientes para determinar la ubicación del archivo Block Change Tracking:

- Si se establece el parámetro **db_create_file_dest**, el archivo Block Change Tracking se crea en la ubicación especificada por este parámetro.
- Si el parámetro **db_create_file_dest** no está establecido, el archivo Block Change Tracking se crea en el mismo directorio que el espacio de tabla SYSTEM.

Copia de seguridad del registro

- El daemon **cron** debe estar habilitado en el servidor de aplicaciones.
- El usuario agente de IBM Spectrum Protect Plus debe disponer de los privilegios necesarios para utilizar el mandato **crontab** y crear trabajos cron. Los privilegios se pueden otorgar a través del archivo de configuración `cron.allow`.

Configuración de ejemplo de un usuario agente de IBM Spectrum Protect Plus

Los mandatos siguientes son ejemplos para crear y configurar un usuario del sistema operativo que IBM Spectrum Protect Plus utilizará para iniciar la sesión en el servidor de Oracle. La sintaxis del mandato puede variar en función del tipo de sistema operativo y de la versión.

- Cree el usuario que se designará como usuario agente de IBM Spectrum Protect Plus: `useradd -m sppagent`
- Establezca una contraseña: `passwd sppagent`
- Si utiliza la autenticación basada en claves, coloque la clave pública en `/home/sppagent/.ssh/authorized_keys` o el archivo correspondiente en función de la configuración de SSHD, y asegúrese de que se establezcan la propiedad y los permisos correctos como, por ejemplo:

```
chown -R sppagent:sppagent /home/sppagent/.ssh
chmod 700 /home/sppagent/.ssh
chmod 600 /home/sppagent/.ssh/authorized_keys
```

- Añada el usuario a la instalación de Oracle y al grupo OSDBA: `usermod -a -G oinstall,dba sppagent`
- Si ASM se está utilizando, añada también el usuario al grupo OSASM: `usermod -a -G asmadmin sppagent`
- Coloque las líneas siguientes en el final del archivo de configuración de `sudoers`, normalmente `/etc/sudoers`. Si el archivo de `sudoers` existente está configurado para importar la configuración desde otro directorio (por ejemplo, `/etc/sudoers.d`), también puede colocar las líneas en un archivo nuevo en dicho directorio:

```
Defaults:sppagent !requiretty
Defaults:sppagent env_keep+="ORACLE_HOME"
Defaults:sppagent env_keep+="ORACLE_SID"
sppagent ALL=(ALL) NOPASSWD:ALL
```

Puertos

Los agentes de usuario de IBM Spectrum Protect Plus utilizan los puertos siguientes. Los puertos que se indican con "Aceptar" en la columna Regla de cortafuegos utilizan una conexión segura (HTTPS o SSL).

Tabla 15. Conexiones de cortafuegos de agentes de IBM Spectrum Protect Plus entrantes				
Puerto	**Protocolo**	**Regla de cortafuegos**	**Servicio**	**Descripción**
22	TCP	Accept	SSH	Se utiliza para transferencia de datos SSH a y desde el servidor vSnap interno.

Tabla 16. Conexiones de cortafuegos de agentes de IBM Spectrum Protect Plus salientes			
Puerto	**Protocolo**	**Servicio**	**Descripción**
111	TCP	Enlace de puerto RPC vSnap	Permite que los clientes descubran los puertos que los clientes de Open Network Computing (ONC) requieren para comunicarse con servidores ONC.
443	TCP	HTTPS	Permite que el servidor de Oracle se comunique con IBM Spectrum Protect Plus para enviar alertas en caso de errores de copia de seguridad de registro.
2049	TCP	NFS vSnap	Se utiliza para compartir archivos NFS a través de vSnap.
20048	TCP	Montaje NFS de vSnap	Monta sistemas de archivos vSnap en clientes tales como proxy VADP, servidores de aplicaciones y almacenes de datos de virtualización.

Requisitos de Microsoft SQL Server

Revise los requisitos de copia de seguridad y restauración de bases de datos de Microsoft SQL Server para IBM Spectrum Protect Plus.

Para ayudarle a garantizar que las operaciones de copia de seguridad y restauración se pueden ejecutar correctamente, el sistema debe cumplir los requisitos de hardware y software. Utilice los requisitos siguientes como punto de partida. Para los requisitos más actuales, que pueden incluir actualizaciones, consulte nota técnica 2013790.

Configuración

Versiones de base de datos

- SQL Server 2008 R2 SP3
- SQL Server 2012
- SQL Server 2012 SP2
- SQL Server 2014
- SQL Server 2016
- SQL Server 2017

Para obtener el mejor rendimiento, instale los últimos parches y las últimas actualizaciones de SQL Server en el entorno.

Sistemas operativos

- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019

Se debe habilitar el shell remoto de Windows (WinRM).

Debe habilitarse una ruta iSCSI entre el sistema SQL Server y el servidor vSnap. Para obtener más información, consulte Guía de paso a paso de Microsoft iSCSI Initiator.

Los trabajos de inventario de IBM Spectrum Protect Plus descubren bases de datos del sistema y marcan las bases de datos que tienen derecho a protección. Las copias de seguridad de registro se marcan como inadmisible para todas las bases de datos y bases de datos del sistema que se ejecutan en modelo de recuperación simple.

OLTP en memoria

El proceso de transacciones en línea en memoria (OLTP) es un motor de base de datos optimizado para la memoria que se utiliza para mejorar el rendimiento de aplicaciones de base de datos. Este motor está soportado en SQL Server 2014 y posteriores. Los requisitos y las limitaciones siguientes se aplican al uso de OLTP en memoria:

- La vía de acceso del archivo de restauración máxima debe tener menos de 256 caracteres. Si la vía de acceso original supera esta longitud, considere la posibilidad de utilizar una vía de acceso de archivo de restauración personalizado para reducir la longitud.
- Los metadatos que se pueden restaurar están sujetos a prestaciones de restauración del Servicio de instantáneas de volumen (VSS) y SQL Server.

Copia de seguridad incremental

IBM Spectrum Protect Plus utiliza la tecnología de diario de cambios de número de secuencia de actualización (USN) para realizar copias de seguridad incrementales en un entorno de SQL Server. El diario de cambios USN proporciona seguimiento de rangos de escritura para un volumen cuando el tamaño del archivo cumple el requisito de umbral de tamaño de archivo mínimo. El desplazamiento de bytes modificado y la información de extensión de longitud se pueden consultar en un archivo específico.

Los requisitos siguientes habilitan el seguimiento de rango de escritura:

- Windows Server 2012 R2 o posterior
- NTFS versión 3.0 o posterior

Las tecnologías siguientes no están soportadas para el seguimiento de bytes modificados:

- Resilient File System (ReFS)
- Protocolo SMB (Server Message Block) 3.0
- SMB TFO (migración tras error transparente)
- SMB 3.0 con compartición de archivos de escalado (SO)

De forma predeterminada, se asignan 512 MB de espacio para el registro por diario de cambios de USN. Asimismo, cuando se detecta un desbordamiento de diario, se asigna un tamaño de diario de 2 GB para gestionar el sistema de archivos ocupado.

El espacio mínimo necesario para el almacenamiento de instantáneas es de 100 MB, aunque es posible que se necesite más espacio en sistemas con una actividad incrementada. El agente de SQL Server comprueba el espacio de volumen de origen y provocará un error de la copia de seguridad si el espacio libre en el volumen de origen es inferior a 100 MB. Se visualiza un mensaje de aviso en el registro de trabajo cuando el espacio libre es inferior al 10% y, a continuación, la copia de seguridad continúa.

Una copia de seguridad base se fuerza cuando se detectan las condiciones siguientes:

- Se notifica una discontinuidad de diario porque el registro alcanza el tamaño máximo, inhabilita del registro por diario o cambia el ID USN catalogado.
- El tamaño de archivo es menor o igual que el tamaño de umbral rastreado, que es de forma predeterminada de 1 MB .
- Se añade un archivo después de un trabajo de copia de seguridad anterior.

Copia de seguridad del registro

Antes de copiar los archivos de registro en el repositorio de vSnap, IBM Spectrum Protect Plus utiliza la carpeta de copia de seguridad configurada para la instancia de servidor SQL para transferir la recopilación de registros. Debe haber disponible suficiente espacio libre para almacenar los registros de transacción entre trabajos de copia de seguridad. El área de transferencia se puede modificar cambiando la configuración de la carpeta de copia de seguridad con SQL Server Management Studio (SSMS).

Para garantizar que la copia de seguridad de registro de SQL Server funcione correctamente, es posible que se necesite un cambio de política de grupo de Windows.

El valor de Objeto de política de grupo (GPO) para la política **Seguridad de red: nivel de autenticación de LAN Manager**, que se encuentra en **Configuración del sistema** > **Valores de Windows** > **Configuración de seguridad** > **Políticas locales** > **Opciones de seguridad**, debe establecerse en una de las opciones siguientes:

- **No definido**
- **Enviar solo respuesta NTLMv2**
- **Enviar solo respuesta NTLMv2. Rechazar LM**
- **Enviar solo respuesta NTLMv2. Rechazar LM & NTLM**

La opción **Enviar solo respuesta NTLM** no es compatible con la versión de vSnap SMB/CIFS y puede provocar problemas de autenticación de CIFS.

Configuración de los grupos de disponibilidad AlwaysOn de SQL Server

Configure la instancia preferida para operaciones de copia de seguridad utilizando SQL Server Management Studio. Siga estos pasos:

1. Seleccione el nodo **Grupo de disponibilidad**.
2. Seleccione el grupo de disponibilidad que desea configurar y, a continuación, seleccione **Propiedades**.
3. En el cuadro de diálogo **Propiedades de grupo de disponibilidad** , seleccione **Preferencias de copia de seguridad**.

Seleccione una opción cualquiera en el panel **¿Dónde se deben realizar las copias de seguridad?**. Cuando se prefiere la réplica secundaria y hay disponible más de una réplica secundaria, el ejecutor de trabajos de IBM Spectrum Protect Plus seleccionará la primera réplica secundaria en la lista preferida notificada por el agente de SQL Server de IBM Spectrum Protect Plus.

El agente de SQL Server establece el tipo de copia de seguridad VSS en COPY_ONLY.

Registro y autenticación

Registre cada SQL Server con IBM Spectrum Protect Plus por nombre o dirección IP. Al registrar un nodo de SQL Server Cluster (AlwaysOn), registre cada nodo por nombre o dirección IP. Las direcciones IP deben ser de orientación pública y estar a la escucha en el puerto 5985. El nombre de dominio completo debe poder resolverse y direccionarse desde el dispositivo de IBM Spectrum Protect Plus.

La identidad de usuario debe tener derechos suficientes para instalar e iniciar el servicio de herramientas de IBM Spectrum Protect Plus en el nodo, incluido derechos **Iniciar sesión como servicio**. Para obtener más información, consulte el artículo Añadir el inicio de sesión como servicio de derecho a una cuenta en el sitio web de Microsoft.

La identidad de usuario sigue el formato *dominio**Nombre* predeterminado si la máquina virtual está conectada a un dominio. El formato *administrador local* se utiliza si el usuario es un administrador local.

Kerberos

La autenticación basada en Kerberos se puede habilitar especificando un archivo de configuración en el dispositivo de IBM Spectrum Protect Plus. Los valores alterarán temporalmente el protocolo NTLM predeterminado de Windows.

Solo para la autenticación basada en Kerberos, la identidad de usuario se debe especificar en el formato `username@FQDN`. El nombre de usuario debe poder autenticarse utilizando la contraseña registrada para obtener un tíquet de otorgamiento de tíquet (TGT) desde el centro de distribución de claves (KDC) en el dominio especificado por el nombre de dominio completo.

Privilegios

El usuario agente de IBM Spectrum Protect Plus de SQL Server debe tener los siguientes permisos:

- Permisos `public` y `sysadmin` de SQL Server
- Permiso de administración local de Windows, que es necesario para la infraestructura VSS y el acceso de volumen y disco
- Permisos para acceder a los recursos de clúster en un entorno de SQL Server FCI y SQL Server AlwaysOn.

Cada instancia de SQL Server puede utilizar una cuenta de usuario específica para acceder a los recursos de dicha instancia de SQL Server.

La infraestructura basada en SQL Server VDI se utiliza para interactuar con las bases de datos de SQL Server y para registrar operaciones de copia de seguridad y restauración. Una conexión de VDI requiere permisos de SQL Server `sysadmin`. El propietario de una base de datos restaurada no se cambia al propietario original. Se precisa un paso manual para modificar el propietario de una base de datos restaurada. Para obtener más información sobre la infraestructura de VDI, consulte el siguiente artículo de Microsoft: Las operaciones de copia de seguridad y restauración VDI de SQL Server requieren privilegios Sysadmin.

La cuenta de servicio de SQL Server de destino debe tener permisos para acceder a los archivos de restauración de SQL Server. Consulte "Consideraciones administrativas" en el siguiente artículo de Microsoft: Protección de archivos de datos y registros.

El Planificador de tareas de Windows se utiliza para planificar copias de seguridad de registro. Dependiendo del entorno, los usuarios pueden recibir el siguiente error: `Una sesión de inicio de sesión especificada no existe. Puede que ya se haya terminado`. Este error se debe a un valor de política de grupo de acceso de red que debe inhabilitarse. Para obtener más información sobre cómo inhabilitar este GPO, consulte el siguiente artículo de soporte de Microsoft: Una sesión de inicio de sesión especificada no existe. Puede que ya se haya terminado. Se produce un error cuando intenta correlacionarse con una unidad de red de una unidad compartida DFS.

Puertos

Los puertos siguientes son utilizados por los usuarios agentes de IBM Spectrum Protect Plus. Los puertos que están indicados con "Aceptar" utilizan una conexión segura (HTTPS o SSL).

Tabla 17. Conexiones de cortafuegos de agentes de IBM Spectrum Protect Plus entrantes

Puerto	Protocolo	Cortafuegos	Servicio	Descripción
5985	TCP	Accept	WinRM	Servicio de administración remota de Windows
5986	TCP	Accept	WinRM	Servicio de administración remota segura de Windows

Tabla 18. Conexiones de cortafuegos de agentes de IBM Spectrum Protect Plus salientes

Puerto	Protocolo	Servicio	Descripción
3260 El iniciador de iSCSI es necesario en este nodo.	TCP	iSCSI vSnap	Puerto de destino iSCSI vSnap utilizado para montar LUNS para las operaciones de copia de seguridad y recuperación.
137	UDP	vSnap SMB/CIFS	Puerto de destino de vSnap SMB/CIFS utilizado para montar unidades compartidas de sistemas de archivo para las operaciones de copia de seguridad y restauración de registro de transacciones.
138	UDP	vSnap SMB/CIFS	Puerto de destino de vSnap SMB/CIFS utilizado para montar unidades compartidas de sistemas de archivo para las operaciones de copia de seguridad y restauración de registro de transacciones.

Tabla 18. Conexiones de cortafuegos de agentes de IBM Spectrum Protect Plus salientes (continuación)

Puerto	Protocolo	Servicio	Descripción
139	TCP	vSnap SMB/CIFS	Puerto de destino de vSnap SMB/CIFS utilizado para montar unidades compartidas de sistemas de archivo para las operaciones de copia de seguridad y restauración de registro de transacciones.
443	TCP	HTTPS	Permite que SQL Server se comunique con IBM Spectrum Protect Plus para enviar alertas en caso de errores de copia de seguridad de registro.
445	TCP	vSnap SMB/CIFS	Puerto de destino de vSnap SMB/CIFS utilizado para montar unidades compartidas de sistemas de archivo para las operaciones de copia de seguridad y restauración de registro de transacciones.

Obtención del paquete de instalación de IBM Spectrum Protect Plus

Puede obtener el paquete de instalación de IBM Spectrum Protect Plus desde un sitio de descargas de IBM, como por ejemplo, Passport Advantage o Fix Central. Estos paquetes contienen archivos que son necesarios para instalar o actualizar los componentes de IBM Spectrum Protect Plus.

Antes de empezar

Para ver la lista de paquetes de instalación por componente, y los enlaces al sitio de descargas de los archivos, consulte Nota técnica 879861.

Procedimiento

Descargue el archivo de instalación adecuado.

Se proporcionan un archivo de instalación diferente para la instalación en sistemas VMware y Microsoft Hyper-V. Asegúrese de descargar el archivo correcto para el entorno.

Importante: No cambie los nombres de los archivos de instalación o actualización. Los nombres de archivo originales son necesarios para que el proceso de instalación o actualización se complete sin errores.

Conceptos relacionados

“Actualización de componentes de IBM Spectrum Protect Plus” en la página 87

Puede actualizar el dispositivo virtual de IBM Spectrum Protect Plus os servidores vSnap y los servidores proxy VADP para obtener las últimas características y mejoras. Los parches de software y las actualizaciones se instalan utilizando la consola administrativa de IBM Spectrum Protect Plus o la interfaz de línea de mandatos para estos componentes.

Tareas relacionadas

"Instalación de IBM Spectrum Protect Plus como un dispositivo virtual VMware" en la página 49
Para instalar IBM Spectrum Protect Plus en un entorno de VMware, despliegue una plantilla OVF (Open Virtualization Format). Al desplegar una plantilla OVF, se crea un dispositivo virtual que contiene la aplicación en un host de VMware como, por ejemplo, un servidor ESXi.

"Instalación de IBM Spectrum Protect Plus como un dispositivo virtual Hyper-V" en la página 51
Para instalar IBM Spectrum Protect Plus en un entorno de Microsoft Hyper-V, importe la plantilla de IBM Spectrum Protect Plus para Hyper-V. Al importar una plantilla, se crea un dispositivo virtual que contiene la aplicación de IBM Spectrum Protect Plus en una máquina virtual Hyper-V. En el dispositivo virtual, también se instala un servidor vSnap local que ya está nombrado y registrado.

"Instalación de servidores vSnap" en la página 57
Cuando se despliega un dispositivo de IBM Spectrum Protect Plus, se instala automáticamente un servidor vSnap. Este servidor es el destino de copia de seguridad primario. En entornos de empresa más grandes, es posible que se necesiten servidores vSnap adicionales.

Instalación de IBM Spectrum Protect Plus como un dispositivo virtual VMware

Para instalar IBM Spectrum Protect Plus en un entorno de VMware, despliegue una plantilla OVF (Open Virtualization Format). Al desplegar una plantilla OVF, se crea un dispositivo virtual que contiene la aplicación en un host de VMware como, por ejemplo, un servidor ESXi.

Antes de empezar

Complete las tareas siguientes:

- Revise los requisitos del sistema IBM Spectrum Protect Plus en "Requisitos de los componentes " en la página 13 y "Requisitos del hipervisor " en la página 26.
- Descargue el archivo de instalación de la plantilla de dispositivo virtual `CC1QCML.ova` de Passport Advantage Online. Para obtener información sobre la descarga de archivos, consulte Nota técnica 879861.
- Verifique la suma de comprobación MD5 del archivo de instalación de plantilla descargado. Asegúrese de que la suma de comprobación generada coincide con la que se proporciona en el archivo de suma de comprobación de MD5, que forma parte de la descarga de software.
- Durante el despliegue, se le solicitará que especifique las propiedades de red desde la interfaz de usuario de VMware. Puede especificar una configuración de dirección IP estática, o dejar todos los campos en blanco para utilizar una configuración de DHCP.
- Para volver a asignar una dirección IP estática después del despliegue, puede utilizar la herramienta de Interfaz de usuario de texto de NetworkManager (nmtui). Para obtener más información, consulte "Asignación de una dirección IP estática" en la página 53.

Tenga en cuenta lo siguiente:

- Tal vez sea necesario configurar una agrupación de direcciones IP que esté asociada a la red de la máquina virtual en la que tiene previsto desplegar IBM Spectrum Protect Plus. La configuración correcta de la agrupación de direcciones IP incluye la configuración del rango de direcciones IP (si se utiliza), máscara de red, pasarela, serie de búsqueda DNS y una dirección IP de servidor DNS.
- Si el nombre de host del dispositivo de IBM Spectrum Protect Plus cambia después del despliegue, ya sea por la intervención del usuario o si se adquiere una nueva dirección IP a través de DNS, deberá reiniciarse el dispositivo de IBM Spectrum Protect Plus.
- Antes del despliegue, debe configurarse correctamente una pasarela predeterminada. Hay varias series DNS soportadas, pero deben ir separadas por comas sin utilizar espacios.
- Para las versiones posteriores de vSphere, es posible que sea necesario que vSphere Web Client despliegue los dispositivos de IBM Spectrum Protect Plus.
- IBM Spectrum Protect Plus no se ha probado en los entornos IPv6.

Procedimiento

Para instalar IBM Spectrum Protect Plus como un dispositivo virtual, complete los pasos siguientes:

1. Despliegue IBM Spectrum Protect Plus realizando una de las acciones siguientes:
   a) Si utiliza vSphere Client, en el menú **Acciones** pulse **Desplegar plantilla OVF**.
   b) Si utiliza vSphere Web Client, pulse **Crear/registrar MV** y, a continuación, seleccione **Desplegar una máquina virtual desde un archivo OVF u OVA**.
2. Seleccione un recurso ESXi para ejecutar el dispositivo virtual. Pulse **Siguiente**.
3. Revise los detalles. Pulse **Siguiente**.

   Importante:

   Si utiliza vSphere Web Client, verifique que aparezca `disk.enableUUID = true` en **Configuración adicional**. Si no es el caso, o si utiliza vSphere Client, continúe con los pasos de instalación y habilite esta opción desde vSphere Web Client más adelante.
4. Especifique la ubicación del archivo `CC1QCML.ova` y selecciónela. Pulse **Siguiente**.
5. Asigne un nombre significativo para la plantilla, que se convertirá en el nombre de la máquina virtual. Identifique una ubicación adecuada para desplegar la máquina virtual. Pulse **Siguiente**.
6. Seleccione el almacenamiento en el que se va a instalar el dispositivo virtual. El almacén de datos de este almacenamiento debe configurarse con el host de destino. El archivo de configuración del dispositivo virtual y los archivos de disco virtual se almacenarán en él. Asegúrese de que el almacenamiento sea lo suficientemente grande para alojar el dispositivo virtual, incluidos los archivos de disco virtual asociados. Seleccione el formato de disco de los discos virtuales. El suministro pesado mejora el rendimiento del dispositivo virtual. El suministro ligero utiliza menos espacio de disco, aunque disminuye el rendimiento. Pulse **Siguiente**.
7. Lea los detalles de la plantilla y acepte el Acuerdo de licencia de usuario final. Seleccione **Acepto todos los acuerdos de licencia** para vSphere Client o pulse **Aceptar** para vSphere Web Client. Pulse **Siguiente**.
8. Seleccione las redes que la plantilla desplegada va a utilizar. Es posible que haya disponibles varias redes disponibles en el servidor ESXi pulsando **Red de destino**. Seleccione una red de destino que le permita definir la asignación de direcciones IP adecuada para el despliegue de la máquina virtual. Pulse **Siguiente**.
9. Para vSphere Web Client, especifique los valores de propiedad del dispositivo virtual: DNS, pasarela predeterminada, dominio, dirección IP de red y prefijo de red. Puede proporcionarse una dirección IP estática. Si se deja en blanco, se utilizará una dirección IP dinámica asignada por un servidor DHCP. El prefijo de red debe escribirse mediante la notación CIDR (Classless Inter-Domain Routing), donde los valores válidos oscilan entre 1 y 24. Pulse **Siguiente**.

   Nota: Para vSphere Client, estas propiedades pueden configurarse utilizando la herramienta de Interfaz de usuario de texto NetworkManager (`nmtui`). Asimismo, puede añadirse la información del campo Dominio de búsqueda utilizando este mandato. Para obtener más información, consulte Asignación de una dirección IP estática.
10. Revise los valores de la plantilla. Pulse **Finalizar** para salir del asistente y para iniciar el despliegue de la plantilla OVF.
11. Una vez desplegada la plantilla OVF, encienda la máquina virtual recién creada. Puede encenderla desde vSphere Client.

    Importante: Espere varios minutos hasta que IBM Spectrum Protect Plus se inicialice por completo.

Qué hacer a continuación

Una vez desplegado el dispositivo virtual, se registrarán e instalarán la aplicación de IBM Spectrum Protect Plus y el servidor vSnap local incorporado en ella. Para iniciar IBM Spectrum Protect Plus, realice las siguientes acciones:

Acción	Cómo
Conéctese a la consola del dispositivo virtual de IBM Spectrum Protect Plus utilizando la consola remota de VMware o SSH. Defina las configuraciones de red utilizando la Interfaz de usuario de texto NetworkManager (`nmtui`).	Consulte Asignación de una dirección IP estática.
Cargue la clave del producto.	Consulte “Carga de la clave de producto” en la página 53.
Inicie IBM Spectrum Protect Plus desde un navegador web soportado.	Consulte “Iniciar IBM Spectrum Protect Plus” en la página 75.

Instalación de IBM Spectrum Protect Plus como un dispositivo virtual Hyper-V

Para instalar IBM Spectrum Protect Plus en un entorno de Microsoft Hyper-V, importe la plantilla de IBM Spectrum Protect Plus para Hyper-V. Al importar una plantilla, se crea un dispositivo virtual que contiene la aplicación de IBM Spectrum Protect Plus en una máquina virtual Hyper-V. En el dispositivo virtual, también se instala un servidor vSnap local que ya está nombrado y registrado.

Antes de empezar

Complete las tareas siguientes:

- Revise los requisitos del sistema IBM Spectrum Protect Plus en “Requisitos de los componentes ” en la página 13 y “Requisitos del hipervisor ” en la página 26.
- Descargue el archivo de instalación `CC1QDML.exe` de Passport Advantage Online. Para obtener información sobre la descarga de archivos, consulte Nota técnica 879861.
- Revise los requisitos adicionales del sistema Hyper-V. Consulte Requisitos del sistema para Hyper-V en Windows Server.
- Verifique la suma de comprobación MD5 del archivo de instalación de plantilla descargado. Asegúrese de que la suma de comprobación generada coincide con la que se proporciona en el archivo de suma de comprobación de MD5, que forma parte de la descarga de software.
- Si el nombre de host del dispositivo virtual de IBM Spectrum Protect Plus cambia después del despliegue, ya sea por la intervención del usuario o si se adquiere una nueva dirección IP a través de DNS, deberá reiniciarse el dispositivo virtual de IBM Spectrum Protect Plus.
- Todos los servidores Hyper-V, incluidos los nodos de clúster, deben tener el servicio del iniciador iSCSI de Microsoft en ejecución en las listas de servicios. Establezca el tipo de inicio de este servicio en Automático para que se empiece a ejecutar cuando se inicie el servidor.
- Es posible que se requieran privilegios administrativos para realizar algunos pasos del proceso de instalación.

Procedimiento

Para instalar IBM Spectrum Protect Plus como un dispositivo virtual, complete los pasos siguientes:

1. Copie el archivo `CC1QDML.exe` en el servidor Hyper-V.
2. Abra el instalador y complete el asistente de instalación.
3. Abra Hyper-V Manager y seleccione el servidor necesario.
4. En el panel **Acciones** de Hyper-V Manager, pulse **Importar máquina virtual**. Se abre el asistente Importar máquina virtual. Pulse **Siguiente**.
5. En el paso **Buscar carpeta**, pulse **Examinar...** y vaya a la carpeta que se ha designado durante la instalación. Seleccione la carpeta que incluye **SPP-{release}**. Pulse **Siguiente**.

6. En el paso **Seleccionar máquina virtual**, asegúrese de que se haya seleccionado la máquina virtual **SPP-{release}** y pulse **Siguiente**. Se abre el diálogo **Elegir tipo de importación**.
7. En el paso **Elegir tipo de importación**, seleccione **Registrar la máquina virtual en vigor (utilizar el ID exclusivo existente)**. Pulse **Siguiente**.

   Importante: No importe varias alianzas virtuales de IBM Spectrum Protect Plus en un único servidor Hyper-V.
8. En el paso **Conectar red**, establezca la conexión en el conmutador virtual que desee utilizar. Pulse **Siguiente**.
9. En el paso **Resumen**, revise la descripción. Pulse **Finalizar** para cerrar el asistente Importar máquina virtual.
10. En Hyper-V Manager, localice la nueva máquina virtual denominada **SPP-{release}**. Pulse con el botón derecho en esta máquina virtual y seleccione **Configuración**.
11. Se abrirá el diálogo Configuración de esta máquina virtual. En el panel izquierdo, pulse **Hardware > Controlador IDE 0 > Unidad de disco duro**.
12. En la sección Soporte, asegúrese de que se haya seleccionado el disco duro virtual correcto. Anote el nombre de archivo del disco virtual original. Pulse **Editar**.
13. Se abrirá el asistente Editar disco duro virtual. Vaya al paso **Elegir acción**.
14. En el paso **Elegir acción**, pulse **Convertir** y, a continuación, pulse **Siguiente**.
15. En el paso **Elegir formato de disco**, asegúrese de que se haya seleccionado **VHDX**. Pulse **Siguiente**.
16. En el paso **Elegir tipo de disco**, pulse **Tamaño fijo**. Pulse **Siguiente**.
17. En el paso **Configurar disco**, localice la carpeta para almacenar el archivo de disco virtual de la alianza virtual de IBM Spectrum Protect Plus. Utilice el mismo nombre de archivo que ha anotado en el paso 12. Si se reutiliza el mismo directorio de instalación del paso 2, utilice otro nombre. Pulse **Siguiente**.

    Importante: Asegúrese de que la unidad de disco donde reside la carpeta tenga suficiente espacio de disco disponible para alojar el archivo de disco virtual de tamaño fijo.
18. En el paso **Resumen**, revise la descripción. Pulse **Finalizar** para cerrar el asistente Editar disco duro virtual e iniciar la conversión del disco virtual. Cuando finalice el proceso, se podrá suprimir el archivo de disco duro virtual original.
19. En el diálogo Configuración de la máquina virtual, pulse **Examinar**. Abra el archivo de disco duro virtual (VHDX) que se acaba de crear en el paso anterior.
20. Repita los pasos del 12 al 19 para cada disco duro en **Hardware > Controlador SCSI**. Pulse **Aceptar** para cerrar el diálogo Configuración.
21. En Hyper-V Manager, pulse con el botón derecho en la máquina virtual y pulse **Iniciar**.
22. Utilice Hyper-V Manager para identificar la dirección IP de la nueva máquina virtual si la dirección se asigna automáticamente. Para asignar una IP estática a la máquina virtual, utilice la herramienta de Interfaz de usuario de texto de NetworkManager (`nmtui`).

    Para obtener más información, consulte "Asignación de una dirección IP estática" en la página 53.

Qué hacer a continuación

Después de instalar el dispositivo virtual, realice las acciones siguientes:

Acción	Cómo
Reinicie el dispositivo virtual.	Consulte la documentación del dispositivo virtual.
Cargue la clave del producto.	Consulte "Carga de la clave de producto" en la página 53.
Inicie IBM Spectrum Protect Plus desde un navegador web soportado.	Consulte "Iniciar IBM Spectrum Protect Plus" en la página 75.

Asignación de una dirección IP estática

Para reasignar una nueva dirección IP estática después del despliegue inicial, un administrador de red puede asignar una dirección IP estática utilizando la herramienta de Interfaz de usuario de texto de NetworkManager (`nmtui`). Los privilegios sudo son necesarios para ejecutar nmtui.

Procedimiento

Para reasignar una nueva dirección IP estática, asegúrese de que la máquina virtual de IBM Spectrum Protect Plus esté encendida y complete los pasos siguientes:

1. Inicie la sesión en la consola de la máquina virtual con el ID de usuario **serveradmin**.

   La contraseña inicial es `sppDP758`.
2. Desde la línea de mandatos de CentOS, especifique `nmtui` para abrir la interfaz.
3. En el menú principal, seleccione **Editar una conexión** y, a continuación, pulse **Aceptar**.
4. Seleccione la conexión de red y, a continuación, pulse **Editar**.
5. En la pantalla **Editar conexión**, especifique una dirección IP estática disponible que ya no esté en uso.
6. Guarde la configuración de IP estática, pulsando **Aceptar**, y reinicie el dispositivo de IBM Spectrum Protect Plus.

Tareas relacionadas

"Instalación de IBM Spectrum Protect Plus como un dispositivo virtual VMware" en la página 49
Para instalar IBM Spectrum Protect Plus en un entorno de VMware, despliegue una plantilla OVF (Open Virtualization Format). Al desplegar una plantilla OVF, se crea un dispositivo virtual que contiene la aplicación en un host de VMware como, por ejemplo, un servidor ESXi.

"Instalación de IBM Spectrum Protect Plus como un dispositivo virtual Hyper-V" en la página 51
Para instalar IBM Spectrum Protect Plus en un entorno de Microsoft Hyper-V, importe la plantilla de IBM Spectrum Protect Plus para Hyper-V. Al importar una plantilla, se crea un dispositivo virtual que contiene la aplicación de IBM Spectrum Protect Plus en una máquina virtual Hyper-V. En el dispositivo virtual, también se instala un servidor vSnap local que ya está nombrado y registrado.

Carga de la clave de producto

IBM Spectrum Protect Plus se ejecuta en una modalidad de evaluación durante un periodo de tiempo limitado. Se necesita una clave de producto válida para habilitar las características de IBM Spectrum Protect Plus de forma indefinida.

Antes de empezar

Guarde la clave de producto en un sistema con acceso a Internet y registre la ubicación de la clave.

Procedimiento

Para cargar la clave de producto, complete los pasos siguientes:

1. Desde un navegador soportado, especifique el URL siguiente:

   ```
   https://HOSTNAME:8090/
   ```

   Donde *HOSTNAME* es la dirección IP de la máquina virtual en la que se despliega la aplicación.
2. En la ventana de inicio de sesión, seleccione **Tipo de autenticación** > **Sistema**. Escriba la contraseña `serveradmin` para acceder a la consola de administración. La contraseña predeterminada es `sppDP758`.

   Se le solicitará que especifique una nueva contraseña para acceder a la consola de administración la primera vez que inicie la sesión.
3. Pulse **Gestionar las licencias**.

4. Pulse **Elegir archivo** y, a continuación, busque la clave de producto en el sistema.
5. Pulse **Cargar nueva licencia**.
6. Pulse **Finalizar sesión**.

Qué hacer a continuación
Después de cargar la clave del producto, complete la acción siguiente:

Acción	Cómo
Inicie IBM Spectrum Protect Plus desde un navegador web soportado.	Consulte “Iniciar IBM Spectrum Protect Plus” en la página 75.

Edición de puertos de cortafuegos

Utilice los ejemplos proporcionados como referencia para abrir puertos de cortafuegos en servidores de aplicaciones o servidores proxy VADP remotos. Debe restringir el tráfico del puerto solo a la red o los adaptadores necesarios.

Red Hat Enterprise Linux 7 y posteriores, y CentOS 7 y posteriores

abrir puertos en servidores de aplicaciones o servidores proxy VADP remotos

Utilice el siguiente mandato para listar los puertos abiertos:

```
firewall-cmd --list-ports
```

Utilice el siguiente mandato para listar las zonas:

```
firewall-cmd --get-zones
```

Utilice el siguiente mandato para listar la zona que contiene el puerto Ethernet `eth0`:

```
firewall-cmd --get-zone-of-interface=eth0
```

Utilice el siguiente mandato para abrir el puerto *8098* para el tráfico TCP. Este mandato no es permanente.

```
firewall-cmd --add-port 8098/tcp
```

Utilice el siguiente mandato para abrir el puerto *8098* para el tráfico TCP después de reiniciar la reglas de cortafuegos. Utilice este mandato para que los cambios sean persistentes:

```
firewall-cmd --permanent --add-port 8098/tcp
```

Para deshacer el cambio en el puerto, utilice este mandato:

```
firewall-cmd --remove-port 8098/tcp
```

Utilice el siguiente mandato para abrir un rango de puertos:

```
firewall-cmd --permanent --add-port 60000-61000/tcp
```

Utilice el siguiente mandato para volver a cargar las reglas de cortafuegos con las actualizaciones de cortafuegos:

```
firewall-cmd --reload
```

SUSE Linux Enterprise Server 12

Edite las opciones de cortafuegos de seguridad avanzada de SUSE Linux Enterprise Server 12 en el menú **Seguridad y usuarios**. Especifique el nuevo rango de puertos que necesite y aplique los cambios.

Configuraciones del cortafuegos que utilizan tablas IP

El programa de utilidad `iptables` está disponible en la mayoría de distribuciones Linux para habilitar las reglas de cortafuegos y la configuración de políticas. Estas distribuciones Linux incluyen Red Hat Enterprise Linux 6.8, Red Hat Enterprise Linux 7 y posteriores, CentOS 7 y posteriores, y SUSE Linux Enterprise Server 12. Antes de utilizar estos mandatos, compruebe qué zonas de cortafuegos están habilitadas de forma predeterminada. Dependiendo de la configuración de zonas, es posible que deba cambiarse el nombre de los términos INPUT y OUTPUT para que coincidan con una zona para la regla necesaria.

Para Red Hat Enterprise Linux 7 y posteriores, consulte los siguientes mandatos de ejemplo:

Utilice el siguiente mandato para listar las políticas de cortafuegos actuales:

```
sudo iptables -S sudo iptables -L
```

Utilice el siguiente mandato para abrir el puerto *8098* para el tráfico TCP de entrada desde una subred interna *<172.31.1.0/24>*:

```
sudo iptables -A INPUT -p tcp -s 172.31.1.0/24 --dport 8098 -j ACCEPT
```

Utilice el siguiente mandato para abrir el puerto *8098* para el tráfico TCP de salida a una subred interna *<172.31.1.0/24>*:

```
sudo iptables -A OUTPUT -p tcp -d 172.31.1.0/24 --sport 8098 -j ACCEPT
```

Utilice el siguiente mandato para abrir el puerto *8098* para el tráfico TCP de salida a una subred externa *<10.11.1.0/24>* y solo para el adaptador de puerto Ethernet `eth1`:

```
sudo iptables -A OUTPUT -o eth1 -p tcp -d 10.11.1.0/24 --sport 8098 -j ACCEPT
```

Utilice el siguiente mandato para abrir el puerto *8098* para el tráfico TCP de entrada a un rango de direcciones IP CES (de 10.11.1.5 a 10.11.1.11) y solo para el adaptador de puerto Ethernet `eth1`:

```
sudo iptables -A INPUT -i eth1 -p tcp -m iprange --dst-range
10.11.1.5-10.11.1.11 --dport 8098 -j ACCEPT
```

Utilice el siguiente mandato para permitir que un adaptador de puerto Ethernet de red interna `eth1` se comunique con un adaptador de puerto Ethernet de red externa `eth0`:

`sudo iptables -A FORWARD -i eth1 -o eth0 -j ACCEPT`. Este ejemplo es específico para Red Hat Enterprise Linux 7 y posteriores.

Utilice el siguiente mandato para abrir el puerto *8098* para el tráfico de entrada desde la subred *10.18.0.0/24* en el puerto Ethernet `eth1` en la zona pública:

```
iptables -A IN_public_allow -i eth1 -p tcp -s 10.18.0.0/24 --dport 8098 -j
ACCEPT
```

Utilice el siguiente mandato para guardar cambios de regla de cortafuegos para que persistan después de un proceso de reinicio de cortafuegos:

```
sudo iptables-save
```

Utilice el siguiente mandato para detener e iniciar un UFW (Uncomplicated Firewall):

```
service iptables stop service iptables start
```

Capítulo 3. Instalación y configuración de servidores vSnap

Cada instalación de IBM Spectrum Protect Plus requiere como mínimo un servidor vSnap, que es el destino de copia de seguridad primario.

En los entornos VMware e Hyper-V, un servidor vSnap con el nombre localhost se instala automáticamente cuando se despliega inicialmente el dispositivo de IBM Spectrum Protect Plus. Un servidor de vSnap incorporado reside en una partición del dispositivo de IBM Spectrum Protect Plus y se registra e inicializa en IBM Spectrum Protect Plus. En entornos de copia de seguridad más pequeños, es posible que el servidor de vSnap incorporado sea suficiente.

En entornos de empresa más grandes, es posible que se necesiten servidores vSnap adicionales. Para obtener instrucciones sobre el dimensionamiento, la creación y la colocación de componentes en el entorno de IBM Spectrum Protect Plus, consulte Blueprints de IBM Spectrum Protect Plus.

Los servidores vSnap adicionales se pueden instalar en dispositivos virtuales o físicos en cualquier momento después de que el dispositivo de IBM Spectrum Protect Plus esté instalado y desplegado. Después de la instalación, se necesitan algunos pasos de registro y configuración para estos servidores vSnap autónomos.

El proceso de configuración de un servidor vSnap autónomo es el siguiente:

1. Instale el servidor vSnap.
2. Añada el servidor vSnap como un almacenamiento de disco en IBM Spectrum Protect Plus.
3. Inicialice el sistema y cree una agrupación de almacenamiento.

Instalación de servidores vSnap

Cuando se despliega un dispositivo de IBM Spectrum Protect Plus, se instala automáticamente un servidor vSnap. Este servidor es el destino de copia de seguridad primario. En entornos de empresa más grandes, es posible que se necesiten servidores vSnap adicionales.

Antes de empezar

Lleve a cabo los pasos siguientes:

1. Revise los requisitos del sistema vSnap en “Requisitos de los componentes ” en la página 13.
2. Descargue el paquete de instalación. Se proporcionan diferentes archivos de instalación para la instalación en máquinas físicas o virtuales. Asegúrese de descargar los archivos correctos para el entorno. Para obtener más información sobre la descarga de archivos, consulte Nota técnica 879861.

Instalación de un servidor vSnap físico

Se necesita un sistema operativo Linux que sea compatible con instalaciones de vSnap físico para instalar un servidor vSnap en una máquina física.

Procedimiento

1. Instale un sistema operativo Linux que sea compatible con instalaciones de vSnap físico. Consulte “Requisitos de instalación física del servidor vSnap” en la página 18 para ver los sistemas operativos soportados.

   La configuración mínima de la instalación es suficiente, pero también puede instalar paquetes adicionales incluyendo una interfaz gráfica de usuario (GUI). La partición raíz debe tener al menos 8 GB de espacio libre después de la instalación.
2. Edite el archivo `/etc/selinux/config` para cambiar la modalidad SELinux por la de permisiva.

3. Ejecute `setenforce 0` para aplicar inmediatamente el valor sin necesidad de realizar un reinicio.
4. Descargue el archivo de instalación de vSnap `CC1QGML.run` desde Passport Advantage Online. Para obtener información sobre la descarga de archivos, consulte Nota técnica 879861.
5. Convierte el archivo en ejecutable mediante el mandato `chmod + x` *`nombre_archivo`*`.run` y, a continuación, ejecute el ejecutable. Se instalan los paquetes de vSnap, además de todos los componentes necesarios.

Qué hacer a continuación
Después de instalar el servidor vSnap, realice la acción siguiente:

Acción	Cómo
Añada el servidor vSnap a IBM Spectrum Protect Plus y configure el entorno vSnap.	Consulte "Gestión de servidores vSnap" en la página 60.

Instalación de un servidor vSnap virtual y un proxy VADP en un entorno VMware

Para instalar un servidor vSnap virtual y un proxy VADP (vStorage API for Data Protection) en un entorno VMware, despliegue una plantilla OVF (Open Virtualization Format). Se creará una máquina que contiene el servidor vSnap y el proxy VADP.

Antes de empezar
Para facilitar la administración de red, utilice una dirección IP estática para la máquina virtual. Asigne la dirección utilizando la herramienta de Interfaz de usuario de texto de NetworkManager (nmtui). Para obtener instrucciones, consulte "Asignación de una dirección IP estática" en la página 53, Trabajar con el administrador de red al configurar las propiedades de red.

Procedimiento

1. Descargue el archivo de instalación de la plantilla de servidor y proxy `CC1QEML.ova` de Passport Advantage Online. Para obtener información sobre la descarga de archivos, consulte Nota técnica 879861.
2. Para desplegar el servidor vSnap, lleve a cabo una de las acciones siguientes:
   - Si utiliza vSphere Client para desplegar el servidor vSnap, en el menú **Archivo**, pulse **Desplegar plantilla OVF**.
   Si utiliza vSphere Web Client, pulse **Crear/registrar MV**, y a continuación, pulse **Desplegar una máquina virtual desde un archivo OVF u OVA**. Pulse **Siguiente**.
3. Especifique la ubicación del archivo `CC1QEML.ova` y selecciónela. Pulse **Siguiente**.
4. Revise los detalles de la plantilla y acepte el Acuerdo de licencia de usuario final. Pulse **Siguiente**.
5. Asigne un nombre significativo para la plantilla, que se convertirá en el nombre de la máquina virtual. Identifique una ubicación adecuada para desplegar la máquina virtual. Pulse **Siguiente**.
6. Identifique el centro de datos, el servidor y la agrupación de recursos para el despliegue. Cuando se le solicite que seleccione el almacenamiento, hágalo desde los almacenes de datos que ya están configurados en el host de destino. El archivo de configuración de la máquina virtual y los archivos de disco virtuales se almacenan en el almacén de datos. Seleccione un almacén de datos que sea lo suficientemente grande para dar cabida a la máquina virtual y a todos sus archivos de disco virtuales. Pulse **Siguiente**.
7. Seleccione un formato de disco para almacenar los discos virtuales. Para optimizar el rendimiento, puede seleccionar el suministro pesado, que está preseleccionado. El suministro ligero requiere menos espacio en disco, pero puede afectar al rendimiento. Pulse **Siguiente**.
8. Seleccione las redes que la plantilla desplegada va a utilizar. Es posible que haya varias redes disponibles en el servidor ESX pulsando Redes de destino. Seleccione una red de destino que le permita definir la asignación de direcciones IP adecuada para el despliegue de la máquina virtual. Pulse **Siguiente**.
9. Especifique las propiedades de red para la pasarela predeterminada de la máquina virtual, DNS, dominio de búsqueda, dirección IP, prefijo de red y nombre de host de la máquina. Si utiliza una

configuración de protocolo de configuración dinámica de host (DHCP), deje todos los campos en blanco.

Restricción: Una pasarela predeterminada debe estar configurada correctamente antes del despliegue de la plantilla OVF. Hay varias series DNS soportadas, pero deben ir separadas por comas sin utilizar espacios.

El prefijo de red lo debe especificar un administrador de red. El prefijo de red se debe especificar utilizando la notación CIDR; los valores válidos oscilan entre 1 y 24.

10. Proporcione detalles de la configuración de VADP, incluida la dirección IP del dispositivo IBM Spectrum Protect Plus.

    Para el servidor de ESXi 5.5, esta solicitud se muestra cuando la plantilla de despliegue OVF alcanza el paso **Propiedades**.

    Para el servidor de ESXi 6.0 y posterior, esta solicitud se muestra cuando la plantilla de despliegue OVF alcanza el paso **Personalizar plantilla**.
11. Pulse **Siguiente**.
12. Revise las selecciones de plantilla. Pulse **Finalizar** para salir del asistente y para iniciar el despliegue de la plantilla OVF. El despliegue puede tardar un tiempo considerable.
13. Después de desplegar la plantilla OVF, encienda la máquina virtual recién creada. Puede encenderla desde vSphere Client.

    Importante: La máquina virtual debe permanecer encendida para que la aplicación IBM Spectrum Protect Plus sea accesible.
14. Registre la dirección IP de la máquina virtual recién creada.

    La dirección IP es necesaria para acceder al servidor vSnap y registrarlo. Busque la dirección IP en vSphere Client pulsando la máquina virtual y revisando la pestaña **Resumen**.

Qué hacer a continuación

Después de instalar el servidor vSnap, realice la acción siguiente:

Acción	Cómo
Añada el servidor vSnap a IBM Spectrum Protect Plus y configure el entorno vSnap.	Consulte “Gestión de servidores vSnap” en la página 60.
Configure el entorno VADP.	Consulte “Establecimiento de opciones para proxies VADP” en la página 114.

Instalación de un servidor virtual vSnap en un entorno Hyper-V

Para instalar un servidor vSnap en un entorno Hyper-V, importe una plantilla Hyper-V. Se creará una dispositivo virtual que contiene el servidor vSnap en una máquina virtual Hyper-V.

Antes de empezar

Todos los servidores Hyper-V, incluidos los nodos de clúster, deben tener el servicio del iniciador iSCSI de Microsoft en ejecución en la lista de servicios. Establezca el servicio en Automático para que esté disponible cuando se reinicie la máquina.

Procedimiento

1. Descargue el archivo de instalación de vSnap `CC1QFML.exe` desde Passport Advantage Online. Para obtener información sobre la descarga de archivos, consulte Nota técnica 879861.
2. Copie el archivo de instalación en el servidor Hyper-V.
3. Inicie el instalador y complete los pasos de instalación.
4. Abra Hyper-V Manager y seleccione el servidor necesario. Para los requisitos del sistema Hyper-V, consulte Requisitos del sistema para Hyper-V en Windows Server.

5. En el menú **Acciones** de Hyper-V Manager, pulse **Importar máquina virtual**, y a continuación, pulse **Siguiente**. Se abre el diálogo **Buscar carpeta**.
6. Vaya hasta la ubicación de la carpeta Máquinas virtuales dentro de la carpeta vSnap descomprimida. Pulse **Siguiente**. Se abre el diálogo **Seleccionar máquina virtual**.
7. Seleccione vSnap y a continuación, pulse **Siguiente**. Se abre el diálogo **Elegir tipo de importación**.
8. Seleccione el tipo de importación siguiente: **Registre la máquina virtual en su lugar**. Pulse **Siguiente**.
9. Si se abre el diálogo Conectar red, especifique el conmutador virtual que se va a utilizar y, a continuación, pulse **Siguiente**. Se abre el diálogo para completar la importación.
10. Revise la descripción y, a continuación, pulse **Finalizar** para completar el proceso de importación y cierre el asistente de **Importar máquina virtual**. Se importa la máquina virtual.
11. Pulse el botón derecho sobre la máquina virtual recién desplegada, y pulse **Valores**.
12. En la sección denominada Controlador IDE 0, seleccione **Unidad de disco duro**.
13. Pulse **Editar** y, a continuación, pulse **Siguiente**.
14. En la pantalla **Elegir acción**, seleccione **Convertir** y, a continuación, pulse **Siguiente**.
15. Para el Formato de disco, seleccione **VHDX**.
16. Para el tipo de disco, seleccione **Tamaño fijo**.
17. En la opción Configurar disco, asigne al disco un nuevo nombre y, opcionalmente, una nueva ubicación.
18. Revise la descripción y, a continuación, pulse **Finalizar** para completar la conversión.
19. Pulse **Examinar** y, a continuación, localice y seleccione el VHDX que se acaba de crear.
20. Repita los pasos 12 al 18 para cada disco debajo la sección Controlador SCSI.
21. Encienda la máquina virtual desde **Hyper-V Manager**. Si se lo solicitan, seleccione la opción donde el kernel se inicia en modalidad de rescate.
22. Utilice Hyper-V Manager para identificar la dirección IP de la nueva máquina virtual si se asigna automáticamente. Para asignar una IP estática a la máquina virtual utilizando la interfaz de usuario de texto de NetworkManager, consulte la sección siguiente.
23. Si la dirección de la nueva máquina virtual se asigna automáticamente, utilice Hyper-V Manager para identificar la dirección IP. Para asignar una IP estática a una máquina virtual, utilice la herramienta de Interfaz de usuario de texto de NetworkManager (nmtui). Para obtener instrucciones, consulte “Asignación de una dirección IP estática” en la página 53.

Qué hacer a continuación

Después de instalar el servidor vSnap, realice la acción siguiente:

Acción	Cómo
Añada el servidor vSnap a IBM Spectrum Protect Plus y configure el entorno vSnap.	Consulte “Gestión de servidores vSnap” en la página 60.

Gestión de servidores vSnap

Para habilitar los trabajos de copia de seguridad y restauración, se necesita al menos un dispositivo virtual de IBM Spectrum Protect Plus y al menos un servidor vSnap. El servidor vSnap puede estar ubicado en el dispositivo de IBM Spectrum Protect Plus o en su propio dispositivo, o bien puede ser una instalación de vSnap física. Debe añadirse cada ubicación de servidor vSnap para que IBM Spectrum Protect Plus lo reconozca.

Adición de un servidor vSnap como proveedor de almacenamiento de copias de seguridad

El servidor de vSnap incorporado se registra en IBM Spectrum Protect Plus al desplegarse el dispositivo. Debe añadir cualquier servidor adicional que esté instalado en los dispositivos virtuales o físicos para que IBM Spectrum Protect Plus los reconozca.

Antes de empezar

Después de añadir un servidor vSnap como proveedor de almacenamiento de copias de seguridad, es posible que tenga que configurar y administrar determinados aspectos de vSnap, como por ejemplo, la configuración de red o la gestión de agrupaciones de almacenamiento. Para obtener más información, consulte "Referencia de administración del servidor vSnap " en la página 66.

Procedimiento

Para añadir un servidor vSnap como dispositivo de almacenamiento de copias de seguridad, complete los pasos siguientes:

1. Inicie la sesión en la consola del servidor vSnap con el ID de usuario `serveradmin`. La contraseña inicial es `sppDP758`.

   Se le solicitará que cambie esta contraseña durante el primer inicio de sesión.
2. Ejecute el mandato **`vsnap user create`** para crear un nombre de usuario y una contraseña para el servidor vSnap.
3. Inicie la interfaz de usuario de IBM Spectrum Protect Plus especificando el nombre de host o la dirección IP de la máquina virtual donde IBM Spectrum Protect Plus se ha desplegado en un navegador soportado.
4. En el panel de navegación, pulse **Configuración del sistema** > **Almacenamiento de copias de seguridad** > **Disco**.
5. Pulse **Añadir almacenamiento de disco**.
6. Complete los campos en el panel **Propiedades de almacenamiento**:

   Nombre de host/IP
   Especifique la dirección IP o el nombre de host que se pueda resolver del almacenamiento de copias de seguridad.

   Sitio
   Seleccione un sitio para el almacenamiento de copias de seguridad. Las opciones disponibles son **Primario**, **Secundario** o **Añadir un sitio nuevo**. Si hay más de un sitio primario, secundario o definido por el usuario está disponible en IBM Spectrum Protect Plus, el sitio con la mayor cantidad de almacenamiento disponible se utiliza en primer lugar.

   Nombre de usuario
   Especifique el nombre de usuario para el servidor vSnap que creó en el paso "2" en la página 61.

   Contraseña
   Escriba la contraseña del usuario.
7. Pulse **Guardar**.

   IBM Spectrum Protect Plus confirma una conexión de red y añade el dispositivo de almacenamiento de copias de seguridad a la base de datos.

Qué hacer a continuación

Después de añadir un proveedor de almacenamiento de copias de seguridad, realice las acciones siguientes:

Acción	Cómo
Inicialice el servidor de aplicaciones.	Consulte "Inicialización del servidor vSnap" en la página 62.
Expanda la agrupación de almacenamiento de vSnap.	Consulte "Expansión de una agrupación de almacenamiento de vSnap" en la página 64.
Si es necesario, configure y administre determinados aspectos de vSnap, como por ejemplo, la configuración de red o la gestión de agrupaciones de almacenamiento.	"Referencia de administración del servidor vSnap " en la página 66

Tareas relacionadas

"Iniciar IBM Spectrum Protect Plus" en la página 75
Inicie IBM Spectrum Protect Plus para empezar a utilizar la aplicación y sus características.

Edición de valores para un servidor vSnap
Puede editar los valores de un servidor vSnap para que refleje los cambios en el entorno de IBM Spectrum Protect Plus.

Procedimiento

Para editar los valores de un servidor vSnap, complete los pasos siguientes:

1. En el panel de navegación, pulse **Configuración del sistema** > **Almacenamiento de copias de seguridad** > **Disco**.
2. Pulse el icono de edición que está asociado a un servidor vSnap.
   Se visualiza el panel **Editar almacenamiento**.
3. Revise los valores del servidor de vSnap y, a continuación, pulse **Guardar**.

Supresión de un servidor vSnap
Puede suprimir un servidor vSnap que ya no se utilice en el entorno de IBM Spectrum Protect Plus.

Procedimiento

Para suprimir un grupo de recursos, realice estos pasos:

1. En el panel de navegación, pulse **Configuración del sistema** > **Almacenamiento de copias de seguridad** > **Disco**.
2. Pulse el icono de suprimir que está asociado a un servidor vSnap.
3. Pulse **Sí** para suprimir el servidor de IBM Spectrum Protect Plus.

Inicialización del servidor vSnap

El proceso de inicialización prepara un nuevo servidor vSnap para su uso cargando y configurando componentes de software e inicializando la configuración interna. Se trata de un proceso único que solo debe ejecutarse en instalaciones nuevas.

Acerca de esta tarea

Como parte del proceso de inicialización, vSnap crea una agrupación de almacenamiento utilizando todos los discos no utilizados disponibles en el sistema. Los despliegues basados en OVA de vSnap contienen cada uno un disco virtual no utilizado predeterminado de 100 GB que se utiliza para crear la agrupación.

Si no se encuentra ningún disco no utilizado, el proceso de inicialización se completa sin crear una agrupación.

Para obtener información sobre cómo expandir, crear y administrar agrupaciones de almacenamiento, consulte "Gestión de almacenamiento" en la página 67.

Puede utilizar la interfaz de usuario de IBM Spectrum Protect Plus o la consola del servidor vSnap para inicializar servidores vSnap.

En el caso de los servidores que se despliegan en un entorno virtual, la interfaz de usuario proporciona un método simple para ejecutar la operación de inicialización.

En el caso de los servidores que se despliegan en un entorno físico, la consola del servidor de vSnap ofrece más opciones para inicializar el servidor, incluida la posibilidad de crear una agrupación de almacenamiento utilizando opciones de redundancia avanzada y una lista específica de discos.

Finalización de una inicialización simple
Para preparar un servidor vSnap para su uso, debe inicializar el servidor vSnap. Utilice IBM Spectrum Protect Plus para inicializar un servidor vSnap que se despliega en un entorno virtual.

Acerca de esta tarea

Para la instalación de vSnap incorporado que se registra como parte de una instalación de IBM Spectrum Protect Plus, se le solicitará que inicie el proceso de inicialización la primera vez que inicie la sesión en la interfaz de usuario. No es necesario realizar pasos adicionales.

Procedimiento

Para inicializar un servidor vSnap utilizando la interfaz de usuario de IBM Spectrum Protect Plus, complete los pasos siguientes:

1. En el panel de navegación, pulse **Configuración del sistema** > **Almacenamiento de copias de seguridad** > **Disco**.
2. En el menú **Acciones** que está asociado al servidor, seleccione el método de inicialización:

   Inicializar con cifrado
   Habilite el cifrado de los datos de copia de seguridad en el servidor vSnap.

   Inicializar
   Inicialice el servidor vSnap sin el cifrado habilitado.

   El proceso de inicialización se ejecuta en segundo plano y no requiere ninguna interacción adicional del usuario. El proceso puede tardar entre 5 y 10 minutos en completarse.

Finalización de una inicialización avanzada

Utilice la consola del servidor vSnap para inicializar un servidor vSnap que se despliega en un entorno físico. Al inicializarse mediante la consola del servidor vSnap se ofrecen más opciones para inicializar el servidor, incluida la posibilidad de crear una agrupación de almacenamiento utilizando opciones de redundancia avanzada y una lista específica de discos.

Procedimiento

Para inicializar un servidor vSnap utilizando la consola del servidor vSnap, complete los pasos siguientes:

1. Inicie la sesión en la consola del servidor vSnap con el ID de usuario `serveradmin`. La contraseña inicial es `sppDP758`.

   También puede utilizar un ID de usuario que tenga privilegios de administración de vSnap que se crean utilizando el mandato **`vsnap user create`**. Para obtener más información sobre el uso de mandatos de consola, consulte “Referencia de administración del servidor vSnap ” en la página 66.
2. Ejecute el mandato **`vsnap system init -- skip_pool`**. El mandato no requiere ninguna interacción adicional y completa todas las tareas de inicialización salvo la creación de una agrupación de almacenamiento. El proceso puede tardar entre 5 y 10 minutos en completarse.

Qué hacer a continuación

Después de completar la inicialización, complete la acción siguiente:

Acción	Cómo
Crear una agrupación de almacenamiento	Consulte “Gestión de almacenamiento” en la página 67.

Establecimiento de opciones de almacenamiento de vSnap

Puede configurar opciones adicionales relacionadas con el almacenamiento para un servidor vSnap.

Procedimiento

Para establecer las opciones de un servidor vSnap, complete los pasos siguientes:

1. En el panel de navegación, pulse **Configuración del sistema** > **Almacenamiento de copias de seguridad** > **Disco**.

2. Pulse el icono de gestión que está asociado al servidor vSnap y, a continuación, expanda la sección **Opciones de almacenamiento**. Establezca las opciones de almacenamiento.

   Habilitar compresión

   Si esta opción está habilitada, cada bloque de datos de entrada se comprime utilizando un algoritmo de compresión antes de que se grabe en la agrupación de almacenamiento. La compresión consume una cantidad moderada de recursos de CPU adicionales.

   Habilitar eliminación de duplicados

   Si esta opción está habilitada, a cada bloque de datos de entrada se le aplica un algoritmo hash y se compara con los bloques existentes de la agrupación de almacenamiento. Si la compresión está habilitada, los datos se comparan después de comprimirse. Los bloques duplicados se pasan por alto en lugar de grabarse en la agrupación. La eliminación de la duplicación se inhabilita de forma predeterminada porque consume una gran cantidad de recursos de memoria (proporcional a la cantidad de datos de la agrupación) para mantener la tabla de eliminación de duplicación de hashes de bloques.

   Modalidad de grabación síncrona

   La inhabilitación de grabaciones síncronas puede producir pérdida de datos y daños silenciosos de los datos de la copia de seguridad si el servidor de almacenamiento experimenta una interrupción brusca o un reinicio durante un trabajo de copia de seguridad. No inhabilite esta opción a menos que el servidor de almacenamiento resida en un entorno estable que esté protegido adecuadamente frente a anomalías de hardware y de alimentación.

   Cifrado habilitado

   Esta opción muestra el estado de cifrado del servidor vSnap. El cifrado solo se puede habilitar durante la inicialización de vSnap. Esta opción es únicamente para fines informativos.
3. Pulse **Guardar**.

Expansión de una agrupación de almacenamiento de vSnap

Si IBM Spectrum Protect Plus notifica que un servidor vSnap ha alcanzado su capacidad de almacenamiento, la agrupación de almacenamiento de vSnap debe expandirse. Para expandir una agrupación de almacenamiento de vSnap, primero debe añadir discos virtuales o físicos al servidor vSnap, añadiendo discos virtuales a la máquina virtual vSnap o añadiendo discos físicos al servidor físico de vSnap. Consulte la documentación de vSphere para obtener información sobre cómo crear discos virtuales adicionales.

Procedimiento

Para ampliar una agrupación de almacenamiento de vSnap, siga estos pasos:

1. En el panel de navegación, pulse **Configuración del sistema** > **Almacenamiento de copias de seguridad** > **Disco**.
2. Seleccione **Acciones** > **Reescanear** para el servidor vSnap que desea volver a escanear.
3. Pulse el icono de gestión que está asociado al servidor vSnap y, a continuación, expanda la sección **Añadir discos nuevos al almacenamiento de copias de seguridad**.
4. Añada y guarde los discos seleccionados. La agrupación de vSnap se expande según el tamaño de los discos que se añaden.

Establecimiento de una asociación de réplica para un servidor vSnap

Mediante la réplica de almacenamiento de copias de seguridad, puede realizar asíncronamente copias de seguridad de datos de un servidor vSnap a otro.

Antes de empezar

Todos los servidores vSnap deben tener el mismo nivel de versión para que la réplica funcione. La réplica entre distintas versiones no está soportada.

Procedimiento

Para establecer una asociación de réplica, complete los pasos siguientes:

1. En el panel de navegación, pulse **Configuración del sistema** > **Almacenamiento de copias de seguridad** > **Disco**.
2. Pulse el icono de gestión que está asociado al servidor al que desea añadir a una asociación de réplica y a continuación, expanda la sección **Configurar socios de almacenamiento**.
3. Pulse el icono de añadir .
4. En la lista **Seleccionar socio**, seleccione un servidor vSnap con el que establecer una asociación de réplica.
5. Pulse **Añadir socio**.

Qué hacer a continuación

Después de crear una asociación de réplica, realice la acción siguiente para habilitar la réplica:

Acción	Cómo
Seleccione la opción **Almacenamiento de copias de seguridad de copias de seguridad** en la política de SLA que está asociada al trabajo de copia de seguridad.	Consulte "Creación de una política de SLA" en la página 93

Modificación de la velocidad de rendimiento de descarga

Cambie el rendimiento de las operaciones de réplica y descarga de sitios para poder gestionar la actividad de la red en una planificación definida.

Procedimiento

1. En el panel de navegación, pulse **Configuración del sistema** > **Sitio** para abrir el panel **Propiedades del sitio**.
2. Pulse el icono de edición que está asociado al sitio cuyo rendimiento desea cambiar.
3. Pulse **Habilitar regulador**.

   La velocidad del rendimiento se muestra en MB/s.
4. Ajuste el rendimiento:
   - Modificación de la velocidad de rendimiento con las teclas de flecha arriba y abajo.
   - Cambie el valor de los datos. Las opciones son Bytes/s, KB/s, MB/s, o GB/s.

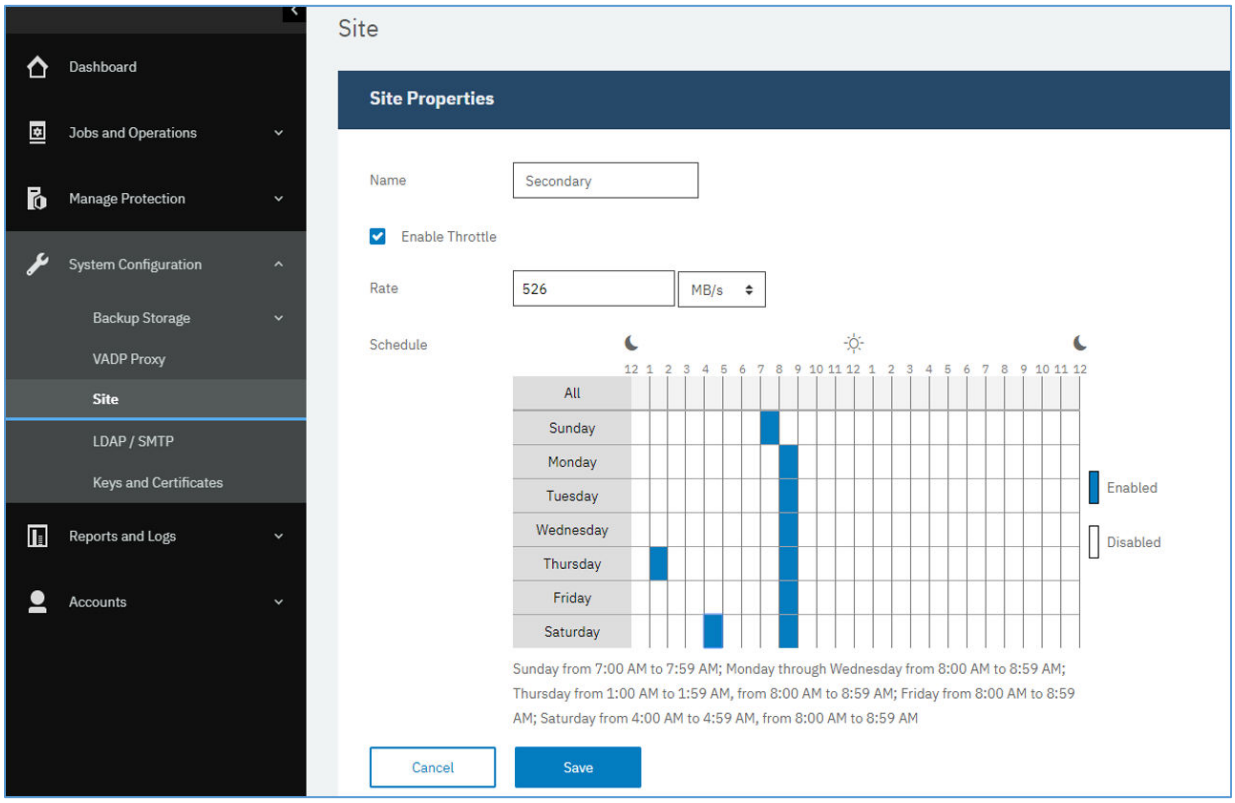


Figura 4. Habilitación de distintos reguladores para diferentes horas para mejorar el rendimiento

5. Seleccione el tiempo para el rendimiento modificado en la tabla de planificación semanal o bien especifique un día y una hora para la velocidad modificada.

   Nota: Para borrar un periodo de tiempo, pulse en él. Las selecciones planificadas se listan debajo de la tabla de planificación.

6. Pulse **Guardar** para confirmar los cambios y cerrar el panel.

Referencia de administración del servidor vSnap

Una vez instalado, registrado e inicializado el servidor vSnap, IBM Spectrum Protect Plus gestiona automáticamente su uso como un destino de copia de seguridad. Los volúmenes y las instantáneas se crean y gestionan automáticamente en función de las políticas de SLA que se definen en IBM Spectrum Protect Plus.

Sin embargo, es posible que todavía deba configurar y administrar determinados aspectos de vSnap, como la configuración de red o la gestión de agrupaciones de almacenamiento.

Gestión de vSnap utilizando la interfaz de línea de mandatos

La interfaz de línea de mandatos de vSnap es el medio principal de administrar vSnap. Ejecute el mandato **vsnap** para acceder a la interfaz de línea de mandatos. El mandato se puede invocar mediante el ID de usuario `serveradmin` o cualquier otro usuario de sistema operativo que tenga privilegios de administración de vSnap. Utilice el mandato **`vsnap user create`** para crear usuarios de sistema operativo adicionales que tengan estos privilegios. La contraseña de `serveradmin` inicial es `sppDP758`.

De forma predeterminada, al usuario `serveradmin` no se le asignan privilegios sudo. Para asignar privilegios sudo al usuario `serveradmin`, inicie la sesión en la interfaz de línea de mandatos del servidor vSnap y especifique el mandato siguiente:

```
echo "serveradmin ALL=(ALL) NOPASSWD: ALL" >/etc/sudoers.d/serveradmin
```

La interfaz de línea de mandatos consta de varios mandatos y submandatos que gestionan varios aspectos del sistema. Consulte "Gestión de almacenamiento" en la página 67 y "Gestión de red" en la página 70 para obtener detalles sobre el uso de estos mandatos. También puede pasar el distintivo **--help** a cualquier mandato o submandato para ver ayuda sobre el uso, por ejemplo, **vsnap --help** o **vsnap pool create --help.**

Gestión de vSnap utilizando la interfaz de usuario de IBM Spectrum Protect Plus

Algunas de las operaciones más comunes también se pueden completar desde la interfaz de usuario de IBM Spectrum Protect Plus. Inicie la sesión a la interfaz de usuario y pulse **Configuración del sistema** > **Almacenamiento de copias de seguridad** > **Disco** en el panel de navegación. Pulse el icono de gestión de un servidor vSnap para gestionarlo.

Tareas relacionadas

"Instalación de servidores vSnap" en la página 57
Cuando se despliega un dispositivo de IBM Spectrum Protect Plus, se instala automáticamente un servidor vSnap. Este servidor es el destino de copia de seguridad primario. En entornos de empresa más grandes, es posible que se necesiten servidores vSnap adicionales.

"Gestión de servidores vSnap" en la página 60
Para habilitar los trabajos de copia de seguridad y restauración, se necesita al menos un dispositivo virtual de IBM Spectrum Protect Plus y al menos un servidor vSnap. El servidor vSnap puede estar ubicado en el dispositivo de IBM Spectrum Protect Plus o en su propio dispositivo, o bien puede ser una instalación de vSnap física. Debe añadirse cada ubicación de servidor vSnap para que IBM Spectrum Protect Plus lo reconozca.

Gestión de almacenamiento

Puede configurar y administrar agrupaciones de almacenamiento para un servidor vSnap.

Gestión de discos

vSnap crea una agrupación de almacenamiento utilizando discos suministrados al servidor vSnap. En el caso de despliegues virtuales, los discos pueden ser RDM o discos virtuales suministrados desde almacenes de datos en cualquier almacenamiento de copia de seguridad. En el caso de despliegues físicos, los discos pueden ser almacenamiento local o SAN conectados al servidor físico. Los discos locales ya pueden tener habilitada la redundancia externa mediante un controlador RAID de hardware, pero si no es así, vSnap también puede crear agrupaciones de almacenamiento basadas en RAID para redundancia interna.

Los discos que están conectados a servidores vSnap deben ser de suministro pesado. Si los discos son de suministro pesado, el servidor vSnap server no tendrá una vista precisa o espacio libre en la agrupación de almacenamiento, lo que puede llevar a la corrupción de datos si el almacén de datos subyacente se queda sin espacio.

Si vSnap se ha desplegado como parte de un dispositivo virtual, ya contiene un disco virtual de inicio de 100 GB que se puede utilizar para crear una agrupación. Puede añadir más discos antes o después de crear una agrupación y, por consiguiente, utilizarlos para crear una agrupación más grande o para ampliar una agrupación existente. Si los registros de trabajo informan de que un servidor vSnap está alcanzando su capacidad de almacenamiento, se pueden añadir discos adicionales a la agrupación de vSnap. De forma alternativa, la creación de políticas de SLA nuevas obligará a las copias de seguridad a utilizar un vSnap alternativo.

Es esencial protegerse contra la corrupción causada por un almacén de datos de VMware en un servidor vSnap que alcanza su capacidad. Cree un entorno estable para servidores vSnap virtuales que no utilicen configuraciones RAID utilizando VMDK de suministro pesado. La réplica a servidores vSnap externos proporciona mayor protección.

Un servidor vSnap se invalidará si se suprime la agrupación de vSnap o si se suprime un disco vSnap en una configuración RAID no redundante. Todos los datos en el servidor vSnap se perderán. Si el servidor vSnap se invalida, debe eliminar el registro del servidor vSnap utilizando la interfaz de IBM Spectrum

Protect Plus y, a continuación, ejecutar el trabajo de mantenimiento. Una vez completado, el servidor vSnap se puede volver a registrar.

Gestión de cifrado

Para habilitar el cifrado de datos de copia de seguridad en un servidor vSnap, seleccione **Inicializar con cifrado habilitado** cuando inicialice el servidor. Los valores de cifrado no se pueden cambiar tras inicializarse el servidor y se crea una agrupación. Todos los discos de una agrupación de vSnap utilizan el mismo archivo de claves de cifrado, que se genera en la creación de la agrupación. Los datos se cifran cuando se encuentran en reposo en el servidor vSnap.

El cifrado de vSnap utiliza el siguiente algoritmo:

Nombre de cifrado
Estándar de cifrado avanzado (AES)

Modalidad de cifrado
xts-plain64

Clave
256 bits

Hashing de cabecera de Linux Unified Key Setup (LUKS)
sha256

Gestión de claves de cifrado

Los archivos de claves de cifrado de disco generados en la creación de la agrupación se almacenan en el directorio /etc/vsnap/keys/ en cada servidor vSnap. Para fines de recuperación tras desastre, vuelva a realizar copias de seguridad de los archivos de claves manualmente fuera del servidor vSnap. Después de crear una agrupación, utilice los mandatos siguientes como usuario serveradmin para copiarlos en una ubicación temporal y, a continuación, copiarlos en una ubicación de copia de seguridad segura y deseada fuera del host vSnap.

```
mkdir /tmp/keybackup-$(hostname)
```

```
sudo cp -r /etc/vsnap/keys /tmp/keybackup-$(hostname)
```

Detección de discos

Si añade discos a un servidor vSnap, utilice la línea de mandatos o la interfaz de usuario de IBM Spectrum Protect Plus para detectar los discos recién conectados.

Línea de mandatos: Ejecute el mandato **`vsnap disk rescan`**.

Interfaz de usuario: Pulse **Configuración del sistema** > **Almacenamiento de copias de seguridad** > **Disco** en el panel de navegación y, a continuación, pulse el menú **Acciones** situado junto al servidor vSnap relevante y seleccione **Reescaneo**.

Mostrar discos

Ejecute el mandato **`vsnap disk show`** para listar todos los discos que están en el sistema vSnap,

La columna USED AS en la salida muestra si cada disco está en uso. Cualquier disco sin formato y sin particiones está marcado como no utilizado; de lo contrario, se marcan como utilizados por la tabla de particiones o por el sistema de archivos que se descubre en ellos.

Solo los discos marcados como no utilizados son admisibles para la creación o adición a una agrupación de almacenamiento. Si un disco que tiene previsto añadir a una agrupación de almacenamiento vSnap no lo ve como no utilizado, puede deberse a que estaba en uso anteriormente y, por lo tanto, contiene restos

de una tabla de particiones o un sistema de archivos anterior. Puede corregirlo utilizando mandatos del sistema como **parted** o **dd** para borrar la tabla de particiones de disco.

Mostrar información de agrupación de almacenamiento

Ejecute el mandato **vsnap pool show** para ver información sobre cada agrupación de almacenamiento.

Creación de una agrupación de almacenamiento

Si ha completado el procedimiento de inicialización simple descrito en "Finalización de una inicialización simple" en la página 62, se ha creado automáticamente una agrupación de almacenamiento y la información de esta sección no es aplicable.

Para completar una inicialización avanzada, utilice el mandato **vsnap pool create** para crear una agrupación de almacenamiento manualmente. Antes de ejecutar el mandato, asegúrese de que uno o más discos no utilizados estén disponibles tal como se describe en "Mostrar discos" en la página 68. Para obtener información sobre las opciones disponibles, pase el distintivo **-- help** para cualquier mandato o submandato.

Especifique un nombre de visualización sencillo para el usuario para la agrupación y una lista de uno o más discos. Si no se especifica ningún disco, se utilizan todos los discos no utilizados disponibles. Puede optar por habilitar la compresión y la deduplicación para la agrupación durante la creación. También puede actualizar los valores de compresión/deduplicación en un momento posterior utilizando el mandato **vsnap pool update**.

El tipo de agrupación que especifique durante la creación de la agrupación de almacenamiento dicta la redundancia de la agrupación:

raid0
: Esta es la opción predeterminada cuando no se especifica ningún tipo de agrupación. En este caso, vSnap supone que los discos tienen redundancia externa, por ejemplo, si utiliza discos virtuales en un almacén de datos con copia de seguridad de almacenamiento redundante. En este caso, la agrupación de almacenamiento no tendrá redundancia interna.

  Una vez que se ha añadido un disco a una agrupación raid0, no se puede eliminar. La desconexión del disco dará como resultado que la agrupación no esté disponible, lo que solo se puede resolver destruyendo y recreando la agrupación.

raid5
: Cuando selecciona esta opción, la agrupación está formada por uno o más grupos RAID5 cada uno formado por tres o más discos. El número de grupos RAID5 y el número de discos de cada grupo depende del número total de discos que especifique durante la creación de la agrupación. Basándose en el número de discos disponibles, vSnap elige los valores que maximizan la capacidad total al mismo tiempo que garantizan la redundancia óptima de los metadatos vitales.

raid6
: Cuando selecciona esta opción, la agrupación está formada por uno o más grupos RAID6 cada uno formado por tres o más discos. El número de grupos RAID6 y el número de discos de cada grupo depende del número total de discos que especifique durante la creación de la agrupación. Basándose en el número de discos disponibles, vSnap elige los valores que maximizan la capacidad total al mismo tiempo que garantizan la redundancia óptima de los metadatos vitales.

Expansión de una agrupación de almacenamiento

Antes de expandir una agrupación, asegúrese de que uno o más discos no utilizados estén disponibles tal como se describe en "Mostrar discos" en la página 68.

Utilice la línea de mandatos o la interfaz de usuario de IBM Spectrum Protect Plus para ampliar una agrupación de almacenamiento.

Línea de mandatos: Ejecute el mandato **vsnap pool expand**. Para obtener información sobre las opciones disponibles, pase el distintivo **-- help** para cualquier mandato o submandato.

Interfaz de usuario: Pulse **Configuración del sistema** > **Almacenamiento de copias de seguridad** > **Disco** en el panel de navegación. Pulse el icono de gestión de un servidor vSnap para gestionarlo y, a continuación, expanda la pestaña **Añadir nuevos discos**. La pestaña visualiza todos los discos sin descubrir en el sistema. Seleccione uno o más discos y pulse **Guardar** para añadirlos a la agrupación de almacenamiento.

Gestión de red

Configure y administre servicios de red para un servidor vSnap.

Mostrar información de interfaz de red

Ejecute el mandato **`vsnap network show`** para listar las interfaces de red y los servicios que están asociados con cada interfaz.

De forma predeterminada, los siguientes servicios de vSnap están a disposición de todas las interfaces de red:

mgmt
Este servicio se utiliza para el tráfico de gestión entre IBM Spectrum Protect Plus y vSnap.

nfs
Este servicio se utiliza para el tráfico de datos al realizar copias de seguridad de datos utilizando NFS.

iscsi
Este servicio se utiliza para el tráfico de datos al realizar copias de seguridad de datos utilizando iSCSI.

smb
Este servicio se utiliza para el tráfico de datos al realizar copias de seguridad de datos utilizando SMB/CIFS.

repl
Este servicio se utiliza para el tráfico de datos entre servidores vSnap durante la réplica.

Modificación de servicios asociados con interfaces de red

Ejecute el mandato **`vsnap network update`** para modificar servicios que están asociados con una interfaz. Por ejemplo, si utiliza una interfaz dedicada para tráfico de datos para mejorar el rendimiento.

Se requieren las opciones siguientes:

`--id <id>`
Especifique el ID de la interfaz que se va a actualizar.

`--services <services>`
Especifique `all` o una lista separada por comas de servicios para habilitar en la interfaz. Lo siguiente son valores válidos: `mgmt`, `nfs`, `smb` y `iscsi`.

Si un servicio está disponible en más de una interfaz, IBM Spectrum Protect Plus puede utilizar cualquiera de las interfaces.

Asegúrese de que el servicio mgmt sigue habilitado en la interfaz que se ha utilizado para registrar el servidor vSnap en IBM Spectrum Protect Plus.

Desinstalación de un servidor vSnap

Puede eliminar un servidor VADP del entorno de IBM Spectrum Protect Plus.

Antes de empezar

Asegúrese de que no hay ningún trabajo que utilice políticas de SLA que definan el servidor vSnap como una ubicación de copia de seguridad. Para ver las políticas de SLA que están asociadas a trabajos, consulte la página **Copia de seguridad** para el hipervisor o la aplicación cuya copia de seguridad se ha

planificado. Por ejemplo, para trabajos de copia de seguridad VMware, pulse **Gestionar protección** > **Hipervisores** > **VMware**.

Procedimiento

1. Inicie la sesión en la consola del servidor vSnap con el ID de usuario `serveradmin`. La contraseña inicial es `sppDP758`.

   También puede utilizar un ID de usuario que tenga privilegios de administrador de vSnap que se crean mediante el mandato **`vsnap user create`**. Para obtener más información sobre el uso de mandatos de consola, consulte "Referencia de administración del servidor vSnap " en la página 66.
2. Ejecute los mandatos siguientes:

   ```
   systemctl stop vsnap
   yum remove vsnap
   ```
3. Opcional: Si no tiene previsto volver a instalar el servidor vSnap después de desinstalarlo, elimine los datos y la configuración ejecutando los mandatos siguientes:

   ```
   rm -rf /etc/vsnap
   rm -rf /etc/nginx
   rm -rf /etc/uwsgi.d
   rm -f /etc/uwsgi.ini
   ```
4. Rearranque el sistema para asegurarse de que se descarguen los módulos de kernel y desconecte los discos de datos que contengan datos de la agrupación de vSnap.

   Nota: Para desinstalar IBM Spectrum Protect Plus en un entorno Hyper-V, suprima el dispositivo SPP de Hyper-V y suprima el directorio de instalación.

Resultados

Una vez desinstalado un servidor vSnap, la configuración se conserva en el directorio `/etc/vsnap`. La configuración se reutiliza si se vuelve a instalar el servidor vSnap. La configuración se elimina si ha ejecutado los mandatos opcionales para eliminar los datos de configuración.

Capítulo 4. Empezar con un inicio rápido

Para empezar a utilizar IBM Spectrum Protect Plus, debe completar los pasos que incluyen la definición de los recursos que desea proteger y la creación de las políticas de acuerdo de nivel de servicio (SLA), también denominadas políticas de copia de seguridad, para dichos recursos. Esta sección de inicio proporciona los pasos básicos para configurar y comenzar a utilizar IBM Spectrum Protect Plus para realizar copias de seguridad de los datos. Otras tareas, como la descarga y la restauración de datos, se describen en detalle en otras áreas de la documentación.

Antes de empezar, asegúrese de que ha seguido las instrucciones de Blueprints de IBM Spectrum Protect Plus para determinar cómo dimensionar, compilar y colocar los componentes que aparecen en el entorno de IBM Spectrum Protect Plus y que las tareas listadas en “Hoja de ruta de despliegue del producto” en la página 13 se han completado.

Tal como se muestra en la tabla siguiente, las tareas iniciales de instalación y configuración las completa el *administrador de infraestructuras* de IBM Spectrum Protect Plus. De forma predeterminada, la cuenta de usuario `admin` se crea para que la utilice el administrador de infraestructuras para iniciar la aplicación por primera vez.

A continuación, el *administrador de aplicaciones* realiza las tareas de copia de seguridad y restauración de la aplicación de hipervisor y base de datos. No obstante, un solo administrador puede ser responsable de todas las tareas del entorno.

Acción	**Propietario**	
Iniciar IBM Spectrum Protect Plus	Administrador de infraestructuras y administrador de aplicaciones	El administrador de infraestructura inicia la aplicación por primera vez utilizando la cuenta de usuario `admin` predeterminada con la contraseña `password`. Se solicita al administrador que restablezca el nombre de usuario de esta cuenta después de iniciar la sesión. El administrador no puede restablecer el nombre de usuario a `admin`, `root` o `test`. Después del arranque inicial, el administrador de la aplicación puede iniciar la aplicación utilizando esta cuenta de usuario u otra cuenta que crea el administrador de infraestructura.

Acción	Propietario	
	Administrador de infraestructuras	Un sitio se utiliza para agrupar servidores vSnap basándose en una ubicación física o lógica para ayudar a identificar e interactuar rápidamente con los datos de copia de seguridad. Se asigna un sitio a un servidor vSnap cuando el servidor se añade a IBM Spectrum Protect Plus. Los sitios predeterminados se denominan Primario y Secundario, pero también puede crearse y asignarse un sitio personalizado cuando se añade el servidor vSnap. Antes de continuar con las siguientes acciones, revise los sitios disponibles y determine si desea añadir nuevos sitios o modificar los existentes.
Crear políticas de copia de seguridad	Administrador de infraestructuras	Las políticas de copia de seguridad definen los parámetros que se aplican a los trabajos de copia de seguridad. Estos parámetros incluyen la frecuencia y retención de copias de seguridad y las opciones para replicar datos de un servidor vSnap a otro y descargar datos de copia de seguridad en el almacenamiento secundario de copias de seguridad para protección a largo plazo. Las políticas de copia de seguridad también definen el sitio de destino para realizar la copia de seguridad de los datos. Un sitio puede contener uno o más servidores vSnap. Las políticas de copia de seguridad se denominan políticas de SLA en IBM Spectrum Protect Plus.
Crear una cuenta de usuario para el administrador de aplicaciones	Administrador de infraestructuras	Las cuentas de usuario determinan los recursos y las funciones que están disponibles para el usuario.

Acción	Propietario	
Añadir recursos para proteger	Administrador de aplicaciones	Los recursos son servidores para hipervisores o aplicaciones de base de datos que alojan los datos que desea proteger.
Añadir recursos a una definición de trabajo	Administrador de aplicaciones	Las definiciones de trabajo asocian los recursos que desea proteger con una o más políticas de SLA. Las opciones y planificaciones que están definidas en las políticas SLA se utilizan para trabajos de copia de seguridad para los recursos.
Iniciar un trabajo de copia de seguridad	Administrador de aplicaciones	Los trabajos de copia de seguridad se inician tal como se define en la política de SLA que está asociada a la definición de trabajo. También puede iniciar manualmente un trabajo.
Ejecutar un informe	Administrador de aplicaciones	IBM Spectrum Protect Plus proporciona un número de informes predefinidos que se pueden ejecutar con parámetros predeterminados o modificarlos para crear informes personalizados.

Iniciar IBM Spectrum Protect Plus

Inicie IBM Spectrum Protect Plus para empezar a utilizar la aplicación y sus características.

Procedimiento

Para iniciar IBM Spectrum Protect Plus, complete los pasos siguientes:

1. En un navegador web soportado, especifique el URL siguiente:

   ```
   https://nombre_host
   ```

   Donde *nombre_host* es la dirección IP de la máquina virtual en la que se despliega la aplicación. Se conectará a IBM Spectrum Protect Plus.
2. Escriba el nombre de usuario y contraseña para iniciar una sesión.

   Si esta es la primera vez que inicia sesión, el nombre de usuario predeterminado es `admin` y la contraseña es `password`. Se le solicita que restablezca el nombre de usuario y la contraseña predeterminados. No puede restablecer el nombre de usuario a `admin`, `root` o `test`.
3. Pulse **Iniciar sesión**.
4. Si está iniciando la sesión en IBM Spectrum Protect Plus por primera vez, se le solicitará que realice las acciones siguientes:

   - Cambie la contraseña de `serveradmin`. La contraseña inicial es `sppDP758`. El usuario `serveradmin` se utiliza para acceder a la consola de administración y al dispositivo virtual de IBM Spectrum Protect Plus. La contraseña de `serveradmin` debe cambiarse antes de acceder a la consola de administración y al dispositivo virtual de IBM Spectrum Protect Plus.

- Inicie el proceso de inicialización del servidor vSnap incorporado. Seleccione **Inicializar** o **Inicializar con el cifrado habilitado** para cifrar los datos en el servidor.

Sitios de gestión

Un sitio se utiliza para agrupar servidores vSnap basándose en una ubicación física o lógica para ayudar a identificar e interactuar rápidamente con los datos de copia de seguridad. Se asigna un sitio a un servidor vSnap cuando el servidor se añade a IBM Spectrum Protect Plus.

Acerca de esta tarea

Se asigna un sitio a un servidor vSnap cuando el servidor se añade a IBM Spectrum Protect Plus. Revise los sitios disponibles pulsando **Configuración del sistema** > **Sitio** en el panel de navegación y decida si desea añadir nuevos sitios o modificar los existentes para los servidores vSnap.

Nota: Puede cambiar el nombre de sitio y otras opciones para los sitios primario y secundario predeterminados.

El sitio de demostración solo está disponible para el servidor vSnap incorporado. No puede utilizar este sitio con ningún otro servidor vSnap.

Procedimiento

Para añadir o editar un sitio, siga estos pasos:

1. En el panel de navegación, pulse **Configuración del sistema** > **Sitio**.
2. Para añadir nuevos sitios o editar sitios existentes, realice la acción correspondiente:

Acción	Procedimiento
Añadir un sitio nuevo.	a. Pulse **Añadir sitio**. b. Especifique un nombre de sitio. c. Opcional: seleccione **Habilitar regulador** para gestionar el rendimiento de las operaciones de descarga y réplica de sitios tal como se describe en "Adición de un sitio" en la página 277. d. Pulse **Guardar**.
Edite un sitio.	a. Pulse **Editar sitio**. b. Pulse el icono de edición que está asociado a un sitio. c. Opcional: seleccione **Habilitar regulador** para gestionar el rendimiento de las operaciones de descarga y réplica de sitios tal como se describe en "Edición de un sitio" en la página 278. d. Pulse **Guardar**.

Conceptos relacionados

"Componentes del producto" en la página 1
La solución IBM Spectrum Protect Plus se proporciona como un dispositivo virtual autocontenido que incluye componentes de almacenamiento y movimiento de datos.

"Gestión de sitios" en la página 277
Un *sitio* es una construcción de política de IBM Spectrum Protect Plus que se utiliza para gestionar la ubicación de datos en un entorno.

Crear políticas de copia de seguridad

Las políticas de copia de seguridad, a las que también se hace referencia como políticas de acuerdo de nivel de servicio (SLA), definen los parámetros que se aplican a los trabajos de copia de seguridad. Estos parámetros incluyen la frecuencia y la retención de copias de seguridad.

Acerca de esta tarea

Las tres políticas de SLA predeterminadas son Oro, Plata y Bronce. Puede utilizar estas políticas tal como están o bien modificarlas. También puede crear políticas de SLA personalizadas.

Si una máquina virtual está asociada a varias políticas de SLA, asegúrese de que las políticas no se han planificado para ejecutarse simultáneamente. Planifíquelas para que se ejecuten con un periodo de tiempo suficiente entre ellas, o bien combínelas en una única política de SLA.

Por ejemplo, esta tarea no incluye instrucciones para habilitar la réplica para servidores vSnap o para la descarga o el archivado en un almacenamiento secundario de copias de seguridad, que son características opcionales. Para obtener información sobre cómo configurar estas características en la política de SLA, consulte "Creación de una política de SLA" en la página 93.

Las copias de seguridad de los datos se denominan instantáneas.

Procedimiento

Para crear una política de SLA, complete los pasos siguientes:

1. En el panel de navegación, pulse **Gestionar protección** > **Descripción general de política**.
2. Pulse **Añadir política de SLA**.

   Se muestra el panel **Nueva política de SLA**.
3. En el campo **Nombre**, escriba un nombre que ofrezca una descripción importante de la política de SLA.
4. En la sección **Protección operativa** en **Política principal**, establezca las opciones siguientes para las operaciones de copia de seguridad. Estas operaciones ocurren en los servidores vSnap que se definen en la ventana **Configuración del sistema** > **Almacenamiento de copias de seguridad** > **Disco**.

   Retención
   Especifique el periodo de retención de las instantáneas de copia de seguridad.

   Deshabilitar planificación
   Marque este recuadro de selección si desea crear la política principal sin definir una frecuencia o una hora de inicio. Las políticas creadas sin una planificación se pueden ejecutar bajo demanda.

   Frecuencia
   Especifique la frecuencia de las operaciones de copia de seguridad.

   Hora de inicio
   Escriba la fecha y hora deseadas para la operación de copia de seguridad.

   Sitio de destino
   Seleccione el sitio de copia de seguridad de destino para realizar la copia de seguridad de los datos.

   Un sitio puede contener uno o más servidores vSnap. Si hay más de un servidor vSnap en un sitio, el servidor de IBM Spectrum Protect Plus gestiona la ubicación de datos en los servidores vSnap.

   En esta lista, solo se muestran los sitios que están asociados con un servidor vSnap. Los sitios que se añaden a IBM Spectrum Protect Plus pero no están asociados con un servidor vSnap no se muestran.

   Utilizar únicamente el almacenamiento de disco cifrado
   Marque este recuadro de selección para realizar una copia de seguridad de los datos en servidores de vSnap cifrados, si el entorno incluye una combinación de servidores cifrados y no cifrados.

   Restricción: Si se selecciona esta opción y no hay disponibles servidores vSnap cifrados, el trabajo asociado no se ejecutará correctamente.

En el ejemplo siguiente se muestra una nueva política de SLA llamada `Cobre` que se ejecuta cada 3 días a medianoche con una retención de 1 mes:

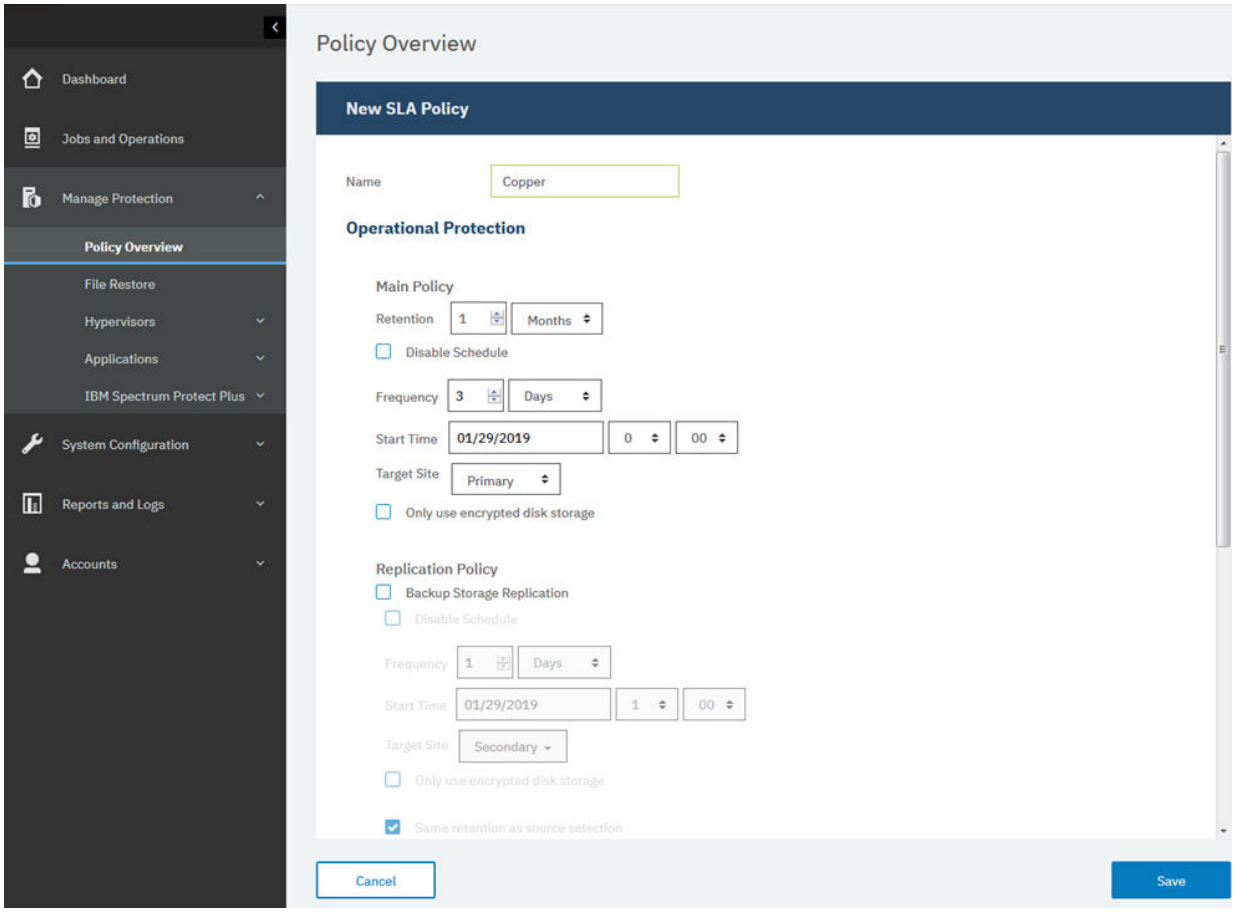


Figura 5. Creación de una política de SLA

5. Pulse **Guardar**. Ahora, la política de SLA se puede aplicar a definiciones de trabajo de copia de seguridad, tal como se muestra en "Añadir recursos a una definición de trabajo" en la página 82.

Conceptos relacionados

"Replicar datos de almacenamiento de copia de seguridad " en la página 6
Cuando habilite la réplica de datos de copia de seguridad, los datos de un servidor vSnap se replican de forma asíncrona en otro servidor vSnap. Por ejemplo, puede replicar los datos de copia de seguridad de un servidor vSnap en un sitio primario en un servidor vSnap en un sitio secundario.

"Descargar en almacenamiento de copia de seguridad secundario" en la página 6
El servidor vSnap es la ubicación de copia de seguridad primaria para las instantáneas. Todos los entornos de IBM Spectrum Protect Plus tienen al menos un servidor vSnap. Opcionalmente, puede descargar instantáneas de un servidor vSnap en un almacenamiento de copias de seguridad secundario.

"Gestión de políticas de SLA para operaciones de copia de seguridad" en la página 93
Las políticas de acuerdo de nivel de servicio (SLA), también denominadas políticas de copia de seguridad, definen parámetros para los trabajos de copia de seguridad. Estos parámetros incluyen la frecuencia y el periodo de retención de las copias de seguridad, y la opción de replicar o descargar los datos de la copia de seguridad. Puede utilizar políticas de SLA predefinidas o personalizarlas según sus necesidades.

Crear una cuenta de usuario para el administrador de aplicaciones

Cree una cuenta de usuario para un administrador que pueda ejecutar operaciones de copia de seguridad y restauración para los hipervisores o las aplicaciones que se encuentran en el entorno.

Antes de empezar

Por ejemplo, los pasos siguientes muestran cómo crear una cuenta para un usuario individual que es responsable de proteger los datos de VMware. Esta cuenta utiliza un rol de usuario y un grupo de recursos existentes.

Para crear una cuenta para un grupo de LDAP, consulte "Creación de una cuenta de usuario para un grupo LDAP" en la página 312.

Para crear roles de usuario y grupos de recursos personalizados, consulte "Creación de un grupo de recursos" en la página 303 y "Creación de un rol" en la página 308

Procedimiento

Para crear una cuenta para un administrador de aplicaciones, complete los pasos siguientes:

1. En el panel de navegación, pulse **Cuentas** > **Usuario**.
2. Pulse **Añadir usuario**. Se muestra el panel **Añadir usuario**.
3. Pulse **Seleccionar el tipo de usuario o grupo que desea añadir** > **Usuario nuevo individual**.
4. Escriba un nombre y una contraseña para el administrador de aplicaciones.
5. En la sección **Asignar rol**, seleccione **VM Admin**.
   Los permisos se muestran en la sección **Grupos de permisos**.

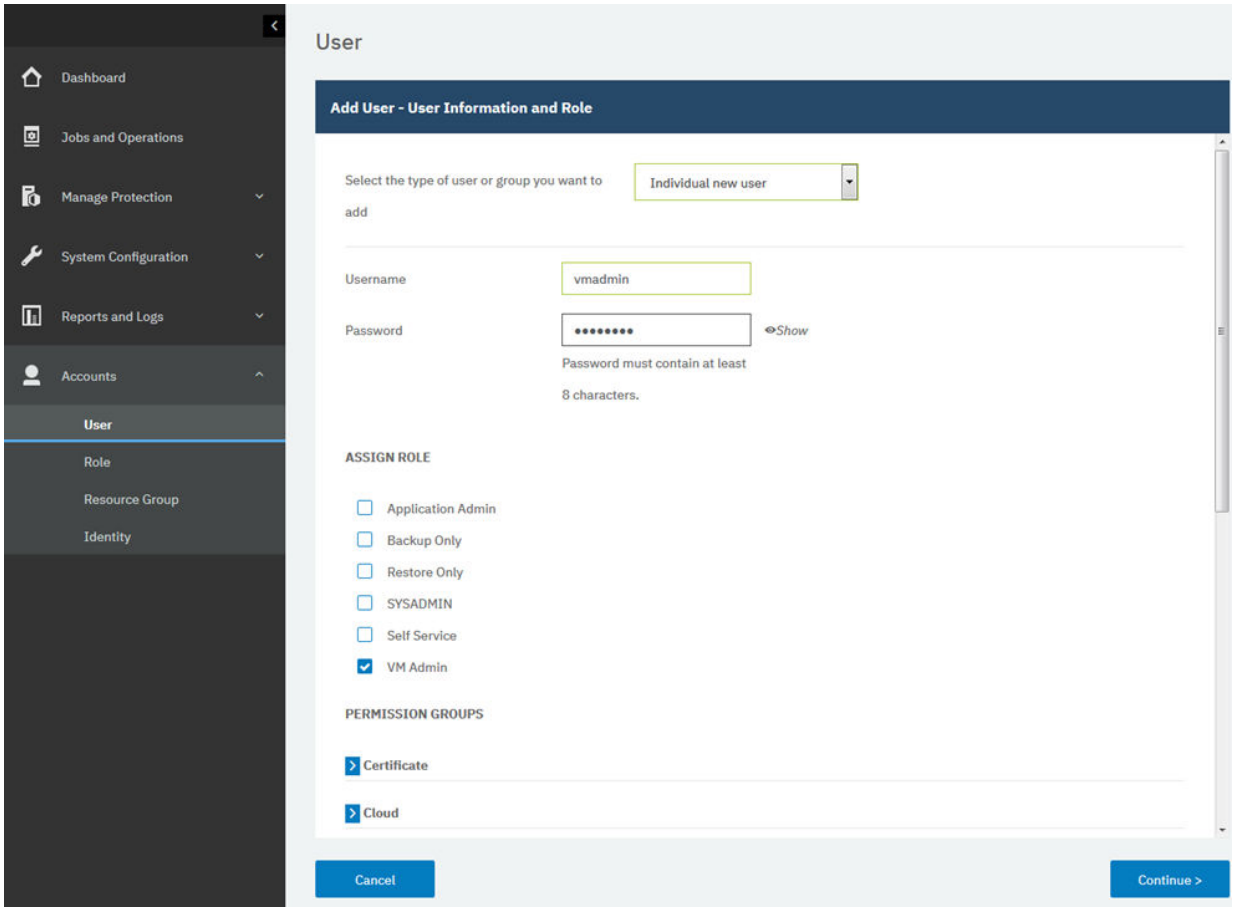


Figura 6. Creación de una cuenta de usuario y asignación de un rol

6. Pulse **Continuar**.
7. En la sección **Añadir usuarios - Asignar recursos**, seleccione el grupo de recursos **Todos los recursos** y, a continuación, pulse **Añadir recursos**.
   El grupo de recursos se añade a la sección **Recursos seleccionados**.

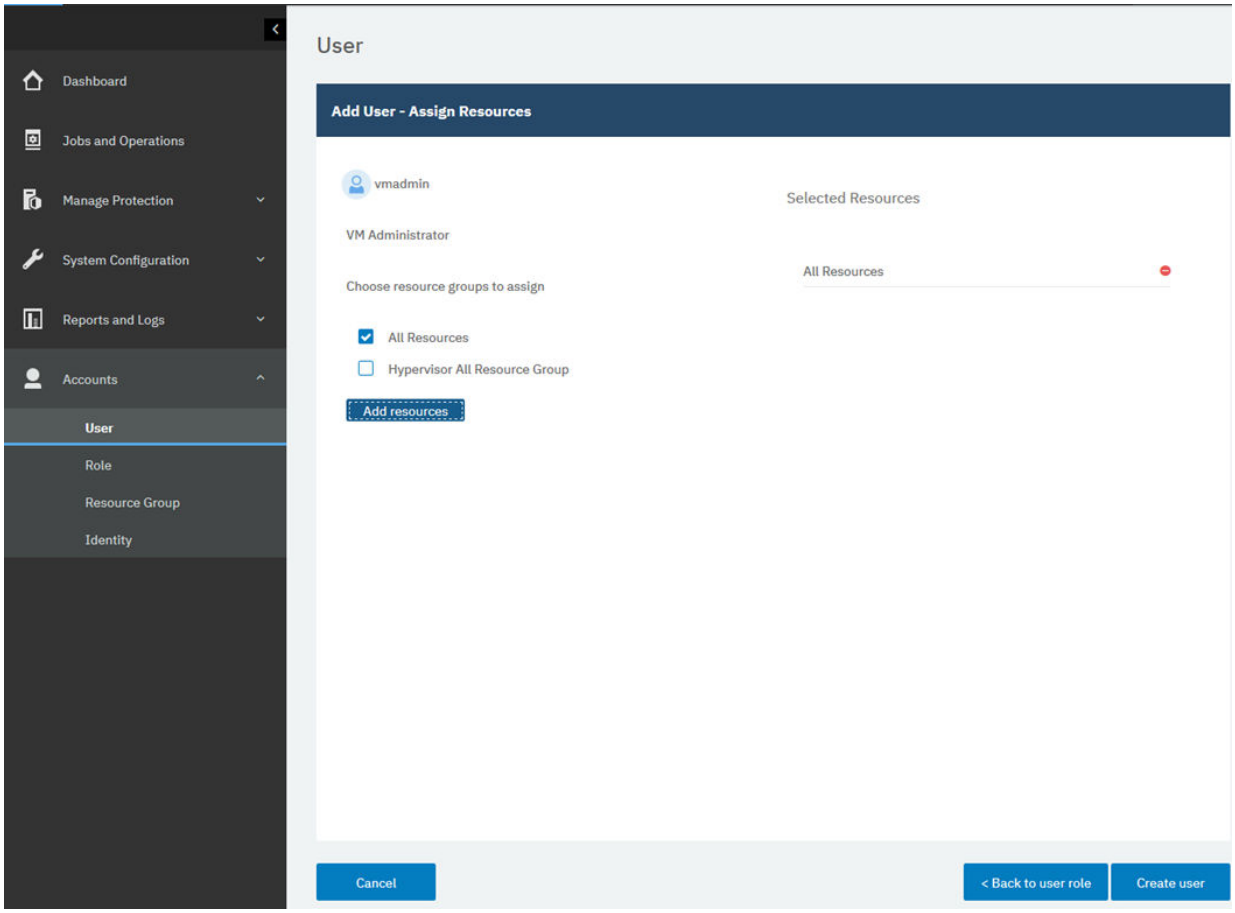


Figura 7. Selección de un grupo de recursos para la cuenta de usuario

8. Pulse **Crear usuario**.

Conceptos relacionados

"Gestión del acceso de usuarios" en la página 303
Al utilizar el control de acceso basado en roles, puede establecer los recursos y permisos disponibles en las cuentas de usuario de IBM Spectrum Protect Plus.

Añadir recursos para proteger

Los recursos son servidores de hipervisores o aplicaciones que alojan los datos que desea proteger. Después de registrar un recurso, se captura un inventario del recurso y se añade al inventario de IBM Spectrum Protect Plus, lo cual permite completar los trabajos de copia de seguridad y restauración, así como ejecutar informes.

Acerca de esta tarea

Por ejemplo, en esta tarea se describe cómo añadir un recurso VMware. Para añadir otros recursos, consulte las instrucciones por el tipo de recurso en Capítulo 7, "Protección de hipervisores", en la página 99 y Capítulo 8, "Protección de aplicaciones", en la página 141.

Procedimiento

Para añadir una instancia de vCenter Server, complete los pasos siguientes:

1. En el panel de navegación, pulse **Gestionar protección** > **Hipervisores** > **VMware**.
2. Pulse **Gestionar vCenter** y, a continuación, pulse **Añadir vCenter**.
3. Cumplimente los campos en la sección **Propiedades de vCenter**:

Nombre de host/IP
Especifique la dirección IP que se pueda resolver o una vía de acceso y un nombre de máquina que se puedan resolver.

Utilizar usuario existente
Habilite esta opción para seleccionar un nombre de usuario y una contraseña especificados anteriormente para la instancia de vCenter Server.

Nombre de usuario
Escriba el nombre de usuario para la instancia de vCenter Server.

Contraseña
Escriba la contraseña para la instancia de vCenter Server.

Puerto
Escriba el puerto de comunicaciones de la instancia de vCenter Server. Seleccione el recuadro **Utilizar SSL** para habilitar una conexión Secure Sockets Layer (SSL) cifrada. El puerto predeterminado típico es 80 para las conexiones no SSL o 443 para las conexiones SSL.

4. En la sección **Opciones**, configure la opción siguiente:

Número máximo de MV para procesar simultáneamente para cada servidor ESX y cada SLA
Establezca el número máximo de instantáneas de máquina virtual simultáneas para procesar en el servidor ESX.

En el ejemplo siguiente se muestran los campos cumplimentados.

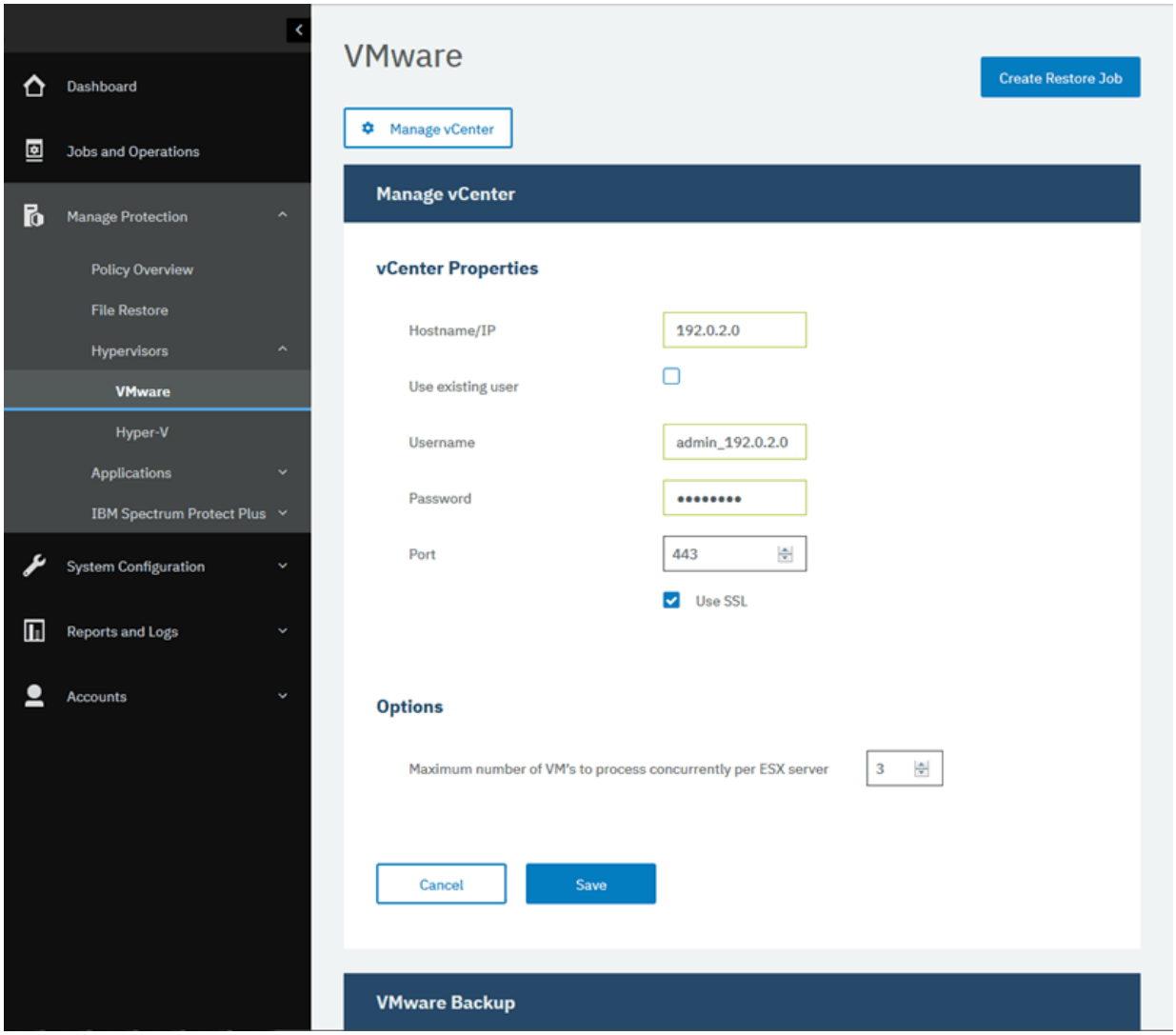


Figura 8. Adición de una instancia de vCenter Server

5. Pulse **Guardar**.

   IBM Spectrum Protect Plus confirma una conexión de red, añade el recurso a la base de datos y, a continuación, cataloga el recurso. Si aparece un mensaje que indica que la conexión no se ha realizado correctamente, revise las entradas. Si las entradas son correctas y la conexión no se ha realizado correctamente, póngase en contacto con un administrador de red para verificar y arreglar las conexiones.

Añadir recursos a una definición de trabajo

Para poder realizar una copia de seguridad de un recurso, debe crear una definición de trabajo que asocie el recurso a una o más políticas de copia de seguridad, también denominadas políticas de SLA.

Acerca de esta tarea

Por ejemplo, en esta tarea se describe cómo se selecciona una política de SLA para los recursos que están en un vCenter de VMware. Para seleccionar una política para otros recursos, consulte las instrucciones por el tipo de recurso en Capítulo 7, “Protección de hipervisores”, en la página 99 y Capítulo 8, “Protección de aplicaciones”, en la página 141.

Procedimiento

Para seleccionar una política de SLA, complete los pasos siguientes:

1. En el panel de navegación, pulse **Gestionar protección** > **Hipervisores** > **VMware**.
2. Seleccione los recursos cuya copia de seguridad desea realizar. Puede seleccionar todos los recursos de un vCenter o bien detallar más para seleccionar recursos específicos.

   Utilice la función de búsqueda para buscar los recursos disponibles y alternar entre los recursos visualizados utilizando el filtro **Ver**. Las opciones disponibles son **MV y plantillas**, **Máquinas virtuales**, **Almacén de datos**, **Etiquetas y categorías** y **Hosts y clústeres**. Las etiquetas, que se aplican en vSphere, hacen posible que se asignen metadatos a las máquinas virtuales.

   El ejemplo siguiente muestra un disco duro específico seleccionado para la copia de seguridad:

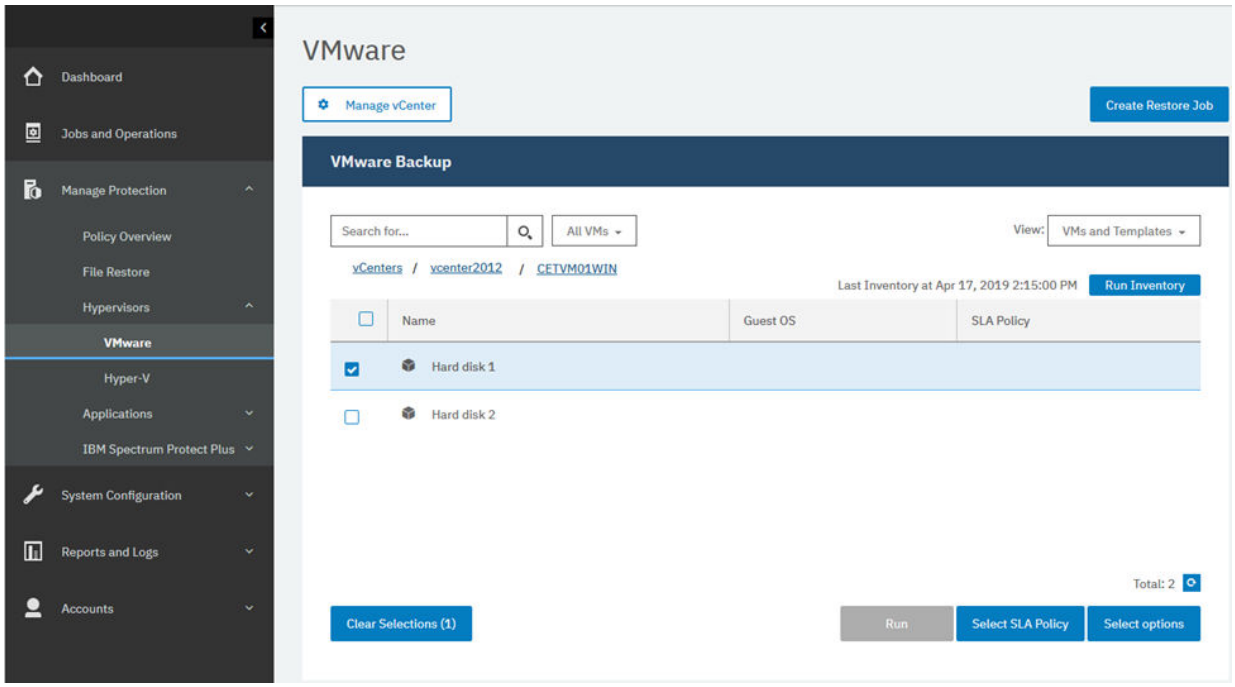


Figura 9. Selección de recursos para copia de seguridad

3. Pulse **Seleccionar política de SLA** para añadir a la definición de trabajo una o más políticas de SLA que cumplen los criterios de datos de copia de seguridad.

   En el ejemplo siguiente se muestra la política de SLA **Cobre** seleccionada:

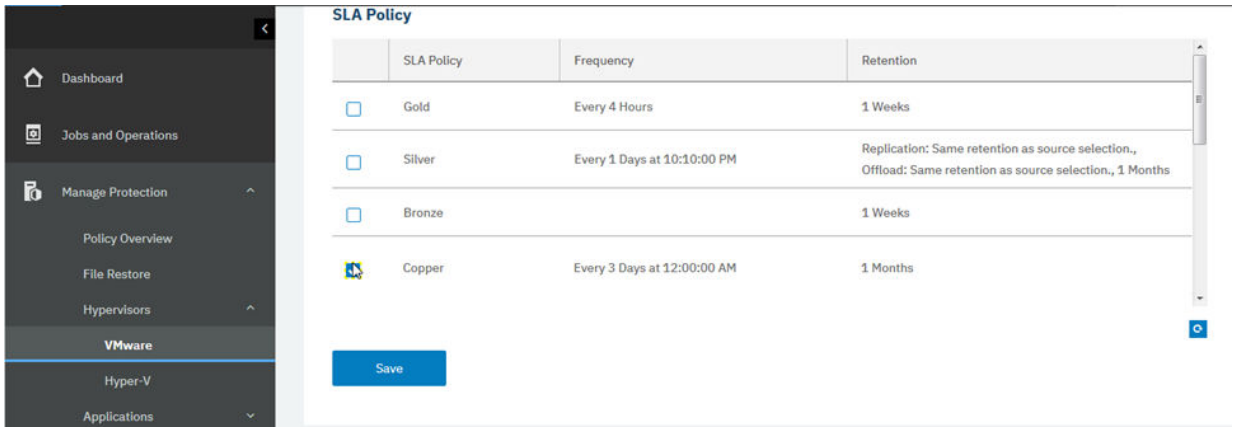


Figura 10. Selección de una política de SLA

4. Para crear la definición de trabajo utilizando las opciones predeterminadas, pulse **Guardar**.
5. Opcional: Para configurar opciones adicionales, pulse **Seleccionar opciones** y siga las instrucciones que se indican en "Copia de seguridad de datos de VMware" en la página 107.
6. Pulse **Guardar**.

Después de guardar la definición de trabajo, se descubren los discos de máquina virtual (VMDK) disponibles en una máquina virtual y se muestran cuando se selecciona **MV y plantillas** en el filtro **Ver**. De forma predeterminada, estos VMDK se asignan a la misma política de SLA que la máquina virtual. De forma opcional, para definir una política más granular excluyendo los VMDK individuales, siga las instrucciones que se indican en "Exclusión de VMDK de la política de SLA para un trabajo" en la página 111.

Resultados

El trabajo se ejecuta según lo definido en las políticas de SLA que ha seleccionado, o bien puede ejecutar manualmente el trabajo pulsando **Trabajos y operaciones** y, a continuación, pulsando la pestaña **Política y lista de trabajos**. Para obtener instrucciones, consulte "Iniciar un trabajo de copia de seguridad" en la página 84.

Conceptos relacionados

"Protección de IBM Spectrum Protect Plus" en la página 253

Proteja la aplicación de IBM Spectrum Protect Plus realizando una copia de seguridad de las bases de datos subyacentes para los escenarios de recuperación ante desastre. Se realiza una copia de seguridad de los valores de configuración, los recursos registrados, los puntos de restauración, los valores de almacenamiento de copia de seguridad, los datos de búsqueda y la información de trabajo en un servidor vSnap definido en la política de SLA asociada.

Iniciar un trabajo de copia de seguridad

Puede iniciar un trabajo de copia de seguridad bajo demanda fuera de la planificación establecida por la política de SLA.

Procedimiento

Para iniciar un trabajo de copia de seguridad bajo demanda, complete los pasos siguientes:

1. En la navegación, pulse **Trabajos y operaciones** y, a continuación, abra la pestaña **Planificación**.

   Si el trabajo no es un trabajo planificado, sino un trabajo bajo demanda, pulse la pestaña **Historial de trabajos**.
2. Elija el trabajo que desea ejecutar y pulse **Acciones** > **Iniciar** tal como se muestra en el ejemplo siguiente:

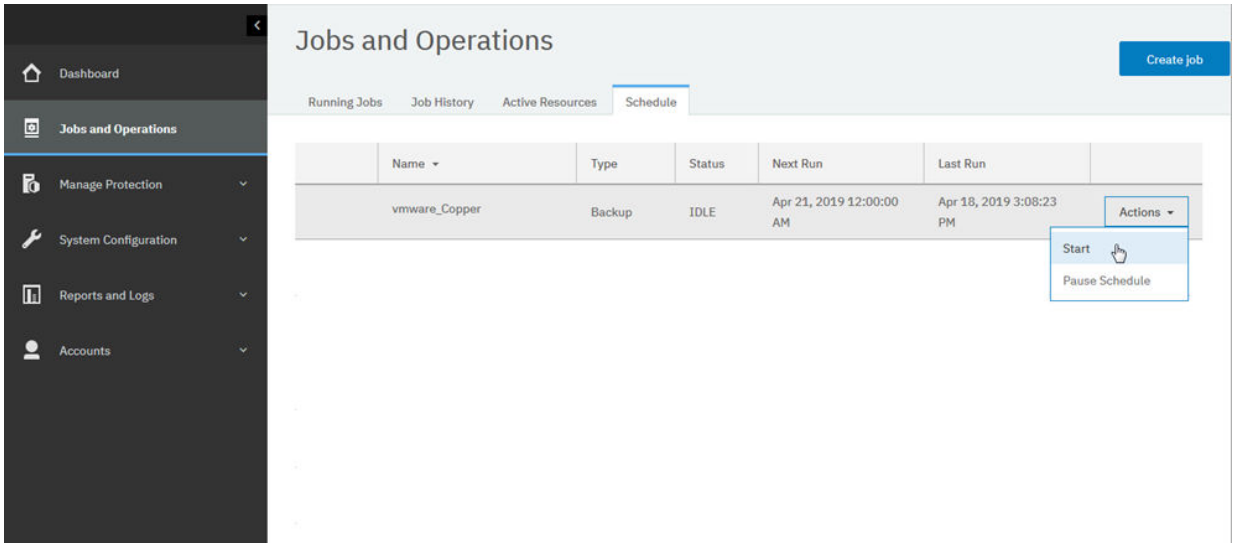


Figura 11. Inicio de un trabajo

3. Para ver el registro de trabajo en detalle, pulse el trabajo en la pestaña **Trabajos en ejecución**.

   La pantalla de registro muestra los siguientes detalles:

- Estado: muestra si el mensaje es un mensaje de error, aviso o información.
- Hora: muestra la indicación de fecha y hora del mensaje.
- ID: muestra el identificador exclusivo del mensaje, si es aplicable.
- Descripción: muestra cuál es el mensaje.

4. Puede descargar un registro de trabajo de la página pulsando **Descargar .zip**. Si desea cancelar el trabajo, pulse **Acciones** > **Cancelar**.
5. Pulse el menú **Acciones** que está asociado al trabajo que desea iniciar y pulse **Iniciar**, tal como se muestra en el ejemplo siguiente:

Conceptos relacionados

"Trabajos y operaciones" en la página 257
Utilice la ventana **Trabajos y operaciones** para supervisar trabajos, revisar el historial de trabajos, planificar trabajos, ver los recursos activos y volver a ejecutar o poner en pausa los trabajos y las planificaciones.

Ejecutar un informe

Ejecute informes con parámetros predefinidos personalizados o predeterminados.

Procedimiento

Para ejecutar un informe, lleve a cabo los pasos siguientes:

1. En el panel de navegación, pulse **Informes y registros** > **Informes**.
2. Expanda un tipo de informe y seleccione uno para ejecutarlo tal como se muestra en el ejemplo siguiente:

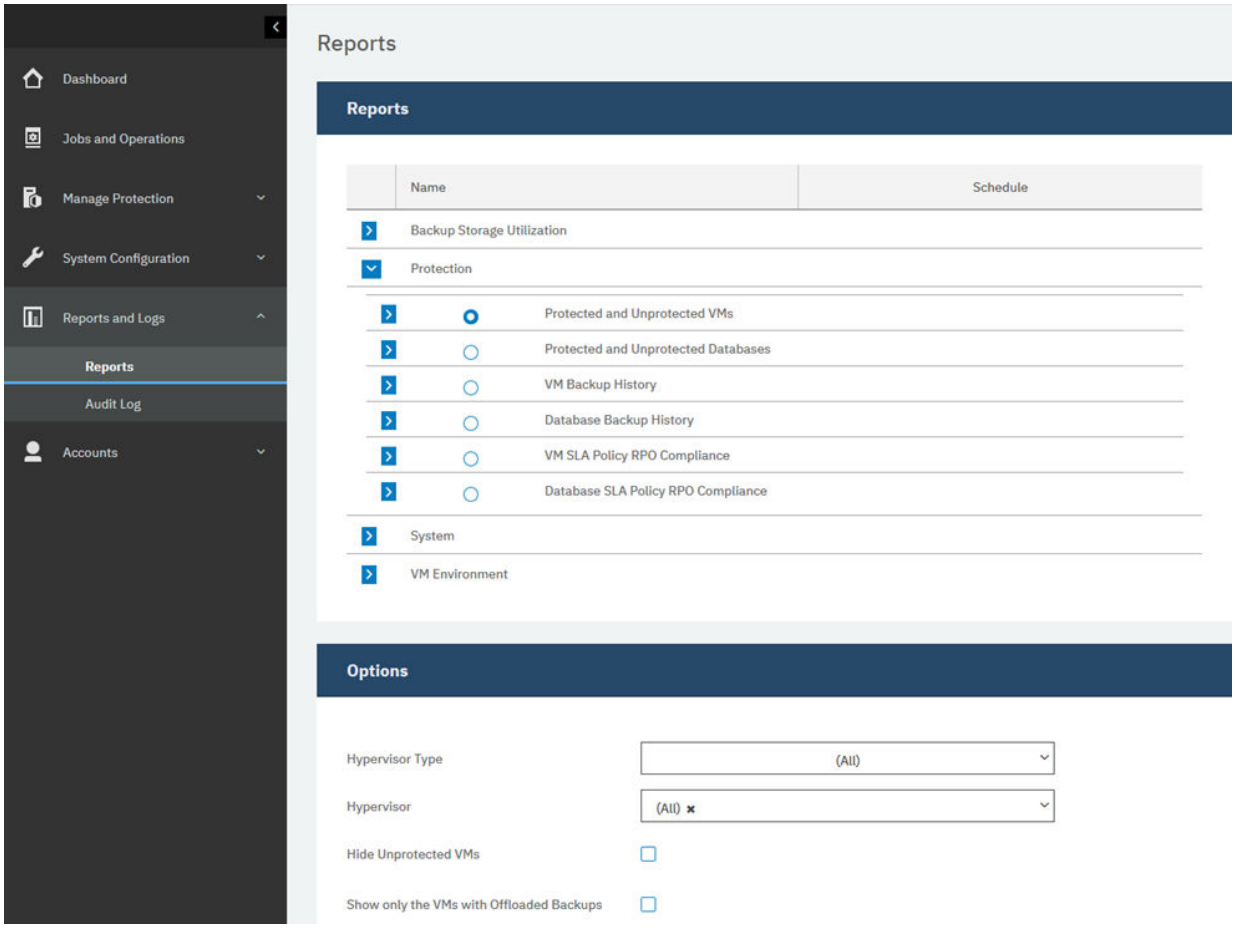


Figura 12. Selección de un informe para ejecutar

3. Ejecute el informe con parámetros personalizados o parámetros predeterminados:
   - Para ejecutar el informe con parámetros personalizados, establezca los parámetros en la sección **Opciones** y pulse **Ejecutar**. Los parámetros son exclusivos de cada informe.
   - Para ejecutar el informe con parámetros predeterminados, pulse **Ejecutar**.

Conceptos relacionados

“Gestión de informes y registros” en la página 295

IBM Spectrum Protect Plus proporciona un número de informes predefinidos que puede personalizar para cumplir los requisitos de creación de informes. También se proporciona un registro de las acciones que los usuarios completan en IBM Spectrum Protect Plus.

Capítulo 5. Actualización de componentes de IBM Spectrum Protect Plus

Puede actualizar el dispositivo virtual de IBM Spectrum Protect Plus os servidores vSnap y los servidores proxy VADP para obtener las últimas características y mejoras. Los parches de software y las actualizaciones se instalan utilizando la consola administrativa de IBM Spectrum Protect Plus o la interfaz de línea de mandatos para estos componentes.

Para obtener información sobre los archivos de actualización disponibles y sobre cómo obtenerlos desde un sitio de descargas de IBM, consulte Nota técnica 879861.

Antes de actualizar los componentes de IBM Spectrum Protect Plus, revise los requisitos de hardware y software de los componentes para confirmar los cambios que se hayan producido en las versiones anteriores.

Revise las restricciones y sugerencias siguientes:

- Debe actualizar por separado los servidores vSnap que no están en los dispositivos virtuales de IBM Spectrum Protect Plus.
- El proceso de actualización a través de la consola de administración actualiza las características de IBM Spectrum Protect Plus y los componentes de infraestructura subyacentes, incluidos el sistema operativo y el sistema de archivos. No utilice otro método para actualizar estos componentes.
- No actualice ninguno de los componentes subyacentes de IBM Spectrum Protect Plus a menos que el componente se proporcione en un paquete de actualización de IBM Spectrum Protect Plus. Las actualizaciones de infraestructura están gestionadas por las instalaciones de actualización de IBM. La consola administrativa es el medio principal para actualizar las características de IBM Spectrum Protect Plus los componentes de infraestructura subyacentes, incluidos el sistema operativo y el sistema de archivos.

Realice las acciones siguientes:

- Antes de actualizar componentes, es importante que realice una copia de seguridad del entorno de IBM Spectrum Protect Plus según lo descrito en “Copia de seguridad de la aplicación de IBM Spectrum Protect Plus ” en la página 253.
- Después de que se actualice IBM Spectrum Protect Plus, no puede retrotraer a una versión anterior sin una instantánea de máquina virtual. Cree una instantánea de máquina virtual del entorno antes de actualizar IBM Spectrum Protect Plus. Si más adelante desea retrotraer IBM Spectrum Protect Plus a una versión anterior, debe tener una instantánea de máquina virtual. Después de que la actualización se haya completado correctamente, elimine la instantánea de la máquina virtual.

Actualización del dispositivo virtual de IBM Spectrum Protect Plus

Utilice la consola de administración de IBM Spectrum Protect Plus para actualizar el dispositivo virtual. La actualización de IBM Spectrum Protect Plus puede ejecutarse fuera de línea, o en línea si tiene acceso a Internet externo.

Antes de empezar

Puede actualizar IBM Spectrum Protect Plus V10.1.2 o posterior directamente a la versión actual. Si utiliza la versión V10.1.1, debe actualizarla a la versión V10.1.2 y, a continuación, actualizarla a la versión actual. Para obtener instrucciones sobre cómo actualizar de V10.1.1 a V10.1.2, consulte Actualización del dispositivo virtual de IBM Spectrum Protect Plus a la versión 10.1.2.

Antes de empezar el proceso de actualización, complete los pasos siguientes:

1. Asegúrese de realizar una copia de seguridad del entorno de IBM Spectrum Protect Plus antes de ejecutar las actualizaciones. Para obtener más información sobre cómo realizar una copia de

seguridad del entorno, consulte “Copia de seguridad de la aplicación de IBM Spectrum Protect Plus ” en la página 253.

2. Para las actualizaciones fuera de línea, descargue la actualización de IBM Spectrum Protect Plus previa necesaria denominada `CC1QHML.iso` en un directorio del sistema en el que se ejecute el navegador de la consola de administración. El archivo de actualización se instalará en primer lugar.
3. Asegúrese de que no hay ningún trabajo en ejecución durante el procedimiento de actualización. Ponga en pausa la planificación de cualquier trabajo que tenga un estado DESOCUPADO o COMPLETADO.

Para obtener una lista de las imágenes de descarga, incluida la actualización del sistema operativo necesaria para el dispositivo virtual, consulte Nota técnica 879861.

Acerca de esta tarea

Si tiene acceso a Internet, puede elegir ejecutar el procedimiento de actualización en línea. Si no tiene acceso a Internet, puede ejecutar el procedimiento de actualización fuera de línea.

Procedimiento

Para actualizar el dispositivo virtual de IBM Spectrum Protect Plus, complete los pasos siguientes:

1. Desde un navegador web soportado, acceda a la consola de administración especificando la siguiente dirección:

   ```
   https://hostname:8090/
   ```

   donde *hostname* es la dirección IP de la máquina virtual en la que se despliega la aplicación.
2. En la ventana de inicio de sesión, seleccione uno de los tipos de autenticación siguientes en la lista **Tipo de autenticación**:

Tipo de autentificación	Información de inicio de sesión
IBM Spectrum Protect Plus	Para iniciar la sesión como un usuario de IBM Spectrum Protect Plus con privilegios SYSADMIN, especifique el nombre de usuario y la contraseña del administrador. Si inicia la sesión utilizando la cuenta de usuario `admin`, se le solicita que restablezca el nombre de usuario y la contraseña. No puede restablecer el nombre de usuario a `admin`, `root` o `test`.
Sistema (recomendado)	Para iniciar una sesión como un usuario del sistema, escriba la contraseña de administrador del servidor. La contraseña predeterminada es `sppDP758`. Se le solicitará que cambie esta contraseña durante el primer inicio de sesión.

3. Pulse **Gestión de revisiones y actualizaciones** para abrir la página de gestión de actualizaciones.

   Si tiene acceso al sitio FTP public.dhe.ibm.com, la consola de administrador comprueba automáticamente si hay actualizaciones disponibles y las muestra.
4. Pulse **Ejecutar actualización** para instalar las actualizaciones disponibles.
   - Si las actualizaciones se instalan correctamente, vaya al paso 6.
   - Si tiene previsto instalar una actualización desde un archivo ISO, seleccione **Pulse aquí** para ejecutar las actualizaciones fuera de línea.Vaya al paso 5.

   Nota: Si desea ejecutar las actualizaciones en línea pero solo puede ver la modalidad fuera de línea, compruebe la conectividad a Internet e intente de nuevo acceder al sitio FTP public.dhe.ibm.com.
5. Seleccione la actualización que desee ejecutar de la siguiente manera:

- Modalidad en línea: las actualizaciones se listan automáticamente en el repositorio cuanto están disponibles. Pulse **Ejecutar actualización**.
- Modalidad fuera de línea: pulse **Elegir archivo** para buscar el archivo descargado. El archivo tiene una extensión `iso` o `rpm` como en este ejemplo: `<nombre_archivo>.iso`. Pulse **Cargar la imagen de actualización (o revisión)**.

  Nota: Solo puede seleccionar un archivo de actualización cada vez.

Cuando se complete la actualización, la máquina virtual en la que se despliega la aplicación se reiniciará automáticamente.

Importante: Una vez completada la actualización de IBM Spectrum Protect Plus, debe actualizar los servidores vSnap y VDAP externos en el entorno.

6. Borre la memoria caché de navegador.

   El contenido HTML de las versiones anteriores de IBM Spectrum Protect Plus podría estar almacenado en la memoria caché.
7. Inicie la versión actualizada de IBM Spectrum Protect Plus.
8. En el panel de navegación, pulse **Trabajos y operaciones**y, a continuación, pulse la pestaña **Planificación** .

   Encuentre los trabajos que ha puesto en pausa.
9. En el menú **Acciones** para los trabajos en pausa, seleccione **Liberar planificación**.

Tareas relacionadas

“Actualización de servidores vSnap” en la página 89
El servidor vSnap predeterminado se actualiza con el dispositivo de IBM Spectrum Protect Plus. Debe actualizar los servidores vSnap adicionales que están instalados por separado en dispositivos virtuales o físicos.

Actualización de servidores vSnap

El servidor vSnap predeterminado se actualiza con el dispositivo de IBM Spectrum Protect Plus. Debe actualizar los servidores vSnap adicionales que están instalados por separado en dispositivos virtuales o físicos.

Antes de empezar

Puede actualizar los servidores vSnap directamente desde la versión 10.1.2 o posterior a la versión actual. Si utiliza la versión 10.1.1, debe actualizar a la versión 10.1.2 y, a continuación, actualizar a la versión actual. Para obtener instrucciones sobre cómo actualizar a la versión 10.1.2, consulte Actualización de servidores vSnap a la versión 10.1.2.

Los trabajos de restauración de prueba deben finalizar para poder iniciar una actualización en vSnap. Los trabajos que no hayan finalizado o no se hayan cancelado al iniciar una actualización no estarán visibles cuando finalice la actualización. Si no hay trabajos visibles cuando finalice la actualización, vuelva a ejecutar los trabajos de restauración de prueba.

Es posible que también se le solicite actualizar el sistema operativo de los servidores vSnap antes de actualizar los servidores. Para conocer los requisitos del sistema operativo, consulte “Requisitos de los componentes ” en la página 13.

Para comprobar la versión actual y el sistema operativo de los servidores vSnap, complete los pasos siguientes:

1. Inicie la sesión en el servidor vSnap como el usuario `serveradmin`. Si utiliza IBM Spectrum Protect Plus 10.1.1, inicie la sesión utilizando la cuenta raíz.

2. Para comprobar la versión y el sistema operativo del servidor vSnap, utilice la interfaz de línea de mandatos de vSnap para emitir el mandato siguiente:

```
vsnap system info
```

Asegúrese de que no se están ejecutando trabajos que utilicen el servidor vSnap durante el procedimiento de actualización. Ponga en pausa la planificación de cualquier trabajo que tenga un estado DESOCUPADO o COMPLETADO.

Actualización del sistema operativo para un servidor vSnap físico

Si ha instalado el servidor vSnap en una máquina que está ejecutando Red Hat Enterprise Linux, debe actualizar el sistema operativo a la versión 7.5 o 7.6 antes de actualizar el servidor vSnap. Para obtener instrucciones sobre cómo actualizar el sistema operativo, consulte la documentación de Red Hat Enterprise Linux.

Tareas relacionadas

"Actualización de un servidor vSnap" en la página 90

El servidor vSnap predeterminado se actualiza con el dispositivo de IBM Spectrum Protect Plus. Debe actualizar los servidores vSnap adicionales que están instalados por separado en dispositivos virtuales o físicos.

Actualización del sistema operativo para un servidor vSnap virtual

Si el sistema operativo es CentOS Linux versión 7.4 o una versión anterior, debe actualizar el sistema operativo antes de actualizar el servidor vSnap. Para actualizar el sistema operativo, siga las instrucciones que se indican en Actualización de servidores vSnap a la versión 10.1.2. La instalación de la versión 10.1.2 incluye CentOS Linux versión 7.5.

Tareas relacionadas

"Actualización de un servidor vSnap" en la página 90

El servidor vSnap predeterminado se actualiza con el dispositivo de IBM Spectrum Protect Plus. Debe actualizar los servidores vSnap adicionales que están instalados por separado en dispositivos virtuales o físicos.

Actualización de un servidor vSnap

El servidor vSnap predeterminado se actualiza con el dispositivo de IBM Spectrum Protect Plus. Debe actualizar los servidores vSnap adicionales que están instalados por separado en dispositivos virtuales o físicos.

Antes de empezar

Antes de empezar el proceso de actualización, complete los pasos siguientes:

1. Asegúrese de que ha realizado una copia de seguridad del entorno de IBM Spectrum Protect Plus tal como se describe en "Copia de seguridad de la aplicación de IBM Spectrum Protect Plus " en la página 253.
2. Si está actualizando desde IBM Spectrum Protect Plus 10.1.1, debe actualizar a la versión 10.1.2 y, a continuación, actualizar a la versión actual. Para obtener instrucciones sobre cómo actualizar a la versión 10.1.2, consulte Actualización de servidores vSnap a la versión 10.1.2.
3. Descargue el archivo de actualización de vSnap `CC1QGML.run` y cópielo en una ubicación temporal en el servidor vSnap. Para obtener información sobre la descarga de archivos, consulte Nota técnica 879861.

Procedimiento

Para actualizar un servidor vSnap, complete los pasos siguientes:

1. Inicie la sesión en el servidor vSnap como el usuario **serveradmin**.

2. En el directorio donde se encuentra el archivo `CC1QGML.run`, realice el ejecutable del archivo y ejecute el instalador emitiendo los mandatos siguientes:

```
chmod +x CC1QGML.run
```

```
sudo ./CC1QGML.run
```

   Se instalan los paquetes de vSnap.
3. Inicie la versión actualizada de IBM Spectrum Protect Plus.
4. En el panel de navegación, pulse **Trabajos y operaciones**y, a continuación, pulse la pestaña **Planificación** .

   Encuentre los trabajos que ha puesto en pausa.
5. En el menú **Acciones** para los trabajos en pausa, seleccione **Liberar planificación**.

Actualización de proxies VADP

La actualización del dispositivo virtual de IBM Spectrum Protect Plus actualiza automáticamente todos los proxies VADP asociados al dispositivo virtual. En casos excepcionales, como por ejemplo, la pérdida de conectividad de red, debe actualizar manualmente el proxy VADP.

Antes de empezar

Antes de empezar, asegúrese de que ha realizado una copia de seguridad del entorno de IBM Spectrum Protect Plus tal como se describe en "Copia de seguridad de la aplicación de IBM Spectrum Protect Plus " en la página 253.

Procedimiento

Si hay disponible una actualización de proxy VADP para proxies externos durante un reinicio del dispositivo virtual de IBM Spectrum Protect Plus, la actualización se aplicará automáticamente a cualquier proxy VADP asociado con una identidad. Para asociar un proxy VADP a una identidad, vaya a **Configuración del sistema** > **Proxy VADP**. Pulse el icono de opciones ••• y seleccione **Establecer opciones**. Mediante el valor de usuario, seleccione un nombre de usuario y una contraseña especificados anteriormente para el servidor proxy VADP.

Para actualizar manualmente un proxy VADP, complete los pasos siguientes:

1. Vaya a página **Configuración del sistema** > **Proxy VADP** en IBM Spectrum Protect Plus.
2. La página **Proxy VADP** muestra cada servidor proxy. Si hay disponible una versión más reciente del software proxy VADP, se muestra un icono en el campo **Estado**.
3. Asegúrese de que no haya ningún trabajo activo que utilice el proxy y, a continuación, pulse el icono de actualizar .

   El servidor proxy accede a un estado suspendido e instala la actualización más reciente. Cuando la actualización se completa, el servidor proxy se reanuda automáticamente y accede a un estado habilitado.

Si intenta actualizarse como un usuario no root, deberá seguir instrucciones especiales para poder enviar-instalar o enviar-actualizar un proxy VADP.

1. Cree un archivo en el directorio /etc/sudoers.d/.

```
sudo cd /etc/sudoers.d/
```

2. Grabe el texto en el archivo y guárdelo pulsando CTRL+D en el teclado cuando haya terminado.

```
sudo cat > 99-vadpuser
     Defaults !requiretty
```

```
     vadpuser ALL=NOPASSWD: /tmp/cdm_guestapps_vadpuser/runcommand.sh
<<Press CTRL+D>>
```

3. Establezca los permisos adecuados en el archivo.

```
sudo chmod 0440 99-vadpuser
```

Qué hacer a continuación

Después de actualizar los proxies VADP, realice la acción siguiente:

Acción	Cómo
Ejecute el trabajo de copia de seguridad de VMware.	Consulte “Copia de seguridad de datos de VMware” en la página 107. Los proxies se indican en el registro de trabajo con un mensaje de registro similar al texto siguiente: `Run remote vmdkbackup of MicroService: http://<proxy` *`nombrenodo`*`, IP:`*`dirección_IP_proxy`*

Tareas relacionadas

“Creación de proxies VADP” en la página 113
Puede crear proxies VADP para ejecutar trabajos de copia de seguridad de VMware con IBM Spectrum Protect Plus en entornos de Linux.

Referencia relacionada

“Edición de puertos de cortafuegos” en la página 54
Utilice los ejemplos proporcionados como referencia para abrir puertos de cortafuegos en servidores de aplicaciones o servidores proxy VADP remotos. Debe restringir el tráfico del puerto solo a la red o los adaptadores necesarios.

Aplicación de actualizaciones de disponibilidad anticipada

Las actualizaciones de disponibilidad anticipada proporcionan arreglos para los informes autorizados de análisis de programa (APAR) y problemas menores entre los releases de IBM Spectrum Protect Plus. Estas actualizaciones están disponibles para paquetes en el sitio web de Fix Central Online.

Acerca de esta tarea

Es posible que las actualizaciones de disponibilidad anticipada no contengan arreglos para todos los componentes de IBM Spectrum Protect Plus.

Para obtener instrucciones sobre cómo obtener e instalar arreglos temporales, consulte la información de descarga que se publica cuando los arreglos están disponibles.

Capítulo 6. Gestión de políticas de SLA para operaciones de copia de seguridad

Las políticas de acuerdo de nivel de servicio (SLA), también denominadas políticas de copia de seguridad, definen parámetros para los trabajos de copia de seguridad. Estos parámetros incluyen la frecuencia y el periodo de retención de las copias de seguridad, y la opción de replicar o descargar los datos de la copia de seguridad. Puede utilizar políticas de SLA predefinidas o personalizarlas según sus necesidades.

Están disponibles las siguientes políticas de SLA predeterminadas. Cada política especifica un periodo de frecuencia y de retención para la copia de seguridad. Puede utilizar estas políticas tal como son o modificarlas. También puede crear políticas de SLA personalizadas.

Oro
Esta política se ejecuta cada 4 horas con un período de retención de 1 semana.

Plata
Esta política se ejecuta diariamente con un periodo de retención de 1 mes.

Bronce
Esta política se ejecuta diariamente con un período de retención de 1 semana.

Para ver y gestionar políticas de copia de seguridad y para supervisar las máquinas virtuales y las bases de datos que están protegidas por políticas, pulse **Gestionar protección** > **Descripción general de política** en el panel de navegación.

Si edita una política de SLA existente cambiando el origen de descarga de la nube, el tipo de destino de descarga o las opciones del servidor de descarga de destino, los trabajos asociados iniciarán una copia de seguridad base completa, no una copia de seguridad incremental, durante la siguiente ejecución del trabajo.

Para las instalaciones de IBM Spectrum Protect Plus V10.1.4, hay disponible una configuración de demostración de SLA para la realización de pruebas. Esta función de demostración incluye los siguientes elementos:

- Un sitio de demostración denominado **Demo**
- Una política de SLA denominada **Demo**
- Una configuración de vSnap local para el SLA de demostración.

Puede optar por utilizar el sitio de demostración para la realización de pruebas de operaciones de copia de seguridad y restauración. Se realiza una copia de seguridad de los datos en la configuración de vSnap local cuando ejecuta la política de SLA de demostración.

Nota: El vSnap incorporado se establece de forma que solo lo puede utilizar el sitio Demo. No utilice el vSnap de IBM Spectrum Protect Plus incorporado con otro sitio.

Creación de una política de SLA

Puede crear políticas de SLA personalizadas para definir políticas de frecuencia de copia de seguridad, retención, duplicación y descarga que sean específicas del entorno.

Acerca de esta tarea

Si una máquina virtual está asociada a varias políticas de SLA, asegúrese de que no planifica las políticas que ha creado para que se ejecuten simultáneamente. Planifíquelas para que se ejecuten con un periodo de tiempo suficiente entre ellas, o bien combínelas en una única política de SLA.

Si se inicia una tarea de réplica de instantánea antes de que se complete una copia de seguridad inicial en un servidor vSnap, los errores del registro de trabajo indican que no existen puntos de recuperación para

la base de datos. Una vez completada la copia de seguridad inicial en el servidor vSnap, vuelva a ejecutar la tarea de réplica para replicar las instantáneas tal como están configuradas en la política de SLA.

Procedimiento

Para crear una política de SLA, complete los pasos siguientes:

1. En el panel de navegación, pulse **Gestionar protección** > **Descripción general de política**.
2. Pulse **Añadir política de SLA**.

   Se muestra el panel **Nueva política de SLA**.
3. En el campo **Nombre**, escriba un nombre que ofrezca una descripción importante de la política de SLA.
4. En la sección **Protección operativa** en **Política principal**, establezca las opciones siguientes para las operaciones de copia de seguridad. Estas operaciones ocurren en los servidores vSnap que se definen en la ventana **Configuración del sistema** > **Almacenamiento de copias de seguridad** > **Disco**.

   Retención
   Especifique el periodo de retención de las instantáneas de copia de seguridad.

   Deshabilitar planificación
   Marque este recuadro de selección si desea crear la política principal sin definir una frecuencia o una hora de inicio. Las políticas creadas sin una planificación se pueden ejecutar bajo demanda.

   Frecuencia
   Escriba una frecuencia para las operaciones de copia de seguridad.

   Hora de inicio
   Escriba la fecha y hora deseadas para la operación de copia de seguridad.

   Sitio de destino
   Seleccione el sitio de copia de seguridad de destino para realizar la copia de seguridad de los datos.

   Un sitio puede contener uno o más servidores vSnap. Si hay más de un servidor vSnap en un sitio, el servidor de IBM Spectrum Protect Plus gestiona la ubicación de datos en los servidores vSnap.

   En esta lista, solo se muestran los sitios que están asociados con un servidor vSnap. Los sitios que se añaden a IBM Spectrum Protect Plus pero no están asociados con un servidor vSnap no se muestran.

   Utilizar únicamente el almacenamiento de disco cifrado
   Marque este recuadro de selección para realizar una copia de seguridad de los datos en servidores de vSnap cifrados, si el entorno incluye una combinación de servidores cifrados y no cifrados.

   Restricción: Si se selecciona esta opción y no hay ningún servidor vSnap cifrado, el trabajo asociado no se ejecutará correctamente.
5. En **Política de réplica**, establezca las opciones siguientes para habilitar la réplica asíncrona de un servidor vSnap en otro. Por ejemplo, puede replicar los datos del sitio de copia de seguridad principal al sitio de copia de seguridad secundario.

   Requisito de réplicas de las asociaciones: Estas opciones solo se aplican a las asociaciones de réplica establecidas. Para añadir una asociación de réplica, vea las instrucciones de "Establecimiento de una asociación de réplica para un servidor vSnap" en la página 64.

   Réplica del almacenamiento de copias de seguridad
   Seleccione esta opción para habilitar la réplica.

   Deshabilitar planificación
   Marque este recuadro de selección para crear la relación de réplica sin definir una frecuencia o una hora de inicio.

   Frecuencia
   Escriba una frecuencia para las operaciones de réplica.

   Hora de inicio
   Escriba la fecha y la hora de inicio deseadas para la operación de réplica.

Sitio de destino
Seleccione el sitio de copia de seguridad de destino para replicar los datos.

Un sitio puede contener uno o más servidores vSnap. Si hay más de un servidor vSnap en un sitio, el servidor de IBM Spectrum Protect Plus gestiona la ubicación de datos en los servidores vSnap.

En esta lista, solo se muestran los sitios que están asociados con un servidor vSnap. Los sitios que se añaden a IBM Spectrum Protect Plus pero no están asociados con un servidor vSnap no se muestran.

Utilizar únicamente el almacenamiento de disco cifrado
Seleccione esta opción para replicar datos en servidores de vSnap cifrados, si el entorno incluye una combinación de servidores cifrados y no cifrados.

Restricción: Si se selecciona esta opción y no hay ningún servidor vSnap cifrado, el trabajo asociado no se ejecutará correctamente.

La misma retención que la selección de origen
Seleccione esta opción si desea utilizar la misma política de retención que el servidor vSnap de origen. Para establecer una política de retención distinta, deseleccione esta opción y establezca una política distinta.

6. En la sección **Protección adicional** , establezca las opciones siguientes en los datos de descarga y archivado.

Consejo: Cuando especifica Protección adicional, está eligiendo crear una copia.

Nube
Seleccione esta opción para descargar datos en un almacenamiento en la nube o en un servidor de repositorio.

Importante: Si pulsa **Protección adicional** > **Nube**, se crea una copia incremental de los datos en un sistema de almacenamiento en la nube o en un servidor IBM Spectrum Protect.

Se realiza una copia de seguridad de los datos en el servidor vSnap para la protección a corto plazo y, a continuación, se descargan en el almacenamiento en la nube o en un servidor de repositorio seleccionado para la protección a largo plazo. Durante la primera descarga de un volumen de copia de seguridad, se realiza una copia de seguridad de toda la instantánea. Una vez completada la primera descarga de la instantánea base, las descargas posteriores son incrementales y capturan los cambios acumulativos desde la última descarga. Las operaciones de restauración del servidor de nube o de repositorio se pueden realizar desde cualquier servidor vSnap disponible.

Deshabilitar planificación
Marque este recuadro de selección si desea crear la relación de descarga sin definir una frecuencia o una hora de inicio.

Frecuencia
Especifique una frecuencia para las operaciones de descarga.

Hora de inicio
Escriba la fecha y la hora de inicio deseadas para la operación de descarga.

La misma retención que la selección de origen
Seleccione esta opción si desea utilizar la misma política de retención para la copia de seguridad de descarga en la nube que el servidor vSnap de origen. Para establecer una política de retención distinta, deseleccione esta opción y establezca una política distinta.

Restricción: Las políticas de retención de descarga se inhabilitan si un servidor que utiliza la retención Grabar una vez leer varias (WORM) aparece seleccionado en el campo **Servidor de descarga de destino**.

Origen
Pulse el origen de la operación de descarga:

Destino de política principal
El origen de la operación de descarga es el sitio de destino definido en la sección **Política principal**.

Destino de política de réplica
El origen de la operación de descarga es el sitio de destino que aparece definido en la sección **Política de réplica**.

Esta opción solo está disponible cuando se selecciona **Réplica del almacenamiento de copias de seguridad**.

Destino
Pulse **Servidores de nube** o **Servidores de repositorio**.

Objetivo
Pulse el sistema de almacenamiento en la nube o el servidor de repositorio donde desea descargar los datos.

Esta lista contiene los sistemas de almacenamiento secundario que se han añadido a IBM Spectrum Protect Plus. Si no ha añadido almacenamiento secundario o desea añadirlo, consulte "Gestión del almacenamiento de copia de seguridad secundario" en la página 263 para obtener información sobre los sistemas de almacenamiento en la nube y los servidores de repositorio que están soportados, y cómo añadirlos a IBM Spectrum Protect Plus.

Archivado.
Seleccione esta opción para archivar datos en un almacenamiento en la nube o en un servidor de repositorio para la protección a largo plazo.

Importante: Si pulsa **Protección adicional** > **Archivado**, se crea una copia completa de los datos en un sistema de almacenamiento en la nube o en cinta utilizando un servidor IBM Spectrum Protect.

Esta operación proporciona una descarga de imagen completa en el almacenamiento de archivos seleccionado.

Deshabilitar planificación
Marque este recuadro de selección para crear la relación de archivado sin definir una frecuencia u hora de inicio.

Frecuencia
Especifique una frecuencia para las operaciones de archivado.

Hora de inicio
Especifique la fecha y la hora en que desea que se inicie la operación de archivado.

Retención
Especifique el periodo de retención para las instantáneas de archivado como una unidad de tiempo en días, meses o años.

Origen
Pulse el origen para el destino de archivado:

Destino de política principal
El origen de la operación de archivado es el sitio de destino definido en la sección **Política principal**.

Destino de política de réplica
El origen de la operación de archivado es el sitio de destino que se define en la sección **Política de réplica** .

Esta opción solo está disponible cuando se selecciona **Réplica del almacenamiento de copias de seguridad**.

Destino
Pulse **Servidores de nube** o **Servidores de repositorio**.

Objetivo
Pulse el sistema de almacenamiento en la nube o el servidor de repositorio donde desea archivar los datos.

En esta lista, solo se muestran los destinos de nube que tienen un grupo de archivado definido. Para añadir un grupo de archivado para un sistema de almacenamiento en la nube, siga las instrucciones de "Gestión del almacenamiento en la nube" en la página 263.

7. Pulse **Guardar**. Ahora, la política de SLA se puede aplicar a las definiciones de trabajo de copia de seguridad.

Qué hacer a continuación

Después de crear una política de SLA, realice las acciones siguientes:

Acción	Cómo
Asigne permisos de usuario a la política de SLA.	Consulte "Creación de un rol" en la página 308
Cree una definición de trabajo de copia de seguridad que utilice la política de SLA.	Consulte los temas de copia de seguridad que se indican en Capítulo 7, "Protección de hipervisores", en la página 99 y Capítulo 8, "Protección de aplicaciones", en la página 141.

Conceptos relacionados

"Replicar datos de almacenamiento de copia de seguridad " en la página 6
Cuando habilite la réplica de datos de copia de seguridad, los datos de un servidor vSnap se replican de forma asíncrona en otro servidor vSnap. Por ejemplo, puede replicar los datos de copia de seguridad de un servidor vSnap en un sitio primario en un servidor vSnap en un sitio secundario.

"Descargar en almacenamiento de copia de seguridad secundario" en la página 6
El servidor vSnap es la ubicación de copia de seguridad primaria para las instantáneas. Todos los entornos de IBM Spectrum Protect Plus tienen al menos un servidor vSnap. Opcionalmente, puede descargar instantáneas de un servidor vSnap en un almacenamiento de copias de seguridad secundario.

Edición de una política de SLA

Edite las opciones de una política de SLA para que refleje los cambios en el entorno de IBM Spectrum Protect Plus.

Procedimiento

Para editar una política de SLA, complete los pasos siguientes:

1. En el panel de navegación, pulse **Gestionar protección** > **Descripción general de política**.
2. Pulse el icono de edición que está asociado a una política.
   Se visualiza el panel **Editar política de SLA**.
3. Edite las opciones de política y, a continuación, pulse **Guardar**.

Supresión de una política de SLA

Suprima una política de SLA cuando está obsoleta.

Antes de empezar

Asegúrese de que no hay ningún trabajo que esté asociado a la política de SLA.

Procedimiento

Para suprimir una política de SLA, complete los pasos siguientes:

1. En el panel de navegación, pulse **Gestionar protección** > **Descripción general de política**.
2. Pulse el icono de suprimir que está asociado a una política de SLA.

3. Pulse **Sí** para suprimir la política.
4. Si está suprimiendo la política de SLA de demostración, vaya a **Configuración del sistema** > **Sitio** y suprima el sitio denominado Demo.

   Nota:

   Cuando suprime el sitio de demostración, debe registrar el vSnap de host local con las credenciales de usuario en otro sitio válido.

Capítulo 7. Protección de hipervisores

Debe registrar los hipervisores que desea proteger en IBM Spectrum Protect Plus y, a continuación, crear trabajos para realizar copias de seguridad de las máquinas virtuales y de los recursos que están asociados con los hipervisores y restaurarlos.

Copia de seguridad y restauración de datos de VMware

Para proteger datos de VMware, añada en primer lugar instancias de vCenter Server en IBM Spectrum Protect Plus y, a continuación, cree trabajos para las operaciones de copia de seguridad y restauración para el contenido de las instancias.

Requisitos del sistema

Asegúrese de que el entorno de VMware cumple los requisitos del sistema en “Requisitos del hipervisor ” en la página 26.

Soporte para etiquetas de VMware

IBM Spectrum Protect Plus da soporte a etiquetas de máquina virtual de VMware. Las etiquetas se aplican en vSphere y permiten a los usuarios asignar metadatos a las máquinas virtuales. Cuando se aplican e vSphere y se añaden al inventario de IBM Spectrum Protect Plus, las etiquetas de máquina virtual se pueden ver a través del filtro **Ver** > **Códigos y categorías** al crear una definición de trabajo. Para obtener más información sobre el etiquetado de VMware, consulte Etiquetado de objetos.

Soporte para cifrado

La copia de seguridad y la restauración de las máquinas virtuales cifradas está soportada en entornos de vSphere 6.5 y posterior. Se puede hacer una copia de seguridad y restauración de las máquinas virtuales cifradas en el nivel de máquina virtual en su ubicación original. Si está restaurando en una ubicación alternativa, la máquina virtual cifrada se restaura sin cifrado y se debe cifrar manualmente a través de vCenter Server después de que se complete la restauración.

Se precisan los privilegios de vCenter Server siguientes para habilitar operaciones para máquinas virtuales cifradas:

- Cryptographer.Access
- Cryptographer.AddDisk
- Cryptographer.Clone

Adición de una instancia de vCenter Server

Cuando se añade una instancia vCenter Server a IBM Spectrum Protect Plus, se captura un inventario de la instancia, lo que permite completar los trabajos de copia de seguridad y restauración, así como los informes de ejecución.

Procedimiento

Para añadir una instancia de vCenter Server, complete los pasos siguientes:

1. En el panel de navegación, pulse **Gestionar protección** > **Hipervisores** > **VMware**.
2. Pulse **Gestionar vCenter**.
3. Pulse **Añadir vCenter**.
4. Cumplimente los campos en la sección **Propiedades de vCenter**:

Nombre de host/IP
Especifique la dirección IP que se pueda resolver o una vía de acceso y un nombre de máquina que se puedan resolver.

Utilizar usuario existente
Habilite esta opción para seleccionar un nombre de usuario y una contraseña especificados anteriormente para la instancia de vCenter Server.

Nombre de usuario
Escriba el nombre de usuario para la instancia de vCenter Server.

Contraseña
Escriba la contraseña para la instancia de vCenter Server.

Puerto
Escriba el puerto de comunicaciones de la instancia de vCenter Server. Seleccione el recuadro **Utilizar SSL** para habilitar una conexión Secure Sockets Layer (SSL) cifrada. El puerto predeterminado típico es 80 para las conexiones no SSL o 443 para las conexiones SSL.

5. En la sección **Opciones**, configure la opción siguiente:

   Número máximo de MV para procesar simultáneamente para cada servidor ESX y cada SLA
   Establezca el número máximo de instantáneas de máquina virtual simultáneas para procesar en el servidor ESX.

6. Pulse **Guardar**. IBM Spectrum Protect Plus confirma una conexión de red, añade la instancia de vCenter Server a la base de datos y, a continuación, cataloga la instancia.

   Si aparece un mensaje que indica que la conexión no se ha realizado correctamente, revise las entradas. Si las entradas son correctas y la conexión no se ha realizado correctamente, póngase en contacto con un administrador de red para revisar las conexiones.

Qué hacer a continuación
Después de añadir una instancia de vCenter Server, complete los pasos siguientes:

Acción	Cómo
Asigne permisos de usuario al hipervisor.	Consulte “Creación de un rol” en la página 308.

Conceptos relacionados
“Gestión de identidades” en la página 313
Algunas características de IBM Spectrum Protect Plus requieren credenciales para acceder a los recursos. Por ejemplo, IBM Spectrum Protect Plus se conecta a servidores de Oracle como usuario del sistema operativo local que se especifica durante el registro para completar tareas como la catalogación, la protección de datos y la restauración de datos.

Tareas relacionadas
“Copia de seguridad de datos de VMware” en la página 107
Utilice un trabajo de copia de seguridad para realizar una copia de seguridad de recursos de VMware, tales como máquinas virtuales, almacenes de datos, carpetas, vApps y centros de datos con instantáneas.

“Restauración de datos de VMware” en la página 116
Los trabajos de restauración de VMware admiten los casos de ejemplo de Restauración de máquina virtual instantánea y Restauración de disco instantánea, que se crean automáticamente basándose en el origen seleccionado.

Privilegios de máquinas virtuales
Los privilegios de vCenter Server son necesarios para las máquinas virtuales que están asociadas con un proveedor de VMware. Estos privilegios se incluyen en el rol de administrador de vCenter.

Si el usuario que está asociado con el proveedor no se le asigna l rol de administrador para un objeto de inventario, el usuario debe tener asignado un rol que tenga los siguientes privilegios necesarios. Asegúrese de que los privilegios se propagan a los objetos hijo. Para obtener instrucciones, consulte la documentación de VMware sobre cómo añadir un permiso a un objeto de inventario.

Objeto de vCenter Server	Privilegios necesarios
Alarma	• Alarma reconocida • Establecer estado de alarma
Operaciones criptográficas	• Añadir discos • Acceso directo • Cifrar • Cifrar nuevo • Gestionar políticas de cifrado
Centro de datos	• Crear centro de datos • Reconfigurar centro de datos
Almacén de datos	• Asignar espacio • Examinar almacén de datos • Configurar almacén de datos • Operaciones de archivo de bajo nivel • Eliminar archivo • Actualizar archivos de máquina virtual
Clúster de almacenes de datos	• Configurar un clúster de almacén de datos
Conmutador distribuido	• Crear • Suprimir • Operación de host • Modificar • Mover • Operación de control de E/S de red • Operación de política • Opción de configuración de puerto • Operación de parámetro de puerto • Operación VSPAN
Gestor de agentes ESX	• Configurar • Modificar • Ver
Extensión	• Registrar extensión
Carpeta	• Crear carpeta • Suprimir carpeta • Mover carpeta • Renombrar carpeta

Objeto de vCenter Server	Privilegios necesarios
Global	• Cancelar tarea • Diagnóstico (utilizado para la resolución de problemas, no es necesario para operaciones) • Inhabilitar métodos • Habilitar métodos • Licencias • Suceso de registro • Gestionar atributos personalizados • Establecer atributos personalizados • Valores
Host > Configuración	• Configuración avanzada • Configuración de partición de almacenamiento
Servicio de inventario > Descodificación de vSphere	• Asignar o desasignar código vSphere • Crear código vSphere • Crear categoría de código vSphere • Campo Modificar UsedBy para categoría • Campo Modificar UsedBy para código
Red	• Asignar una red • Configurar • Mover red • Eliminar
Recurso	• Aplicar recomendación • Asignar una vApp a la agrupación de recursos • Asignar máquina virtual a agrupación de recursos • Crear agrupación de recursos • Migrar máquina virtual apagada • Migrar máquina virtual encendida • Modificar agrupación de recursos • Mover agrupación de recursos • Consultar vMotion • Eliminar agrupación de recursos • Renombrar agrupación de recursos
Sesiones	• Ver y detener sesiones
Vistas de almacenamiento	• Configurar servicio • Ver
Tareas	• Crear tarea • Actualizar tarea

Objeto de vCenter Server	Privilegios necesarios
Máquina virtual > Configuración	• Añadir disco existente • Añadir nuevo disco • Añadir o eliminar dispositivo • Avanzado • Cambiar recuento de CPU • Cambiar recurso • Configurar managedBy • Seguimiento de cambios de disco • Arrendamiento de disco • Mostrar valores de conexión • Ampliar disco virtual • Dispositivo USB de host • Memory • Modificar valores de dispositivo • Consultar compatibilidad con la tolerancia a errores • Consultar archivos propietarios • Dispositivo en bruto • Recargar desde vía de acceso • Eliminar disco (desconectar y eliminar disco virtual) • Renombrar • Restablecer información de invitado • Establecer anotación • Valores • Ubicación del archivo Swapfile • Desbloquear máquina virtual • Actualizar compatibilidad de máquina virtual
Máquina virtual > Operaciones de invitado	• Modificaciones de operaciones de invitado • Ejecución del programa de operaciones de invitado • Consultas de operaciones de invitado

Objeto de vCenter Server	Privilegios necesarios
Máquina virtual > Interacción	• Responder a pregunta • Operación de copia de seguridad en máquina virtual • Configurar soporte de CD • Configurar soporte de disquete • Interacción de consola • Crear captura de pantalla • Desfragmentar todos los discos • Conexión de dispositivo • Inhabilitar tolerancia a errores • Habilitar tolerancia a errores • Gestión del sistema operativo invitado por la API de VIX • Inyectar códigos de exploración HID USB • Realizar operaciones de borrado o de reducción • Apagar • Encender • Grabar sesión en VM • Reproducir sesión en VM • Restablecer • Reanudar tolerancia a errores • Suspender • Suspender tolerancia a errores • Migración tras error de prueba • Reiniciar máquina virtual secundaria de prueba • Desactivar tolerancia a errores • Activar tolerancia a errores • Instalación de herramientas de VMware
Máquina virtual > Inventario	• Crear desde existente • Crear nuevo • Mover • Registrar • Eliminar • Anular registro

Objeto de vCenter Server	Privilegios necesarios
Máquina virtual > Suministro	• Permitir acceso a disco • Permitir acceso a disco de sólo lectura • Permitir descarga de la máquina virtual • Permitir carga de archivos de máquina virtual • Clonar plantilla • Clonar máquina virtual • Crear plantilla a partir de máquina virtual • Personalizar • Desplegar plantilla • Marcar como plantilla • Marcar como máquina virtual • Modificar especificación de personalización • Ascender discos • Leer especificaciones de personalización
Máquina virtual > Configuración de servicio	• Permitir notificaciones • Permitir sondeo de notificaciones de sucesos globales • Gestionar configuraciones de servicio • Modificar configuraciones de servicio • Consultar configuraciones de servicio • Leer configuraciones de servicio
Máquina virtual > Gestión de instantáneas	• Crear instantánea • Eliminar instantánea • Renombrar instantánea • Revertir a instantánea
Máquina virtual > Réplica de vSphere	• Configurar réplica • Gestionar réplica • Supervisar réplica

Objeto de vCenter Server	Privilegios necesarios
vApp	• Añadir máquina virtual a vApp • Asignar agrupación de recursos a vApp • Asignar vApp a otra vApp • Clonar • Crear • Suprimir • Exportar • Importar • Mover • Apagar • Encender • Renombrar • Suspender • Anular registro • Ver entorno OVF • Configuración de aplicación vApp • Configuración de instancia de vApp • Configuración de vApp managedBy • Configuración de recursos de vApp

Detección de recursos de VMware
Los recursos de VMware se detectan automáticamente después de que se añada la instancia de vCenter Server a IBM Spectrum Protect Plus. Sin embargo, puede ejecutar un trabajo de inventario para detectar cualquier cambio que se haya producido desde que se añadió la instancia.

Procedimiento

Para ejecutar un trabajo de inventario, realice los pasos siguientes:

1. En el panel de navegación, pulse **Gestionar protección** > **Hipervisores** > **VMware**.
2. En la lista de instancias de vCenters Server, seleccione una instancia o pulse el enlace de la instancia para navegar hasta el recurso que desee. Por ejemplo, si desea ejecutar un trabajo de inventario para una máquina virtual individual de la instancia, pulse el enlace de la instancia y, a continuación, seleccione una máquina virtual.
3. Pulse **Ejecutar inventario**.

Prueba de conexión con una máquina virtual de vCenter Server
Puede probar la conexión con una máquina virtual de vCenter Server. La función de prueba verifica la comunicación con la máquina virtual y prueba los valores del servidor de nombres de dominio (DNS) entre el dispositivo virtual de IBM Spectrum Protect y la máquina virtual.

Procedimiento

Para probar la conexión, complete los pasos siguientes:

1. En el panel de navegación, pulse **Gestionar protección** > **Hipervisores** > **VMware**.
2. En la lista de instancias de vCenters Servers, pulse el enlace de un vCenter Server para ir hasta las máquinas virtuales individuales.
3. Seleccione una máquina virtual y, a continuación, pulse **Seleccionar opciones**.
4. Seleccione **Utilizar usuario existente**.

5. Seleccione un usuario en la lista **Seleccionar usuario**.
6. Pulse **Probar**.

Copia de seguridad de datos de VMware

Utilice un trabajo de copia de seguridad para realizar una copia de seguridad de recursos de VMware, tales como máquinas virtuales, almacenes de datos, carpetas, vApps y centros de datos con instantáneas.

Antes de empezar

Revise los procedimientos y las consideraciones siguientes antes de crear una definición de trabajo de copia de seguridad:

- Registre los proveedores cuya copia de seguridad desea realizar. Para obtener más instrucciones, consulte "Adición de una instancia de vCenter Server" en la página 99.
- Configure las políticas de SLA. Para obtener más instrucciones, consulte "Crear políticas de copia de seguridad" en la página 77.
- Para que un usuario de IBM Spectrum Protect Plus pueda implementar operaciones de copia de seguridad y restauración, deben asignarse roles al usuario. Otorgue a los usuarios acceso a los hipervisores y a las operaciones de copia de seguridad y restauración utilizando el panel **Cuentas**. Los roles y los permisos asociados se asignan durante la creación de cuentas de usuario. Para obtener más información, consulte Capítulo 13, "Gestión del acceso de usuarios", en la página 303 y "Gestión de cuentas de usuario" en la página 311.
- Si una máquina virtual está asociada a varias políticas de SLA, asegúrese de que las políticas no se han planificado para ejecutarse simultáneamente. Planifíquelas para que se ejecuten con un periodo de tiempo suficiente entre ellas, o bien combínelas en una única política de SLA.
- Si el vCenter es una máquina virtual, para ayudar a maximizar la protección de datos, tenga el vCenter en un almacén de datos dedicado y realice una copia de seguridad en un trabajo de copia de seguridad aparte.
- Cuando realice una copia de seguridad de las máquinas virtuales VMware, IBM Spectrum Protect Plus descarga los archivos .vmx, .vmxf y .nvram, si es necesario, y luego transfiere dichos archivos a vSnap según sea necesario. Para que esto funcione correctamente, el dispositivo IBM Spectrum Protect Plus debe poder resolver y acceder a todos los hosts ESXi protegidos; y cuando se comunique con un host ESXi, se debe devolver la dirección IP correcta.
- Si una VM está protegida por una política de SLA, las copias de seguridad de la VM se mantendrán basándose en los parámetros de retención de la política de SLA, aunque se haya eliminado la VM del vCenter.
- En algunos casos, los trabajos de copia de seguridad de VMware generan errores de tipo "anomalía en el montaje". Para resolver este problema, aumente el número máximo de montajes NFS hasta al menos 64 utilizando los valores de NFS.MaxVolumes (vSphere 5.5 y posteriores) y NFS41.MaxVolumes (vSphere 6.0 y posteriores). Siga las instrucciones que se indican en Aumentar el valor predeterminado que define el número máximo de montajes NFS en un host ESXi/ESX.
- Si se ha aplicado vMotion en una VM existente, IBM Spectrum Protect Plus realizará un cambio de base si es necesario.

Procedimiento

Para definir un trabajo de copia de seguridad de VMware, complete los pasos siguientes:

1. En el panel de navegación, pulse **Gestionar protección** > **Hipervisores** > **VMware**.
2. Seleccione los recursos para realizar la copia de seguridad.

   Utilice la función de búsqueda para buscar los recursos disponibles y alternar entre los recursos visualizados utilizando el filtro **Ver**. Las opciones disponibles son **MV y plantillas**, **Máquinas virtuales**, **Almacén de datos**, **Etiquetas y categorías** y **Hosts y clústeres**. Las etiquetas se aplican en vSphere y permiten que un usuario asigne metadatos a las máquinas virtuales.
3. Pulse **Seleccionar política de SLA** para añadir a la definición de trabajo una o más políticas de SLA que cumplen los criterios de datos de copia de seguridad.

4. Para crear la definición de trabajo utilizando las opciones predeterminadas, pulse **Guardar**.

   El trabajo se ejecuta según lo definido en las políticas de SLA que ha seleccionado. Para ejecutar el trabajo manualmente, pulse **Trabajos y operaciones** > **Planificación**. Seleccione el trabajo y pulse **Acciones** > **Iniciar**.

   Sugerencia: el botón **Ejecutar** solo se habilita para una copia de seguridad de hipervisor individual, y el hipervisor debe tener una política de SLA aplicada.

   Cuando se guarda la definición de trabajo, se descubren los discos de máquina virtual (VMDK) disponibles en una máquina virtual y se muestran cuando se selecciona **Máquinas y plantillas** en el filtro **Ver**. De forma predeterminada, estos VMDK se asignan a la misma política de SLA que la máquina virtual. Si desea una operación de copia de seguridad más granular, puede excluir los VMDK individuales de la política de SLA. Para obtener instrucciones, consulte "Exclusión de VMDK de la política de SLA para un trabajo" en la página 111.
5. Para editar opciones antes de crear la definición de trabajo, pulse **Seleccionar opciones**.

   En la sección **Opciones de copia de seguridad**, establezca las opciones de definición de trabajo siguientes:

   Omitir almacenes de datos de solo lectura

   Omita los almacenes que están montados como de solo lectura.

   Omitir almacenes de datos temporales montados para el acceso instantáneo

   Excluya almacenes de datos temporales de acceso instantáneo de la definición de trabajo de copia de seguridad.

   Proxy VADP

   Seleccione un proxy VADP para equilibrar la carga.

   Prioridad

   Establezca la prioridad de copia de seguridad del recurso seleccionado. Los recursos con un valor de prioridad más alta se copian en primer lugar en el trabajo. Pulse el recurso que desee priorizar en la sección **Copia de seguridad de VMware** y establezca la prioridad de copia de seguridad en el campo **Prioridad**. Establezca 1 para el recurso de prioridad más alta o 10 para la más baja. Cuando un valor de prioridad no está establecido, se asigna automáticamente una prioridad predeterminada de 5.

   En la sección **Opciones de instantánea**, establezca las opciones de definición de trabajo siguientes:

   Hacer que el sistema de archivos/aplicación de instantánea de MV sea coherente

   Habilite esta opción para activar la coherencia de la aplicación o del sistema de archivos para la instantánea de la máquina virtual. Todas las aplicaciones compatibles con VSS como, por ejemplo, Microsoft Active Directory, Microsoft Exchange, Microsoft SharePoint, Microsoft SQL y el estado del sistema están desactivadas temporalmente. Los VMDK y las máquinas virtuales se pueden montar instantáneamente para restaurar los datos relacionados con las aplicaciones desactivadas temporalmente.

   Intentos de reintento de instantánea de MV

   Establezca el número de veces que IBM Spectrum Protect Plus intenta capturar una instantánea coherente de la aplicación o el archivo de una máquina virtual antes de que se cancele el trabajo. Si la opción **Retroceder a la instantánea no desactivada temporalmente si falla la instantánea desactivada** está inhabilitada, se tomará una instantánea no desactivada temporalmente después de los intentos de reintento.

   Retroceder a la instantánea no desactivada temporalmente si falla la instantánea desactivada

   Habilite esta opción para volver a una instantánea coherente que no sea de aplicación o de sistema de archivos si la instantánea coherente de la aplicación falla. Al seleccionar esta opción se garantiza que se toma una instantánea no desactivada temporalmente si los problemas ambientales prohíben la captura de una instantánea coherente de la aplicación o del sistema de archivos.

   En la sección **Opciones de agente**, establezca las opciones de definición de trabajo siguientes:

Truncar registros SQL

Para truncar los registros de aplicación para SQL Server durante el trabajo de copia de seguridad, habilite la opción **Truncar registros SQL**. Las credenciales se deben establecer para la máquina virtual asociada utilizando la opción Nombre de usuario del SO invitado y Contraseña del SO invitado dentro de la definición de trabajo de copia de seguridad. Cuando la máquina virtual se conecta a un dominio, la identidad de usuario respeta el formato predeterminado *dominio\nombre*. Si el usuario es un administrador local, se utiliza el formato *administrador_local*.

La identidad de usuario debe tener privilegios de administrador local. En el servidor de SQL Server, la credencial de inicio de sesión del sistema debe disponer de los permisos siguientes:

- Los permisos sysadmin de SQL Server deben estar habilitados.
- El derecho **Iniciar sesión como servicio** debe estar establecido. Para obtener más información sobre este derecho, consulte Añadir el inicio de sesión como servicio de derecho a una cuenta.

IBM Spectrum Protect Plus genera archivos de registro para la función de corte de registro y los copia en la ubicación siguiente en el dispositivo de IBM Spectrum Protect:

```
/data/log/guestdeployer/última_fecha/última_entrada/nombre_mv
```

Donde *última_fecha* es la fecha en que se ha producido el trabajo de copia de seguridad y el corte de registro, *última_entrada* es el UUID (Universal Unique Identifier) del trabajo y *nombre_mv* es el nombre de host o dirección IP de la máquina virtual donde se ha producido el corte de registro.

Restricción: La indexación de archivos y la restauración de archivos no están soportadas en los puntos de restauración descargados en los recursos de nube o servidores de repositorio.

Metadatos del archivo de catálogo

Active la indexación de archivos de la instantánea asociada. Cuando se complete la indexación de archivos, se pueden restaurar los archivos individuales utilizando el panel **Restauración de archivos** en IBM Spectrum Protect Plus. Las credenciales se deben establecer para la máquina virtual asociada utilizando una clave SSH, o las opciones **Nombre de usuario de SO invitado** y **Contraseña del SO invitado** dentro de la definición de trabajo de copia de seguridad. Asegúrese de que se puede acceder a la máquina virtual desde el dispositivo de IBM Spectrum Protect Plus utilizando el DNS o un nombre de host.

Restricciones: Las claves SSH no son un mecanismo de autorización válido en las plataformas Windows.

La indexación de archivos y la restauración de archivos no están soportadas en los puntos de restauración descargados en los recursos de nube o servidores de repositorio.

Excluir archivos

Especifique los directorios que se deben omitir cuando se realiza la indexación de archivos. Los archivos que hay dentro de estos directorios no se añaden al catálogo de IBM Spectrum Protect Plus y no están disponibles para la recuperación de archivos. Los directorios se pueden excluir mediante una coincidencia exacta o con asteriscos comodín especificados antes del patrón (* test) o después del patrón (test *). También se admiten varios comodines de asterisco en un único patrón. Los patrones admiten caracteres alfanuméricos estándar, así como los siguientes caracteres especiales:-_ y *. Separe varios con un punto y coma.

Utilizar usuario existente

Seleccione un nombre de usuario y una contraseña especificados anteriormente para el proveedor.

Nombre de usuario/Contraseña del SO invitado

Para algunas tareas (como, por ejemplo, la catalogación de metadatos de archivos, la restauración de archivos y la reconfiguración de IP), las credenciales deben establecerse para la máquina virtual asociada. Escriba el nombre de usuario y la contraseña, y asegúrese de que se puede acceder a la máquina virtual desde el dispositivo de IBM Spectrum Protect Plus utilizando DNS o un nombre de host.

6. Para resolver problemas de conexión con una máquina virtual de hipervisor, utilice la función **Probar**.

   La función **Probar** verifica la comunicación con la máquina virtual y prueba los valores DNS entre el dispositivo IBM Spectrum Protect Plus y la máquina virtual. Para probar una conexión, seleccione una única máquina virtual y, a continuación, pulse **Seleccionar opciones**. Seleccione **Utilizar usuario existente** y seleccione un nombre de usuario y una contraseña especificados anteriormente para el proveedor. El botón **Probar** se muestra a la derecha y el botón **Guardar** en la sección **Opciones**. Pulse **Probar**.
7. Pulse **Guardar**.
8. Para configurar opciones adicionales, pulse el campo **Opciones de política** que está asociado al trabajo en la sección **Estado de política de SLA**. Establezca las opciones de política adicionales:

   Scripts anteriores y scripts posteriores

   Ejecute un script anterior o script posterior. Los scripts anteriores y los scripts posteriores se pueden ejecutar antes o después de que se ejecute un trabajo. Las máquinas basadas en Windows scripts Batch y PowerShell mientras que las máquinas basadas en Linux admiten scripts de shell.

   En la sección **Script anterior** o **Script posterior**, seleccione un script cargado y un servidor de script donde se va a ejecutar el script. Los scripts y servidores de script se configuran mediante la página **Configuración del sistema** > **Script**.

   Para seguir ejecutando el trabajo si falla el script asociado con el trabajo, seleccione **Continuar trabajo/tarea en error de script**.

   Cuando esta opción está habilitada, si un script anterior o un script posterior completa el proceso con un código de retorno distinto de cero, se intenta la operación de copia de seguridad o restauración y se informa sobre el estado de la tarea previa del script anterior como COMPLETADO. Si un script posterior se completa con un código de retorno distinto de cero, se informa sobre el estado de la tarea del script posterior como COMPLETADO.

   Cuando esta opción está inhabilitada, no se intenta realizar la copia de seguridad o la restauración y se informa sobre el estado de la tarea del script anterior o del script posterior como FALLIDO.

   Ejecutar inventario antes de la copia de seguridad

   Ejecute un trabajo de inventario y capture los datos más recientes de los recursos seleccionados antes de iniciar el trabajo de copia de seguridad.

   Excluir recursos

   Excluya recursos específicos del trabajo de copia de seguridad utilizando patrones de exclusión únicos o múltiples. Los recursos se pueden excluir mediante una coincidencia exacta o con asteriscos de comodín especificados antes del patrón (* test) o después del patrón (test *).

   También se admiten varios comodines de asterisco en un único patrón. Los patrones admiten caracteres alfanuméricos estándar, así como los siguientes caracteres especiales:-_ y *.

   Separe varios con un punto y coma.

   Forzar copia de seguridad completa de los recursos

   Fuerce operaciones de copia de seguridad base para máquinas virtuales o bases de datos específicas en la definición de trabajo de copia de seguridad. Separe varios recursos con un punto y coma.
9. Para guardar las opciones adicionales que haya configurado, pulse **Guardar**.

Qué hacer a continuación

Después de definir un trabajo de copia de seguridad, puede realizar las acciones siguientes:

Acción	Cómo
Si utiliza un entorno Linux, considere la posibilidad de crear proxies VADP para habilitar el equilibrio de carga.	Consulte “Creación de proxies VADP” en la página 113.

Acción	Cómo
Cree una definición de trabajo de restauración de VMware.	Consulte “Restauración de datos de VMware” en la página 116.

Conceptos relacionados

“Configuración de scripts para las operaciones de copia de seguridad y restauración” en la página 261
Los scripts anteriores y posteriores son scripts que se pueden ejecutar antes o después de que los trabajos de copia de seguridad y restauración se ejecuten en el nivel de trabajo. Los scripts soportados incluyen scripts de shell para máquinas basadas en Linux y scripts Batch y PowerShell para máquinas basadas en Windows. Los scripts se crean localmente, se suben al entorno a través de la página **Script** y se aplican a continuación a las definiciones de trabajos.

Tareas relacionadas

“Inicio de trabajos” en la página 258
Puede ejecutar cualquier trabajo bajo demanda, incluso si el trabajo se ha establecido para que se ejecute en una planificación.

Exclusión de VMDK de la política de SLA para un trabajo

Después de guardar una definición de trabajo de copia de seguridad, puede excluir los VMDK individuales de una máquina virtual de la política de SLA que se asigna al trabajo.

Procedimiento

Para excluir los VMDK de la política de SLA:

1. En el panel de navegación, pulse **Gestionar protección** > **Hipervisores** > **VMware**.
2. Seleccione **VM y plantillas** en el filtro **Ver**.
3. Pulse el enlace para el vCenter y, a continuación, pulse el enlace de la máquina virtual que contiene los VMDK que desea excluir.
4. Seleccione uno o más VMDK y, a continuación, pulse **Seleccionar política de SLA**.
5. Desmarque el recuadro de selección de la política de SLA seleccionada y, a continuación, pulse **Guardar**.

Copia de seguridad de un dispositivo de servidor vCenter basado en Linux

Para realizar una copia de seguridad de un dispositivo de servidor vCenter basado en Linux, debe modificar los scripts pree-freeze y post-thaw de VMware en la máquina virtual de vCenter para evitar copias de seguridad de vCenter dañadas.

Procedimiento

Para modificar los scripts, complete los pasos siguientes:

1. En la máquina virtual, acceda al directorio `/usr/sbin` y sustituya el contenido del script `pree-freeze-script` por el contenido siguiente:

```
#!/bin/bash
#set log directory
log="/var/log/vpostgres_backup.log"
#set and log start date
today=`date +%Y\/%m\/%d\ %H:%M:%S`
echo "${today}: Start of creation consistent state" >> ${log}
#execute freeze command
cmd="echo \"SELECT pg_start_backup('${today}', true);\" | sudo /opt/vmware/vpostgres/9.4/bin/psql -U postgres >> ${log}
2>&1"
eval ${cmd}
#set and log end date
today=`date +%Y\/%m\/%d\ %H:%M:%S`
echo "${today}: Finished freeze script" >> ${log}
```

2. Sustituya el contenido del script `post-thaw-script` por el contenido:

```
#!/bin/bash
#set log directory
log="/var/log/vpostgres_backup.log"
#set and log start date
today=`date +%Y\/%m\/%d\ %H:%M:%S`
echo "${today}: Release of backup" >> ${log}
#execute release command
cmd="echo \"SELECT pg_stop_backup();\" | sudo /opt/vmware/vpostgres/9.4/bin/psql -U postgres >> ${log} 2>&1"
```

```
eval ${cmd}
#set and log end date
today=`date +%Y\/%m\/%d\ %H:%M:%S`
echo "${today}: Finished thaw script" >> ${log}
```

Gestión de proxies de copias de seguridad VADP

En IBM Spectrum Protect Plus, puede crear proxies para ejecutar trabajos de copia de seguridad de VMware mediante la utilización de VADP (vStorage API for Data Protection) en entornos Linux. Los proxies reducen los recursos del sistema bajo demanda habilitando el compartimiento de carga y el equilibrio de carga. La limitación garantiza que varios proxies VADP se utilicen de forma óptima para sacar el máximo provecho del rendimiento de los datos. Para cada máquina virtual de la que se hace copia de seguridad, IBM Spectrum Protect Plus determina qué proxy VADP es el menos ocupado y tiene la memoria más disponible y las tareas libres. Las tareas libres se determinan mediante el número de núcleos de CPU disponibles o mediante la opción **Límite de tarea Softcap**.

Asegúrese de que dispone de los permisos de usuario necesarios para trabajar con proxies VADP. Para obtener instrucciones sobre la gestión de permisos de proxy VADP, consulte “Tipos de permisos ” en la página 309.

La copia de seguridad de una máquina virtual de VMware incluye los archivos siguientes:

- VMDKs que corresponden a todos los disco. La copia de seguridad base captura todos los datos asignados, o bien todos los datos si los discos están en almacenes de datos NFS. Las copias de seguridad incrementales capturarán sólo los bloques cambiados desde la última copia de seguridad satisfactoria.
- Plantillas de máquinas virtuales
- Archivos de VMware con las extensiones siguientes:
  - .vmx
  - .vmfx (si está disponible)
  - .nvram (almacena el estado de la BIOS de la máquina virtual)

Si existen proxies, toda la carga de proceso se desplaza fuera del sistema host y a los proxies. Si los proxies no existen, la carga completa permanece en el host. La limitación garantiza que varios proxies VADP se utilicen de forma óptima para sacar el máximo provecho del rendimiento de los datos. Para cada máquina virtual de la que se hace copia de seguridad, IBM Spectrum Protect Plus determina qué proxy VADP es el menos ocupado y tiene la memoria más disponible y las tareas libres.

Si un servidor proxy cae o no está disponible por algún motivo antes del inicio del trabajo, los demás proxies toman el control y el trabajo se completa. Si no existe ningún otro proxy, el host se hace cargo del trabajo. Si un servidor proxy pasa a no estar disponible cuando se ejecuta un trabajo, es posible que el trabajo falle.

Las modalidades de transporte describen el método mediante el cual un proxy VADP mueve los datos. La modalidad de transporte se establece como una propiedad del proxy. La mayoría de los trabajos de copia de seguridad y recuperación se configuran más adelante para utilizar uno o más proxies.

Los proxies VADP en IBM Spectrum Protect Plus dan soporte a las siguientes modalidades de transporte de VMware: SAN, HotAdd, NBDSSL y NBD.

Aunque cada empresa es diferente y las prioridades en términos de tamaño, velocidad, fiabilidad y complejidad varían de un entorno a otro, se aplican las directrices generales siguientes a la selección de modalidad de transporte:

- La modalidad de transporte SAN debe utilizarse en un entorno de almacenamiento directo porque esta modalidad es rápida y, por lo general, fiable.
- La modalidad de transporte HotAdd se debe utilizar si el proxy VADP está virtualizado. Esta modalidad da soporte a todos los tipos de almacenamiento de vSphere.
- La modalidad de transporte NBD o NBDSSL (LAN) es la modalidad de reserva porque funciona en entornos físicos, virtuales y mixtos. Sin embargo, con esta modalidad, la velocidad de transferencia de datos puede verse comprometida si las conexiones de red son lentas. La modalidad NBDSSL es similar

a la modalidad NBD, excepto que los datos transferidos entre el proxy VADP y el servidor ESXi están cifrados cuando se utiliza NBDSSL.

Creación de proxies VADP

Puede crear proxies VADP para ejecutar trabajos de copia de seguridad de VMware con IBM Spectrum Protect Plus en entornos de Linux.

Antes de empezar

Tenga en cuenta las consideraciones siguientes antes de crear proxies VADP:

- Revise los requisitos del sistema IBM Spectrum Protect Plus en "Requisitos del proxy VADP" en la página 20.
- La versión de IBM Spectrum Protect Plus del instalador proxy VADP incluye Virtual Disk Development Kit (VDDK) versión 6.5. Esta versión del instalador del proxy VADP proporciona el soporte de proxy VADP externo con vSphere 6.5.

Procedimiento

Para crear proxies VADP de VMware, complete los pasos siguientes:

1. En el panel de navegación, pulse **Configuración del sistema** > **Proxy VADP**.
2. Pulse **Registrar proxy**.
3. Complete los campos siguientes en el panel **Instalar proxy VADP**:

   Nombre de host/IP

   Especifique la dirección IP que se pueda resolver o una vía de acceso y un nombre de máquina que se puedan resolver.

   Seleccionar un sitio

   Seleccione un sitio para asociarlo con el proxy.

   Utilizar usuario existente

   Habilite esta opción para seleccionar un nombre de usuario y una contraseña especificados anteriormente para el proveedor.

   Nombre de usuario

   Escriba el nombre de usuario del servidor proxy VADP.

   Contraseña

   Escriba el nombre de la contraseña del servidor proxy VADP.
4. Pulse **Instalar**.

   El proxy se añade a la tabla **Proxy VADP**.
5. Pulse **Registrar** para registrar el servidor proxy.

   Puede eliminar el registro o suspender el servidor utilizando el menú **Acciones**. Suspender un proxy impide que los próximos trabajos de copia de seguridad utilicen el proxy, y los trabajos que utilizan un proxy suspendido o no registrado se ejecutarán localmente, lo cual puede afectar al rendimiento. Puede completar las tareas de mantenimiento en el proxy mientras está en suspenso. Para reanudar el uso del proxy, seleccione **Acciones** > **Reanudar**.

   Después del registro satisfactorio, el vadp de servicio se inicia en la máquina proxy. Se genera un archivo de registro `vadp.log` en el directorio `/opt/IBM/SPP/logs`.
6. Repita los pasos anteriores para cada proxy que desee crear.

La conexión entre el dispositivo virtual de IBM Spectrum Protect Plus y un proxy de VADP registrado es una conexión bidireccional que requiere que el dispositivo virtual de IBM Spectrum Protect Plus tenga conectividad con el proxy VADP y que el proxy VADP tenga conectividad con el dispositivo virtual de IBM Spectrum Protect Plus. Para garantizar una conexión adecuada del dispositivo virtual de IBM Spectrum

Protect Plus al proxy VADP, verifique si el dispositivo virtual de IBM Spectrum Protect Plus puede hacer ping en el proxy de VADP completando los pasos siguientes:

1. Conéctese a la línea de mandatos para el dispositivo virtual de IBM Spectrum Protect Plus utilizando el protocolo de red Secure Shell (SSH).
2. Ejecute `ping <vadp_ip>`, donde <vadp_ip> es la dirección IP resoluble del proxy VADP.

Si el ping no se ejecuta correctamente, asegúrese de que la dirección IP del proxy VADP se puede resolver, de que el dispositivo de IBM Spectrum Protect Plus se puede direccionar y de que existe una ruta desde el dispositivo de IBM Spectrum Protect Plus hasta el proxy VADP. Si el ping se ejecuta correctamente, asegúrese de que hay una conexión adecuada desde el proxy VADP al dispositivo virtual de IBM Spectrum Protect Plus realizando el procedimiento siguiente:

1. Conéctese a la línea de mandatos del proxy VADP utilizando el protocolo de red Secure Shell (SSH).
2. Ejecute `ping<spectrum_protect_plus_ip>`, donde <spectrum_protect_plus_ip> es la dirección IP que se puede resolver del dispositivo virtual de IBM Spectrum Protect Plus.

Si el ping no se ejecuta correctamente, asegúrese de que la dirección IP del dispositivo virtual de IBM Spectrum Protect Plus se puede resolver y de que el proxy VADP se puede direccionar. Asegúrese de que existe una ruta del proxy VADP al dispositivo virtual de IBM Spectrum Protect Plus.

Qué hacer a continuación

Después de crear los proxies VADP, realice la acción siguiente:

Acción	Cómo
Ejecute el trabajo de copia de seguridad de VMware.	Consulte “Copia de seguridad de datos de VMware” en la página 107. Los proxies se indican en el registro de trabajo con un mensaje de registro similar al texto siguiente: `Run remote vmdkbackup of MicroService: http://<proxy>` *`nombrenodo`*`, IP:`*`dirección_IP_proxy`*

Tareas relacionadas

“Establecimiento de opciones para proxies VADP” en la página 114
Puede crear proxies VADP para ejecutar trabajos de copia de seguridad de VMware con IBM Spectrum Protect Plus en entornos de Linux.

Establecimiento de opciones para proxies VADP

Puede crear proxies VADP para ejecutar trabajos de copia de seguridad de VMware con IBM Spectrum Protect Plus en entornos de Linux.

Procedimiento

Para establecer opciones para proxies VADP de VMware, complete los pasos siguientes:

1. En el panel de navegación, pulse **Configuración del sistema** > **Proxy VADP**.
2. Pulse el icono de opciones ••• para ver las opciones disponibles del proxy.
3. Complete los campos siguientes en el panel **Establecer opciones de proxy VADP**:

   Sitio

   Asigne un sitio al proxy.

   Usuario

Seleccione un nombre de usuario especificado previamente para el proveedor. Para habilitar las actualizaciones automáticas del proxy VADP, se debe seleccionar un nombre de usuario especificado anteriormente.

Modalidades de transporte

Establezca las modalidades de transporte que debe utilizar el proxy. Para obtener más información sobre las modalidades de transporte de VMware, consulte Métodos de transporte de disco virtual.

Habilitar compresión NBDSSL

Si ha seleccionado la modalidad de transporte NBDSSL, habilite la compresión para aumentar el rendimiento de las transferencias de datos.

Para desactivar la compresión, seleccione **inhabilitado**.

Retención de registro en días

Escriba el número de días que se deben retener los registros antes de suprimirse.

Tamaño del almacenamiento intermedio de lectura y escritura

Establezca el tamaño de almacenamiento intermedio de la transferencia de datos, medido en bytes.

Tamaño de bloque del volumen NFS

Establezca el tamaño de bloque que debe utilizar el volumen NFS montado, medido en bytes.

Límite de tarea Softcap

Establezca el número de máquinas virtuales simultáneas que un proxy puede procesar. Si selecciona **Utilizar todos los recursos**, el número de CPU del proxy determina el límite de tareas basándose en la fórmula siguiente:

1 CPU = 1 VMDK

Una CPU es la unidad de hardware más pequeña capaz de ejecutar una hebra. El número de CPU en un proxy se determina utilizando el mandato `lscpu`.

Qué hacer a continuación

Después de crear los proxies VADP, realice las acciones siguientes:

Acción	Cómo
Ejecute el trabajo de copia de seguridad de VMware.	Consulte “Copia de seguridad de datos de VMware” en la página 107. Los proxies se indican en el registro de trabajo con un mensaje de registro similar al texto siguiente: `Run remote vmdkbackup of MicroService: http://<proxy` *`nombrenodo`*`, IP:`*`dirección_IP_proxy`*
Desinstale los proxies cuando deje de ejecutar los trabajos de copia de seguridad de VMware.	Para desinstalar un proxy, ejecute el siguiente mandato en el sistema host desde el subdirectorio de desinstalación del directorio de instalación `/opt/IBM/SPP`: `./uninstall_vmdkbackup`

Tareas relacionadas

“Creación de proxies VADP” en la página 113
Puede crear proxies VADP para ejecutar trabajos de copia de seguridad de VMware con IBM Spectrum Protect Plus en entornos de Linux.

Desinstalación de proxies VADP

Puede eliminar proxies VADP del entorno de IBM Spectrum Protect Plus.

Procedimiento

Para desinstalar proxies VADP de IBM Spectrum Protect Plus, siga estos pasos:

1. Desde un indicador de mandatos, vaya hasta el directorio `/opt/IBM/SPP/uninstall` en el sistema host de proxy.
2. Ejecute el siguiente mandato:
   `./uninstall_vmdkbackup`

Restauración de datos de VMware

Los trabajos de restauración de VMware admiten los casos de ejemplo de Restauración de máquina virtual instantánea y Restauración de disco instantánea, que se crean automáticamente basándose en el origen seleccionado.

Antes de empezar

Complete las tareas siguientes:

- Asegúrese de que se ha ejecutado un trabajo de copia de seguridad de VMware al menos una vez. Para obtener instrucciones, consulte “Copia de seguridad de datos de VMware” en la página 107.
- Para que un usuario de IBM Spectrum Protect Plus pueda completar las operaciones de copia de seguridad y restauración, se deben asignar roles al usuario. Otorgue a los usuarios acceso a los hipervisores y a las operaciones de copia de seguridad y restauración mediante el panel **Cuentas**. Los roles y los permisos asociados se asignan durante la creación de cuentas de usuario. Para obtener más información, consulte Capítulo 13, “Gestión del acceso de usuarios”, en la página 303 y “Gestión de cuentas de usuario” en la página 311.
- El tamaño de una máquina virtual que se restaura desde una descarga de vSnap a un punto de restauración de IBM Spectrum Protect será igual al tamaño suministrado pesado de la máquina virtual, independientemente del suministro de origen debido al uso de almacenes de datos NFS durante la descarga. El tamaño completo de los datos se debe transferir incluso si no están asignados en la máquina virtual de origen.
- Asegúrese de que el destino que tiene previsto utilizar para el trabajo de restauración esté registrado en IBM Spectrum Protect Plus. Este requisito se aplica a los trabajos de restauración que restauran los datos a los hosts o clústeres originales.
- La indexación de archivos de Windows y la restauración de archivos en volúmenes que residen en discos dinámicos no están soportadas.
- Cuando se realiza una restauración desde un archivado de IBM Spectrum Protect, los archivos se migrarán a una agrupación de transferencia desde la cinta antes del inicio del trabajo. Dependiendo del tamaño de la restauración, este proceso puede tardar varias horas.

Acerca de esta tarea

Si se selecciona un VMDK para la operación de restauración, IBM Spectrum Protect Plus presenta automáticamente opciones para un trabajo de restauración de disco instantánea, que proporciona acceso de grabación instantánea a puntos de restauración de datos y de aplicaciones. Una instantánea de IBM Spectrum Protect Plus está correlacionada con un servidor de destino al que se puede acceder o que se puede copiar cuando sea necesario.

Todos los demás orígenes se restauran mediante trabajos de restauración de la máquina virtual instantánea, que se pueden ejecutar en las modalidades siguientes:

Modalidad de prueba
La modalidad de prueba crea máquinas virtuales para el desarrollo o las pruebas, la verificación de instantáneas y la verificación de recuperación tras desastre de una forma programada y repetida sin que por ello afecte a los entornos de producción. Las máquinas de prueba se mantienen en

funcionamiento mientras son necesarias para completar las pruebas y la verificación y luego se limpian. A través de redes delimitadas, puede establecer un entorno seguro para probar los trabajos sin interferir con las máquinas virtuales que se utilizan para la producción. Las máquinas virtuales que se crean en modalidad de prueba también reciben nombres e identificadores exclusivos para evitar conflictos dentro del entorno de producción. Para obtener instrucciones sobre la creación de una red delimitada, consulte “Creación de una red delimitada con un trabajo de restauración de VMware” en la página 122.

Modalidad de clonación
La modalidad de clonación crea copias de máquinas virtuales para los casos de uso que requieren copias permanentes o de larga ejecución para la minería de datos o la duplicación de un entorno de prueba en una red delimitada. Las máquinas virtuales creadas en la modalidad de clonación también reciben nombres e identificadores exclusivos para evitar conflictos dentro del entorno de producción. Con la modalidad de clonación, debe tener en cuenta el consumo de recursos porque la modalidad de clonación crea máquinas virtuales permanentes o a largo plazo.

Modalidad de producción
La modalidad de producción permite la recuperación tras desastre en el sitio local desde el almacenamiento primario o un sitio remoto de recuperación tras desastre, sustituyendo las imágenes de máquina originales por las imágenes de recuperación. Todas las configuraciones se llevan a cabo como parte de la recuperación, incluidos los nombres e identificadores, y todos los trabajos de datos de copia asociados a la máquina virtual continúan ejecutándose.

Procedimiento

Para definir un trabajo de restauración de VMware, realice los pasos siguientes:

1. En el panel de navegación, pulse **Gestionar protección** > **Hipervisores** > **VMware** > **Crear trabajo de restauración** para abrir el asistente "Restauración de instantáneas".

   Sugerencias:

   - También puede abrir el asistente "Restauración de instantáneas" pulsando **Trabajos y operaciones** > **Crear trabajo de restauración** > **VMware**.
   - Para obtener un resumen en ejecución de las selecciones en el asistente "Restauración de instantáneas", mueva el cursor al icono de información en el panel de navegación del asistente.
   - Para omitir las páginas opcionales en el asistente, seleccione **Omitir pasos opcionales**.

2. En la página **Selección de origen**, lleve a cabo las acciones siguientes:
   a) Revise los orígenes disponibles, incluidas las máquinas virtuales (VM) y los discos virtuales (VDisks). Utilice el filtro **Ver** para conmutar entre los orígenes visualizados para mostrar los hosts y los clústeres, las MV, o las etiquetas y categorías. Puede expandir un origen pulsando su nombre.

      También puede especificar todo o parte de un nombre en el recuadro **Buscar** para localizar las máquinas virtuales que coinciden con los criterios de búsqueda. Puede utilizar el carácter comodín (*) para representar todo o parte de un nombre. Por ejemplo, `vm2*` representa todos los recursos que comienzan con "vm2".

   b) Pulse el icono de signo más situado junto al elemento que desea añadir a la lista de restauración al lado de la lista de orígenes. Puede añadir más de un elemento del mismo tipo (MV o disco virtual).

      Para eliminar un elemento de la lista de restauración, pulse el icono de signo menos situado junto al elemento.

   c) Pulse **Siguiente**.
3. En la página **Instantánea de origen** , especifique la instancia de la máquina virtual o del disco virtual que desea restaurar. Complete los siguientes campos y pulse **Siguiente** para continuar. Algunos campos no se visualizan hasta que se selecciona un campo relacionado.

Opción	Descripción
Tipo de restauración	Seleccione el tipo de trabajo de restauración: **Bajo demanda** Ejecuta una operación de restauración puntual. **Recurrente** Crea un trabajo de restauración de punto en el tiempo repetitivo que se ejecuta en una planificación.
Tipo de ubicación de restauración	Seleccione un tipo de ubicación desde donde se restauran los datos: **Sitio** El sitio en el que se hizo la copia de seguridad de las instantáneas. El sitio se define en el panel **Configuración del sistema** > **Sitio**. **Descarga de la nube** El servidor de nube en el que se han descargado las instantáneas. El servidor de nube se define en el panel **Configuración del sistema** > **Almacenamiento de copia de seguridad** > **Cloud**. **Descarga del repositorio** El servidor de repositorio donde se han descargado las instantáneas. El servidor de repositorio se define en el panel **Configuración del sistema** > **Almacenamiento de copia de seguridad** > **Servidor de repositorio**. **Archivado de nube** El servidor de nube en el que se han archivado las instantáneas. El servidor de nube se define en el panel **Configuración del sistema** > **Almacenamiento de copia de seguridad** > **Cloud**. **Archivado de repositorio** El servidor de repositorio en el que se han archivado las instantáneas. El servidor de repositorio se define en el panel **Configuración del sistema** > **Almacenamiento de copia de seguridad** > **Servidor de repositorio**.
Seleccionar una ubicación	Si está restaurando datos desde un sitio, seleccione una de las siguientes ubicaciones de restauración: **Demo** El sitio de demostración desde el que se restauran las instantáneas. **Primario** La ubicación del sitio primario desde la que se restauran las instantáneas. **Secundario** La ubicación del sitio secundario desde la que se restauran las instantáneas. Si está restaurando datos desde un servidor de nube o de repositorio, seleccione un servidor en el menú **Seleccionar una ubicación**.
Selector de fecha	Para las operaciones de restauración bajo demanda, especifique un rango de fechas para mostrar las instantáneas disponibles dentro de ese rango.
Punto de restauración	Para las operaciones de restauración bajo demanda, seleccione una instantánea en la lista de instantáneas disponibles en el rango de datos seleccionado.
Utilizar el servidor vSnap alternativo para el trabajo de restauración	Si está restaurando datos desde un recurso de nube o un servidor de repositorio, seleccione este recuadro para especificar un servidor de vSnap alternativo y, a continuación, seleccione un servidor en el menú **Seleccionar vSnap alternativo**.

Opción	Descripción
	Cuando restaura datos desde un punto de restauración que se ha descargado o archivado en un servidor de repositorio o de recursos de nube, se utiliza un servidor vSnap como pasarela para completar la operación. De forma predeterminada, el servidor vSnap que se utiliza para completar la operación de restauración es el mismo servidor vSnap que se utiliza para completar las operaciones de copia de seguridad y de descarga. Para reducir la carga en el servidor vSnap, puede seleccionar un servidor vSnap alternativo para que sirva como pasarela.

4. En la página **Establecer destino** , especifique la instancia que desea restaurar para cada origen elegido y pulse **Siguiente**:

   Host o clúster ESX original
   Seleccione esta opción para restaurar los datos en el host o clúster original.

   Host o clúster de ESX alternativo
   Seleccione esta opción para restaurar los datos en un destino local que sea diferente del host o clúster original y, a continuación, seleccione la ubicación alternativa de los recursos disponibles. Las redes de prueba y producción se pueden configurar en la ubicación alternativa para crear una red delimitada, lo cual impide que las máquinas virtuales que se utilizan para prueba interfieran con las máquinas virtuales que se utilizan para producción. En la sección **vCenters**, seleccione una ubicación alternativa. Puede filtrar las ubicaciones alternativas por hosts o clústeres.

   En el campo **Destino de carpeta de MV**, especifique la vía de acceso a carpeta de la máquina virtual en el almacén de datos de destino. Tenga en cuenta que el directorio se creará si no existe. Utilice "/" como carpeta de máquina virtual raíz del almacén de datos de destino.

   Host ESX si vCenter está inactivo
   Seleccione esta opción para omitir los datos de vCenter y restaurar los datos directamente al host ESX. En otros casos de ejemplo de restauración, las acciones se completan a través de vCenter. Si vCenter no está disponible, esta opción restaura la máquina virtual o máquinas virtuales de vCenter de las que vCenter depende.

5. En la página **Establecer almacén de datos**, lleve a cabo las acciones siguientes:
   - Si está restaurando datos en un clúster o host de ESX alternativo, seleccione el almacén de datos de destino y haga clic en **Siguiente**.
   - Si está restaurando datos en el host o clúster ESX original, no es necesario que establezca un almacén de datos. Pulse **Siguiente**.
6. En la página **Establecer red**, especifique los valores de red que desea utilizar para cada origen elegido y pulse **Siguiente**.
   - Si está restaurando datos en el host o clúster ESX original, especifique los valores de red siguientes:

     Permitir que el sistema defina la configuración de IP
     Seleccione esta opción para permitir que el sistema operativo defina la dirección IP de destino. Durante una operación de restauración en modalidad de prueba, la máquina virtual de destino recibe una nueva dirección MAC junto con un NIC asociado. En función del sistema operativo, se puede asignar una nueva dirección IP basándose en el NIC original de la máquina virtual o bien se puede asignar mediante DHCP. Durante una restauración en modalidad de producción, la dirección MAC no cambia; por lo tanto, la dirección IP debe mantenerse.

     Utilizar la configuración de IP original
     Seleccione esta opción para restaurar al host o clúster original utilizando la configuración de la dirección IP predefinida. Durante la operación de restauración, la máquina virtual de destino recibe una nueva dirección MAC, pero la dirección IP se conserva.
   - Si está restaurando datos en un host o clúster ESX alternativo, complete los pasos siguientes:

a. En los campos **Producción** y **Prueba**, establezca las redes virtuales para la ejecución de trabajos de restauración de prueba y producción. Los valores de red de destino para entornos de producción y de prueba deben apuntar a diferentes ubicaciones para crear una red delimitada, que impide a las máquinas virtuales utilizadas para la realización de pruebas interferir con máquinas virtuales utilizadas para la producción. Las redes asociadas con las modalidades de prueba y producción se utilizarán cuando el trabajo de restauración se ejecute en la modalidad asociada.

b. Establezca una dirección IP o una máscara de subred para que las máquinas virtuales se vuelvan a dirigir para casos de desarrollo, de prueba o de recuperación tras desastre. Los tipos de correlación soportados incluyen IP a IP, IP a DHCP y subred a subred. Las máquinas virtuales que contienen múltiples NIC están soportadas.

   Realice una de las acciones siguientes:

   – Para permitir que el sistema operativo defina las subredes de destino y las direcciones IP, pulse **Utilizar direcciones IP y subredes definidas por el sistema para el SO invitado de máquina virtual en el destino**.
   – Para utilizar las direcciones IP y subredes predefinidas, pulse **Utilizar direcciones IP y subredes originales para el SO invitado de máquina virtual en el destino**.
   – Para crear una nueva configuración de correlación, seleccione **Añadir correlaciones para subredes y direcciones IP para el SO invitado de máquina virtual en el destino**, pulse **Añadir correlación** y especifique una subred o una dirección IP en el campo **Añadir dirección IP o subred de origen** .

     Elija uno de los protocolos de red siguientes:

     - Seleccione **DHCP** para seleccionar automáticamente una IP y la información de configuración relacionada si DHCP está disponible en el origen seleccionado.
     - Seleccione **Estático** para especificar una subred o dirección IP específica, máscara de subred, pasarela y DNS. Los campos **Subred/Dirección IP**, **Máscara de subred** y **Pasarela** son campos necesarios. Si se especifica una subred como origen, también se debe especificar una subred como destino.

     La reconfiguración de IP se omite para las máquinas virtuales si se utiliza una IP estática, pero no se encuentra ninguna correlación de subred adecuada, o si la máquina virtual de origen está apagada y hay más de un NIC asociado. En un entorno de Windows, si una máquina virtual utiliza solo DHCP, la recuperación de IP se omite para dicha máquina virtual. En un entorno de Linux, se presupone que todas las direcciones son estáticas y solo la correlación IP estará disponible.

7. En los **Métodos de restauración**, seleccione el método de restauración que se utilizará para la selección de origen. Establezca de forma predeterminada el trabajo de restauración de VMware para que se ejecute en modalidad de prueba, producción o clonación. Una vez que se ha creado el trabajo, se puede ejecutar en modalidad de producción o de clonación mediante el panel **Sesiones de trabajo** . También puede cambiar el nombre de la máquina virtual restaurada especificando el nuevo nombre de máquina virtual en el campo **Renombrar VM (opcional)**. Pulse **Siguiente** para continuar.
8. En la página **Opciones de trabajo (opcional)**, configure las opciones avanzadas y haga clic en **Siguiente**.

   Hacer que el recurso de clonación de IA sea permanente
   Habilite esta opción para mover el disco virtual a un almacenamiento permanente y para limpiar los recursos temporales. Esta acción se lleva a cabo iniciando una operación vMotion para los recursos en segundo plano. El destino de la operación vMotion es el almacén de datos de configuración de máquina virtual. El disco de Acceso instantáneo sigue estando disponible para las operaciones de lectura/escritura durante esta operación.

   Encender después de la recuperación
   Alterne el estado de alimentación de una máquina virtual después de que se realice una recuperación. Las máquinas virtuales se encienden en el orden en el que se recuperan, tal como se establece en el paso Origen.

Restricción: Las plantillas de máquina virtual restauradas no se pueden encender después de la recuperación.

Sobrescribir máquina virtual
Habilite esta opción para permitir que el trabajo de restauración sobrescriba la máquina virtual seleccionada. De forma predeterminada, esta opción está inhabilitada.

Continuar con la restauración incluso si falla
Alterne la recuperación de un recurso en una serie si falla la recuperación del recurso anterior. Si esta opción está inhabilitada, el trabajo de restauración se detiene en caso de que falle la recuperación de un recurso.

Ejecutar la limpieza inmediatamente en caso de anomalía del trabajo
Habilite esta opción para limpiar automáticamente los recursos asignados como parte de un trabajo de restauración si falla la recuperación de la máquina virtual.

Permitir sobrescribir y forzar la limpieza de las sesiones anteriores pendientes
Habilite esta opción para permitir que una sesión planificada de un trabajo de recuperación obligue a una sesión pendiente a limpiar los recursos asociados para que se pueda ejecutar la nueva sesión. Inhabilite esta opción para mantener en funcionamiento un entorno de prueba existente sin que se limpie.

Restaurar etiquetas de MV
Habilite esta opción para restaurar las etiquetas aplicadas a máquinas virtuales a través de vSphere.

Arreglar el archivo VMX para el disco que falta
Si los discos individuales se excluyen de una copia de seguridad, la máquina virtual asociada no se iniciará. Habilite esta opción para eliminar las entradas de los discos excluidos del archivo de configuración VMX y asegurarse de que la máquina virtual restaurada se inicia como parte de un trabajo de restauración de máquina virtual instantánea.

Añadir sufijo al nombre de la máquina virtual
Escriba un sufijo para añadirlo a los nombres de las máquinas virtuales restauradas.

Agregar al principio el prefijo para el nombre de máquina virtual
Escriba un prefijo para añadirlo a los nombres de las máquinas virtuales restauradas.

9. Opcional: En la página **Aplicar scripts**, elija las opciones de script siguientes y haga clic en **Siguiente**.
   - Seleccione **Script anterior** para seleccionar un script cargado, y un servidor de aplicaciones o de scripts donde se ejecuta el script anterior. Para seleccionar un servidor de aplicaciones en el que se va a ejecutar el script, desmarque el recuadro de selección **Utilizar servidor de scripts**. Vaya a la página **Configuración del sistema** > **Script** para configurar los scripts y los servidores de scripts.
   - Seleccione **Script posterior** para seleccionar un script cargado, y un servidor de aplicaciones o de scripts donde se ejecuta el script posterior. Para seleccionar un servidor de aplicaciones en el que se ejecuta el script, desmarque el recuadro de selección **Utilizar servidor de scripts**. Vaya a la página **Configuración del sistema** > **Script** para configurar los scripts y los servidores de scripts.
   - Seleccione **Continuar trabajo/tarea en error de script** para seguir ejecutando el trabajo cuando falle el script asociado al trabajo. Cuando esta opción está habilitada y el script anterior se completa con un código de retorno distinto de cero, el trabajo de copia de seguridad o restauración sigue ejecutándose y el estado de la tarea del script anterior devuelve `COMPLETADO`. Si un script posterior se completa con un código de retorno distinto de cero, el estado de la tarea del script posterior devuelve `COMPLETADO`. Cuando esta opción no está seleccionada, el trabajo de copia de seguridad o restauración no se ejecuta, y el estado de la tarea del script anterior o el script posterior devuelve un estado `FALLIDO`.
10. Realice una de las acciones siguientes en la página **Planificación** :
    - Para ejecutar un trabajo bajo demanda, pulse **Siguiente**.
    - Para configurar un trabajo recurrente, especifique un nombre para la planificación de trabajos y especifique la frecuencia y el momento en que se inicia el trabajo de restauración. Pulse **Siguiente**.

11. En la página **Revisar**, revise los valores del trabajo de restauración y pulse **Enviar** para crear el trabajo.

    Los trabajos bajo demanda se iniciarán inmediatamente; los trabajos recurrentes se iniciarán a la hora de inicio planificada.

Qué hacer a continuación

Una vez completado el trabajo, seleccione una de las opciones siguientes en el menú **Acciones** de las secciones Sesiones de trabajos o Clones activos en el panel **Restaurar**:

Limpieza

Destruye la máquina virtual y limpia todos los recursos asociados. Como se trata de una máquina virtual temporal que se va a utilizar para realizar pruebas, todos los datos se pierden cuando se destruye la máquina virtual.

Trasladar a producción (vMotion)
Migra la máquina virtual a través de vMotion hasta la red virtual definida como red de producción.

Clonar (vMotion)
Migra la máquina virtual a través de vMotion hasta el almacén de datos y la red virtual definida como red de prueba.

Tareas relacionadas

"Adición de una instancia de vCenter Server" en la página 99
Cuando se añade una instancia vCenter Server a IBM Spectrum Protect Plus, se captura un inventario de la instancia, lo que permite completar los trabajos de copia de seguridad y restauración, así como los informes de ejecución.

Creación de una red delimitada con un trabajo de restauración de VMware

A través de redes delimitadas, puede establecer un entorno seguro para probar los trabajos sin interferir con las máquinas virtuales que se utilizan para la producción. Las redes delimitadas se pueden utilizar con trabajos que se ejecutan en modalidad de prueba y en modalidad de producción.

Antes de empezar

Cree y ejecute un trabajo de restauración de VMware. Para obtener instrucciones, consulte "Restauración de datos de VMware" en la página 116.

Procedimiento

Para crear una red delimitada, complete los pasos siguientes:

1. En el panel de navegación, pulse **Gestionar protección** > **Hipervisores** > **VMware**.
2. En el panel **Restaurar**, revise los puntos de restauración disponibles de los orígenes de VMware, incluidas las máquinas virtuales, las plantillas de máquina virtual, los almacenes de datos, las carpetas y vApps. Utilice la función de búsqueda y filtros para ajustar la selección entre tipos de sitios de recuperación específicos. Expanda una entrada en el panel **Restaurar** para ver los puntos de restauración individuales por la fecha.
3. Seleccione los puntos de restauración y pulse el icono de añadir a la lista de restauración para añadir el punto de restauración a la lista de restauración. Pulse el icono de eliminar para eliminar elementos de la lista de restauración.
4. Pulse **Opciones** para establecer las opciones de definición de trabajo.
5. Seleccione **Host o clúster de ESX alternativo** y, a continuación, seleccione un host o clúster alternativo en la lista de vCenter.
6. Expanda la sección **Valores de red**. En los campos **Producción** y **Prueba**, establezca las redes virtuales para la ejecución de trabajos de restauración de prueba y producción. Los valores de red de destino de los entornos de prueba y producción deben estar en ubicaciones diferentes para crear una red delimitada, lo cual impide que las máquinas virtuales que se utilizan para prueba interfieran con

las máquinas virtuales que se utilizan para producción. Las redes asociadas a la prueba y la producción se utilizarán cuando el trabajo de restauración se ejecuta en la modalidad asociada. Las direcciones IP de la máquina de destino se pueden configurar mediante las opciones siguientes:

Utilizar las subredes definidas por el sistema y las direcciones IP para el SO invitado de máquina virtual en el destino.
Seleccione esta opción para permitir que el sistema operativo defina la dirección IP de destino. Durante una restauración en modalidad de prueba, la máquina virtual de destino recibe una nueva dirección MAC junto con un NIC asociado. En función del sistema operativo, se puede asignar una nueva dirección IP basándose en el NIC original de la máquina virtual o bien se puede asignar mediante DHCP. Durante una operación de restauración en modalidad de producción, la dirección MAC no cambia; por lo tanto, la dirección IP se debe conservar.

Utilizar las subredes originales y las direcciones IP para el SO invitado de máquina virtual en el destino
Seleccione esta opción para restaurar al host o clúster original utilizando la configuración de dirección IP predefinida. Durante una restauración, la máquina virtual de destino recibe una nueva dirección MAC, pero la dirección IP se conserva.

Establezca los valores de red para una restauración a un host o clúster ESX alternativo o de larga distancia:

En los campos **Producción** y **Prueba**, establezca las redes virtuales para la ejecución de trabajos de restauración de prueba y producción. Los valores de red de destino de los entornos de prueba y producción deben estar en ubicaciones diferentes para crear una red delimitada, lo cual impide que las máquinas virtuales que se utilizan para prueba interfieran con las máquinas virtuales que se utilizan para producción. Las redes asociadas a la prueba y la producción se utilizarán cuando el trabajo de restauración se ejecuta en la modalidad asociada.

Establezca una dirección IP o máscara de subred para que las máquinas virtuales se vuelvan a dirigir para los casos de uso de desarrollo/pruebas o recuperación tras desastre. Los tipos de correlación soportados incluyen IP a IP, IP a DHCP y subred a subred. Las máquinas virtuales que contienen múltiples NIC están soportadas.

De forma predeterminada, la opción **Utilizar las subredes definidas por el sistema y las direcciones IP para el SO invitado de máquina virtual en el destino** está habilitada. Para utilizar las subredes predefinidas y las direcciones IP, seleccione **Utilizar las subredes originales y las direcciones IP para el SO invitado de máquina virtual en el destino**.

Para crear una nueva configuración de correlación, seleccione **Añadir correlaciones para subredes y direcciones IP para el SO invitado de máquina virtual en el destino** y, a continuación, pulse **Añadir correlación**. Escriba una subred o dirección IP en el campo **Origen**. En el campo de destino, seleccione **DHCP** para seleccionar automáticamente una IP y la información de configuración relacionada si DHCP está disponible en el cliente seleccionado. Seleccione **Estático** para especificar una subred o dirección IP específica, máscara de subred, pasarela y DNS. Tenga en cuenta que los campos **Subred/Dirección IP**, **Máscara de subred** y **Pasarela** son campos obligatorios. Si se especifica una subred como origen, también se debe especificar una subred como destino.

La reconfiguración de IP se omite para las máquinas virtuales si se utiliza una IP estática, pero no se encuentra ninguna correlación de subred adecuada, o si la máquina de origen está apagada y hay más de un NIC asociado. En un entorno Windows, si una máquina virtual solo es DHCP, se pasa por alto la reconfiguración de IP para dicha máquina virtual. En un entorno Linux se supone que todas las direcciones son estáticas, y solo estará disponible la correlación IP.

Almacén de datos de destino
Establezca el almacén de datos de destino para una restauración a un host ESX o un clúster alternativo.

Destino de carpeta de MV
Especifique la vía de acceso a la carpeta de la máquina virtual (MV) en el almacén de datos de destino. Tenga en cuenta que el directorio se creará si no existe. Utilice "/" como la carpeta de máquina virtual raíz del almacén de datos de destino.

7. Pulse **Guardar** para guardar las opciones de política.

8. Una vez completado el trabajo, seleccione una de las opciones siguientes en el menú **Acciones** de las secciones Sesiones de trabajos o Clones activos en el panel **Restaurar**:

   Limpieza

   Destruye la máquina virtual y limpia todos los recursos asociados. Puesto que se trata de una máquina virtual temporal/de prueba, todos los datos se pierden cuando se destruye la máquina virtual.

   Trasladar a producción (vMotion)

   Migra la máquina virtual a través de vMotion al almacén de datos y a la red virtual definida como la red de "producción".

   Clonar (vMotion)

   Migra la máquina virtual a través de vMotion al almacén de datos y a la red virtual definida como la red "Prueba".

Tareas relacionadas

“Adición de una instancia de vCenter Server” en la página 99
Cuando se añade una instancia vCenter Server a IBM Spectrum Protect Plus, se captura un inventario de la instancia, lo que permite completar los trabajos de copia de seguridad y restauración, así como los informes de ejecución.

Restauración de datos cuando no se puede acceder a vCenter u otras VM de gestión

IBM Spectrum Protect Plus proporciona una opción para restaurar datos automáticamente utilizando hosts de ESXi si no se puede acceder al vCenter. Esta opción restaura la máquina virtual (VM) de vCenter o las VM de las que depende vCenter.

Acerca de esta tarea

Este procedimiento se puede utilizar si alguno de los siguientes servicios de gestión se pierde parcial o totalmente en el entorno:

- vCenter
- Platform Services Controller (PSC)
- Software-Defined Data Center (SDDC)
- Active Directory (AD)
- Servidores de Sistema de nombres de dominio (DNS)

Para recuperar los datos sin un vCenter, el host ESXi debe tener un conmutador estándar o un conmutador distribuido preexistente con un enlace efímero. Si no se cumplen estos requisitos, debe crear un nuevo conmutador estándar en el host ESXi. Si no hay enlaces ascendentes disponibles para el conmutador estándar, el conmutador estándar debe eliminarse del conmutador distribuido.

El procedimiento describe los pasos manuales adicionales necesarios para completar una operación de restauración cuando la operación se ejecuta en un entorno de vCenter Server (VCS).

La recuperación de una VM de gestión en un entorno VCS puede provocar la pérdida del acceso a la VM. La pérdida del acceso se debe a una configuración incorrecta del conmutador virtual. Siga estos pasos en la VM afectada para recuperarse de este estado y realizar una operación de recuperación.

Procedimiento

1. Conéctese al host de la interfaz de usuario de ESXi de destino y cree un nuevo conmutador virtual estándar. En este punto, no hay grupos de puertos ni enlaces ascendentes disponibles para el conmutador.
2. Utilice el protocolo SSH para conectarse al servidor ESXi. Identifique y seleccione el NIC físico y el grupo de puertos del conmutador virtual distribuido existente denominado SDDC-Dswitch-Private. El siguiente ejemplo hace referencia a una tarjeta de interfaz de red virtualizada (VNIC) denominada

vmnic0, que forma parte del ID de puerto 64. Puede listar la información del conmutador virtual distribuido (DVS) emitiendo el siguiente mandato:

```
#esxcli network vswitch dvs vmware list
```

3. Basándose en la información anterior, elimine el NIC y el ID de puerto (grupo de puertos) del DVS SDDC-Dconmut-Private utilizando el siguiente mandato. Utilice el ID de puerto del paso 2.

   ```
   #esxcfg-vswitch -Q vnic_físico -V grupo_puertos SDDC-Dswitch-Private
   ```

4. Añada el NIC y el grupo de puertos al conmutador estándar que ha creado en el paso 1 emitiendo el siguiente mandato en una línea:

   ```
   #esxcli network vswitch standard uplink add –-uplink-name=vnic_físico --vswitch-
   name=vswitch_estándar
   ```

5. En la interfaz de ESXi, añada un grupo de puertos y seleccione el conmutador virtual estándar.

   El conmutador virtual debe tener un enlace ascendente y un grupo de puertos.

6. Ejecute una operación de restauración en IBM Spectrum Protect Plus con la opción **Host ESX si vCenter está inactivo** habilitada.
7. Pulse **Opciones** cuando defina la operación de restauración en IBM Spectrum Protect Plus y elija el nuevo conmutador de red que ha creado en el paso 1 en **Redes**.
8. Utilizando la interfaz de usuario de ESXI de destino, encienda la VM recuperada.
9. Una vez que se puede acceder a las VM, inicie una sesión en la interfaz de usuario de vCenter e inicie la migración de las VM de gestión desde el grupo de puertos temporales que ha creado en el paso 5 al grupo de puertos distribuido original, SDDC-DPortGroup-Mgmt.

   Para iniciar una migración en la pestaña **Redes**, seleccione un centro de datos y pulse **Migrar máquinas virtuales a otra red** en el menú **Acciones**. Seleccione la red de origen (el conmutador temporal creado en el paso 5) y la red de destino (el conmutador de gestión).
10. Después de migrar todas las VM al grupo de puertos original, vuelva a incorporar el NIC físico y el grupo de puertos al conmutador virtual distribuido original realizando las siguientes acciones:

    a. Elimine las tarjetas de red (conocidas como vmnics) de un vSwitch estándar que se ha refirmado anteriormente emitiendo el mandato siguiente:

       ```
       #esxcli network vswitch standard uplink remove --uplink-name=vmnic --vswitch-name=vSwitch
       ```

       Por ejemplo:

       ```
       #esxcli network vswitch standard uplink remove --uplink-name=vmnic0
       ```

       ```
       --vswitch-name=vered_recovery
       ```

    b. Añada tarjetas de red a un Conmutador distribuido de vNetwork (vDS) emitiendo el mandato siguiente:

       ```
       #esxcfg-vswitch -P vmnic -V unused_dvPort_ID dvSwitch # add a vDS uplink
       ```

       Por ejemplo:

       ```
       #esxcfg-vswitch -P vmnic0 -V 64 SDDC-Dswitch-Private
       ```

11. Suprima el grupo de puertos temporales y el vSwitch estándar de la interfaz de usuario de host ESXi.
12. Una vez que se han migrado las VM y se puede acceder a ellas, utilice la interfaz de usuario del host ESXI para anular el registro de las VM antiguas, sin suprimirlas, si se puede acceder al host original. Con este método, evita crear información duplicada como, por ejemplo, nombres, direcciones de control de acceso a soportes (MAC), ID de nivel de sistema operativo y Universal Unique Identifiers de máquina virtual (UUID). Debe realizar este paso aunque esté utilizando un almacén de datos nuevo.

En algunas versiones de vSphere o ESXi, la operación de anulación de registros se puede realizar utilizando la opción **Eliminar de inventario**. Esto anula el registro de una VM del catálogo de vCenter, pero deja archivos de VMDK en el almacén de datos, que consumen espacio de almacenamiento en el almacén de datos. Una vez que haya recuperado completamente la VM y el entorno se esté ejecutando correctamente, puede volver a recuperar el espacio eliminando manualmente estos archivos del almacén de datos.

Copia de seguridad y restauración de datos de Hyper-V

Para proteger los datos de Hyper-V, en primer lugar añada servidores Hyper-V a IBM Spectrum Protect Plus y, a continuación, cree trabajos para las operaciones de copia de seguridad y restauración para el contenido de los servidores.

Asegúrese de que el entorno de Hyper-V cumple los requisitos del sistema en "Requisitos del hipervisor " en la página 26.

Adición de un servidor Hyper-V

Cuando se añade un servidor Hyper-V a IBM Spectrum Protect Plus, se captura un inventario del servidor, lo que permite completar los trabajos de copia de seguridad y restauración, así como los informes de ejecución.

Antes de empezar

Tenga en cuenta las siguientes consideraciones y procedimientos antes de añadir un servidor Hyper-V a IBM Spectrum Protect Plus:

- Los servidores Hyper-V se pueden registrar utilizando un nombre DNS o una dirección IP. Los nombres de DNS deben ser resueltos por IBM Spectrum Protect Plus. Si el servidor Hyper-V forma parte de un clúster, todos los nodos del clúster se deben poder resolver mediante DNS. Si DNS no está disponible, el servidor se debe añadir al archivo `/etc/hosts` al dispositivo IBM Spectrum Protect Plus. Si se ha configurado más de un servidor Hyper-V en un entorno de clúster, todos los servidores se deben añadir a `/etc/hosts`. Cuando se registra el clúster en IBM Spectrum Protect Plus, debe registrar el gestor de clústeres de migración tras error.
- Todos los servidores Hyper-V, incluidos los nodos de clúster, deben tener el servicio del iniciador iSCSI de Microsoft en ejecución en la lista de servicios. Establezca el servicio en Automático para que esté disponible cuando arranque la máquina.
- Añada el usuario al grupo de administradores locales en el servidor Hyper-V.

Procedimiento

Para añadir un servidor Hyper-V, complete los pasos siguientes:

1. En el panel de navegación, pulse **Gestionar protección** > **Hipervisores** > **Hyper-V**.
2. Pulse **Gestionar servidor Hyper-V**.
3. Pulse **Añadir servidor Hyper-V**.
4. Cumplimente los campos en el panel **Propiedades de servidor**:

   Nombre de host/IP
   Especifique la dirección IP que se pueda resolver o una vía de acceso y un nombre de máquina que se puedan resolver.

   Utilizar usuario existente
   Habilite esta opción para seleccionar un nombre de usuario y una contraseña especificados anteriormente para el servidor.

   Nombre de usuario
   Escriba el nombre de usuario del servidor.

   Contraseña
   Escriba la contraseña del servidor.

Puerto
Escriba el puerto de comunicaciones del servidor que va a añadir. El puerto predeterminado típico es 5985.

Seleccione el recuadro **Utilizar SSL** para habilitar una conexión Secure Sockets Layer (SSL) cifrada.

Para habilitar una conexión SSL, debe añadir el certificado SSL autofirmado para el servidor Hyper-V o un certificado de entidad emisora de certificados (CA). Para cargar un certificado, consulte "Carga de un certificado SSL desde la consola de administración" en la página 286.

Si no selecciona **Utilizar SSL**, debe completar unos pasos adicionales en el servidor Hyper-V. Consulte "Habilitación de WinRM para la conexión con los servidores Hyper-V" en la página 127.

5. En la sección **Opciones**, configure la opción siguiente:

Número máximo de MV para procesar simultáneamente para cada servidor Hyper-V
Establezca el número máximo de instantáneas de máquina virtual simultáneas para procesar en el servidor Hyper-V.

6. Pulse **Guardar**. IBM Spectrum Protect Plus confirma una conexión de red, añade el servidor a la base de datos y a continuación, cataloga el servidor.

Si aparece un mensaje que indica que la conexión no se ha realizado correctamente, revise las entradas. Si las entradas son correctas y la conexión no se ha realizado correctamente, póngase en contacto con un administrador del sistema para revisar las conexiones.

Qué hacer a continuación
Después de añadir el servidor de aplicaciones Hyper-V, realice la acción siguiente:

Acción	Cómo
Asigne permisos de usuario al hipervisor.	Consulte "Creación de un rol" en la página 308.

Tareas relacionadas
"Copia de seguridad de datos de Hyper-V" en la página 128
Utilice un trabajo de copia de seguridad para realizar copias de seguridad de datos de Hyper-V con instantáneas.

"Restauración de datos de Hyper-V" en la página 132
Los trabajos de restauración de Hyper-V admiten los casos de ejemplo de Restauración de máquina virtual instantánea y Restauración de disco instantánea, que se crean automáticamente basándose en el origen seleccionado.

Habilitación de WinRM para la conexión con los servidores Hyper-V
Si no puede utilizar SSL para habilitar el tráfico de red cifrado entre los servidores Hyper-V de IBM Spectrum Protect Plus, debe configurar WinRM en el host para permitir el tráfico de red sin cifrar. Cerciórese de que conoce los riesgos de seguridad asociados a la habilitación del tráfico de red sin cifrar.

Procedimiento

Para configurar WinRM para la conexión con los hosts Hyper-V:

1. En el sistema host de Hyper-V, inicie la sesión con una cuenta de administrador.
2. Abra un indicador de mandatos de Windows. Si el Control de cuentas de usuario (UAC) está habilitado, debe abrir el indicador de mandatos con privilegios elevados ejecutando con la opción "Ejecutar como administrador" habilitada.
3. Especifique el mandato siguiente para configurar WinRM para permitir el tráfico de red sin cifrar:

```
winrm s winrm/config/service @{AllowUnencrypted="true"}
```

4. Verifique si la opción AllowUnencrypted está establecida en true con el mandato siguiente:

```
winrm g winrm/config/service
```

Detección de recursos Hyper-V
Los recursos de Hyper-V se detectan automáticamente después de que se añada el servidor Hyper-V a IBM Spectrum Protect Plus. Sin embargo, puede ejecutar un trabajo de inventario para detectar cualquier cambio que se haya producido desde que se añadió el servidor.

Procedimiento

Para ejecutar un trabajo de inventario, realice los pasos siguientes:

1. En el panel de navegación, pulse **Gestionar protección** > **Hipervisores** > **Hyper-V**.
2. En la lista de servidores Hyper-V, seleccione un servidor o pulse el enlace para que el servidor navegue hasta el recurso que desee. Por ejemplo, si desea ejecutar un trabajo de inventario para una máquina virtual individual en un servidor, pulse el enlace del servidor y, a continuación, seleccione una máquina virtual.
3. Pulse **Ejecutar inventario**.

Prueba de conexión a una máquina virtual de un servidor Hyper-V
Puede probar la conexión con la máquina virtual del servidor Hyper-V. La función de prueba verifica la comunicación con la máquina virtual y prueba los valores NS entre el dispositivo virtual de IBM Spectrum Protect y la máquina virtual.

Procedimiento

Para probar la conexión, complete los pasos siguientes:

1. En el panel de navegación, pulse **Gestionar protección** > **Hipervisores** > **Hyper-V**.
2. En la lista de servidores Hyper-V, pulse el enlace de una máquina virtual del servidor Hyper-V para ir hasta las máquinas virtuales individuales.
3. Seleccione una máquina virtual y, a continuación, pulse **Seleccionar opciones**.
4. Seleccione **Utilizar usuario existente**.
5. Seleccione un usuario en la lista **Seleccionar usuario**.
6. Pulse **Probar**.

Copia de seguridad de datos de Hyper-V

Utilice un trabajo de copia de seguridad para realizar copias de seguridad de datos de Hyper-V con instantáneas.

Antes de empezar
Tenga en cuenta los procedimientos y consideraciones siguientes antes de crear una definición de trabajo de copia de seguridad:

- Registre los proveedores cuya copia de seguridad desea realizar. Para obtener más información, consulte “Adición de un servidor Hyper-V” en la página 126.
- Configure las políticas de SLA. Para obtener instrucciones, consulte “Crear políticas de copia de seguridad” en la página 77.
- Los trabajos de copia de seguridad y restauración de Hyper-V requieren la instalación de los últimos servicios de integración de Hyper-V.

  Para entornos Microsoft Windows, consulte Sistemas operativos invitados de Windows soportados para Hyper-V en Windows Server.

  En entornos Linux, consulte Máquinas virtuales Linux y FreeBSD soportadas para Hyper-V en Windows.
- Todos los servidores Hyper-V, incluidos los nodos de clúster, deben tener el servicio del iniciador iSCSI de Microsoft en ejecución en la lista de servicios. Establezca el servicio en Automático para que esté disponible cuando arranque la máquina.
- Para que un usuario de IBM Spectrum Protect Plus pueda completar las operaciones de copia de seguridad y restauración, se deben asignar roles al usuario. Otorgue a los usuarios acceso a los

hipervisores y a las operaciones de copia de seguridad y restauración mediante el panel **Cuentas**. Los roles y los permisos asociados se asignan durante la creación de cuentas de usuario. Para obtener más información, consulte Capítulo 13, “Gestión del acceso de usuarios”, en la página 303 y “Gestión de cuentas de usuario” en la página 311.

- Si una máquina virtual está asociada a varias políticas de SLA, asegúrese de que las políticas no se han planificado para ejecutarse simultáneamente. Planifíquelas para que se ejecuten con un periodo de tiempo suficiente entre ellas o bien combínelas en una única política de SLA.
- Si la dirección IP del dispositivo de IBM Spectrum Protect Plus se cambia después de crear una copia de seguridad base de Hyper-V inicial, el IQN de destino del recurso de Hyper-V se puede dejar en un estado incorrecto. Para corregir este problema, desde la herramienta del iniciador iSCSI de Microsoft iSCSI, pulse la pestaña **Descubrimiento**. Seleccione la dirección IP antigua y, a continuación, pulse **Eliminar**. Pulse la pestaña **Destino** y desconecte la sesión de reconexión.
- Si una VM está protegida por una política de SLA, las copias de seguridad de la VM se mantendrán basándose en los parámetros de retención de la política de SLA, aunque se haya eliminado la VM.

Procedimiento

Para definir un trabajo de copia de seguridad de Hyper-V, complete los pasos siguientes:

1. En el panel de navegación, pulse **Gestionar protección** > **Hipervisores** > **Hyper-V**.
2. Seleccione los recursos para realizar la copia de seguridad.

   Utilice la función de búsqueda para buscar los recursos disponibles y alternar entre los recursos visualizados a través del filtro **Ver**. Las opciones disponibles son **Máquinas virtuales** y **Almacén de datos**.
3. Pulse **Seleccionar política de SLA** para añadir a la definición de trabajo una o más políticas de SLA que cumplen los criterios de datos de copia de seguridad.
4. Para crear la definición de trabajo utilizando las opciones predeterminadas, pulse **Guardar**.

   El trabajo se ejecuta según lo definido en las políticas de SLA que ha seleccionado. Para ejecutar el trabajo manualmente, pulse **Trabajos y operaciones** > **Planificación**. Seleccione el trabajo y pulse **Acciones** > **Iniciar**.

   Sugerencia: el botón **Ejecutar** solo se habilita para una copia de seguridad de hipervisor individual, y el hipervisor debe tener una política de SLA aplicada.
5. Para editar opciones antes de iniciar el trabajo, pulse el icono de edición en la tabla **Seleccionar opciones**.

   En la sección **Opciones de copia de seguridad**, establezca las opciones de definición de trabajo siguientes:

   Omitir almacenes de datos de solo lectura

   Habilite esta opción para omitir los almacenes de datos montados como de solo lectura.

   Omitir almacenes de datos temporales montados para el acceso instantáneo

   Habilite esta opción para excluir los almacenes de datos de Acceso instantáneo temporales de la definición de trabajo de copia de seguridad.

   Prioridad

   Establezca la prioridad de copia de seguridad del recurso seleccionado. Los recursos con un valor de prioridad más alta se copian en primer lugar en el trabajo. Pulse el recurso que desee priorizar en la sección **Copia de seguridad de VMware** y establezca la prioridad de copia de seguridad en el campo **Prioridad**. Establezca 1 para el recurso de prioridad más alta o 10 para la más baja. Cuando un valor de prioridad no está establecido, se asigna automáticamente una prioridad predeterminada de 5.

   En la sección **Opciones de instantánea**, establezca las opciones de definición de trabajo siguientes:

   Hacer que el sistema de archivos/aplicación de instantánea de MV sea coherente

   Habilite esta opción para activar la coherencia de la aplicación o del sistema de archivos para la instantánea de la máquina virtual.

Intentos de reintento de instantánea de MV

Establezca el número de veces que IBM Spectrum Protect Plus debe intentar realizar una instantánea de una máquina virtual antes de cancelar el trabajo.

En la sección **Opciones de agente**, establezca las opciones de definición de trabajo siguientes:

Truncar registros SQL

Para truncar los registros de aplicación para SQL durante el trabajo de copia de seguridad, habilite la opción **Truncar registros SQL**. Tenga en cuenta que las credenciales deben establecerse para la máquina virtual asociada mediante la opción Nombre de usuario de SO invitado y Contraseña de SO invitado en la definición de trabajo de copia de seguridad. La identidad de usuario respeta el formato *dominio**nombre* si la máquina virtual está conectada a un dominio. El formato *administrador_local* se utiliza si el usuario es un administrador local.

La identidad de usuario debe tener privilegios de administrador local. Además, en el servidor SQL, la credencial de inicio de sesión del sistema debe tener los permisos sysadmin de SQL habilitados, así como el derecho **Iniciar sesión como servicio**. Para obtener más información sobre este derecho, consulte Añadir el inicio de sesión como servicio de derecho a una cuenta.

IBM Spectrum Protect Plus genera registros que pertenecen a la función de corte de registro y los copia en la ubicación siguiente en el dispositivo de IBM Spectrum Protect Plus:

```
/data/log/guestdeployer/última_fecha/última_entrada/nombre_mv
```

Donde *última_fecha* es la fecha en que se ha producido el trabajo de copia de seguridad y el corte de registro, *última_entrada* es el UUID (Universal Unique Identifier) del trabajo y *nombre_mv* es el nombre de host o dirección IP de la máquina virtual donde se ha producido el corte de registro.

Restricción: La indexación de archivos y la restauración de archivos no están soportadas en los puntos de restauración descargados en un servidor de IBM Spectrum Protect.

Metadatos del archivo de catálogo

Para activar la indexación de archivos para la instantánea asociada, habilite la opción de metadatos del archivo de catálogo. Una vez completada la indexación de archivos, se pueden restaurar archivos individuales utilizando el panel **Restauración de archivos** en IBM Spectrum Protect Plus. Tenga en cuenta que las credenciales deben establecerse para la máquina virtual asociada utilizando una clave SSH, o una opción Nombre de usuario de SO invitado y Contraseña de SO invitado en la definición de trabajo de copia de seguridad. Asegúrese de que se puede acceder a la máquina virtual desde el dispositivo IBM Spectrum Protect Plus utilizando el DNS o el nombre de host. Tenga en cuenta que las claves SSH no son un mecanismo de autorización válido para las plataformas Windows.

Excluir archivos

Especifique los directorios que se deben omitir cuando se realiza la indexación de archivos. Los archivos que hay dentro de estos directorios no se añaden al catálogo de IBM Spectrum Protect Plus y no están disponibles para la recuperación de archivos. Los directorios se pueden excluir mediante una coincidencia exacta o con asteriscos comodín especificados antes del patrón (* test) o después del patrón (test *). También se admiten varios comodines de asterisco en un único patrón. Los patrones admiten caracteres alfanuméricos estándar, así como los siguientes caracteres especiales:-_ y *. Separe varios con un punto y coma.

Utilizar usuario existente

Habilite esta opción para seleccionar un nombre de usuario y una contraseña especificados anteriormente para el proveedor.

Nombre de usuario/Contraseña del SO invitado

Para algunas tareas (como, por ejemplo, la catalogación de metadatos de archivos, la restauración de archivos y la reconfiguración de IP), las credenciales deben establecerse para la máquina virtual asociada. Especifique el nombre de usuario y la contraseña, y asegúrese de que se puede acceder a la máquina virtual desde el dispositivo de IBM Spectrum Protect Plus a través del DNS o del nombre de host.

La política de seguridad predeterminada utiliza el protocolo NTLM de Windows y la identidad de usuario respeta el formato *dominio\nombre* predeterminado si la máquina virtual Hyper-V está conectada a un dominio. El formato *administrador_local* se utiliza si el usuario es un administrador local.

6. Para resolver problemas de conexión con una máquina virtual de hipervisor, utilice la función **Probar**.

   La función **Probar** verifica la comunicación con la máquina virtual y prueba los valores DNS entre el dispositivo IBM Spectrum Protect Plus y la máquina virtual. Para probar una conexión, seleccione una única máquina virtual y, a continuación, pulse **Seleccionar opciones**. Seleccione **Utilizar usuario existente** y seleccione un nombre de usuario y una contraseña especificados anteriormente para el proveedor. El botón **Probar** se muestra a la derecha y el botón **Guardar** en la sección **Opciones**. Pulse **Probar**.
7. Pulse **Guardar**.
8. Para configurar opciones adicionales, pulse el campo **Opciones de política** que está asociado al trabajo en la sección **Estado de política de SLA**. Establezca las opciones de política adicionales:

   Scripts anteriores y scripts posteriores

   Ejecute un script anterior o script posterior. Los scripts anteriores y posteriores son scripts que se pueden ejecutar antes o después de que se ejecute un trabajo en el nivel de trabajo. Las máquinas basadas en Windows soportan scripts Batch y PowerShell mientras que las máquinas basadas en Linux soportan scripts de shell.

   En la sección **Script anterior** o **Script posterior**, seleccione un script cargado y un servidor de script donde se va a ejecutar el script. Los scripts y los servidores de scripts se configuran en la página **Configuración del sistema** > **Script**.

   Para seguir ejecutando el trabajo si falla el script asociado con el trabajo, seleccione **Continuar trabajo/tarea en error de script**.

   Cuando esta opción está habilitada, si un script anterior o un script posterior completa el proceso con un código de retorno distinto de cero, se intenta la operación de copia de seguridad o restauración y se informa sobre el estado de la tarea previa del script anterior como COMPLETADO. Si un script posterior se completa con un código de retorno distinto de cero, se informa sobre el estado de la tarea del script posterior como COMPLETADO.

   Cuando esta opción está inhabilitada, no se intenta realizar la copia de seguridad o la restauración, y se informa sobre el estado de la tarea del script anterior o del script posterior como FALLIDO.

   Ejecutar inventario antes de la copia de seguridad

   Ejecute un trabajo de inventario y capture los datos más recientes de los recursos seleccionados antes de iniciar el trabajo de copia de seguridad.

   Excluir recursos

   Excluya recursos específicos del trabajo de copia de seguridad mediante patrones de exclusión únicos o múltiples. Los recursos se pueden excluir mediante una coincidencia exacta o con asteriscos comodín especificados antes del patrón (* test) o después del patrón (test *).

   También se admiten varios comodines de asterisco en un único patrón. Los patrones admiten caracteres alfanuméricos estándar, así como los siguientes caracteres especiales:-_ y *.

   Separe varios con un punto y coma.

   Forzar copia de seguridad completa de los recursos

   Fuerce operaciones de copia de seguridad base para máquinas virtuales o bases de datos específicas en la definición de trabajo de copia de seguridad. Separe varios recursos con un punto y coma.
9. Para guardar las opciones adicionales que haya configurado, pulse **Guardar**.

Qué hacer a continuación

Después de definir un trabajo de copia de seguridad, realice la acción siguiente:

Acción	Cómo
Cree una definición de trabajo de restauración de Hyper-V.	Consulte “Restauración de datos de Hyper-V” en la página 132.

Conceptos relacionados

“Configuración de scripts para las operaciones de copia de seguridad y restauración” en la página 261
Los scripts anteriores y posteriores son scripts que se pueden ejecutar antes o después de que los trabajos de copia de seguridad y restauración se ejecuten en el nivel de trabajo. Los scripts soportados incluyen scripts de shell para máquinas basadas en Linux y scripts Batch y PowerShell para máquinas basadas en Windows. Los scripts se crean localmente, se suben al entorno a través de la página **Script** y se aplican a continuación a las definiciones de trabajos.

Tareas relacionadas

“Inicio de trabajos” en la página 258
Puede ejecutar cualquier trabajo bajo demanda, incluso si el trabajo se ha establecido para que se ejecute en una planificación.

Restauración de datos de Hyper-V

Los trabajos de restauración de Hyper-V admiten los casos de ejemplo de Restauración de máquina virtual instantánea y Restauración de disco instantánea, que se crean automáticamente basándose en el origen seleccionado.

Antes de empezar

Complete las tareas siguientes:

- Asegúrese de que se ha ejecutado un trabajo de copia de seguridad de Hyper-V al menos una vez. Para obtener instrucciones, consulte “Copia de seguridad de datos de Hyper-V” en la página 128.
- Asegúrese de que el destino que tiene previsto utilizar para el trabajo de restauración esté registrado en IBM Spectrum Protect Plus. Este requisito se aplica a los trabajos de restauración que restauran los datos a los hosts o clústeres originales.
- Asegúrese de que los servicios de integración de Hyper-V más recientes están instalados.

  Para entornos de Microsoft Windows, consulteSistemas operativos invitados de Windows soportados para Hyper-V en Windows Server.

  Para entornos de Linux, consulte Máquinas virtuales Linux y FreeBSD soportadas para Hyper-V en Windows.
- Asegúrese de que los roles adecuados para las operaciones de restauración se asignan a los usuarios afectados. Otorgue a los usuarios acceso a los hipervisores y a las operaciones de copia de seguridad y restauración en el panel **Cuentas**. Los roles y los permisos asociados se asignan durante la creación de cuentas de usuario. Para obtener instrucciones, consulte Capítulo 13, “Gestión del acceso de usuarios”, en la página 303 y “Gestión de cuentas de usuario” en la página 311.
- La indexación de archivos de Windows y la restauración de archivos en volúmenes que residen en discos dinámicos no están soportadas.
- Cuando se realiza una restauración desde un archivado de IBM Spectrum Protect, los archivos se migrarán a una agrupación de transferencia desde la cinta antes del inicio del trabajo. Dependiendo del tamaño de la restauración, este proceso puede tardar varias horas.

Acerca de esta tarea

Si se selecciona un Disco duro virtual (VHDX) para un trabajo de restauración, IBM Spectrum Protect Plus presenta automáticamente opciones para un trabajo de Restauración de disco instantánea, que proporciona acceso de grabación instantáneo a los puntos de restauración de datos y aplicaciones.

Una instantánea de IBM Spectrum Protect Plus se correlaciona con un servidor de destino donde se puede acceder o copiar la instantánea cuando sea necesario. Todos los demás orígenes se restauran

mediante trabajos de restauración de la máquina virtual instantánea, que se pueden ejecutar en las modalidades siguientes:

Modalidad de prueba
La modalidad de prueba crea máquinas virtuales temporales para desarrollo, pruebas, verificación de instantáneas y verificación de recuperación tras desastre de una forma planificada y repetida sin que por ello afecte a los entornos de producción. Las máquinas de prueba se mantienen en funcionamiento mientras son necesarias para completar las pruebas y la verificación y luego se limpian. A través de redes delimitadas, puede establecer un entorno seguro para probar los trabajos sin interferir con las máquinas virtuales que se utilizan para la producción. Las máquinas virtuales que se crean en modalidad de prueba también reciben nombres e identificadores exclusivos para evitar conflictos dentro del entorno de producción.

Modalidad de clonación
La modalidad de clonación crea copias de máquinas virtuales para los casos de uso que requieren copias permanentes o de larga ejecución para la minería de datos o la duplicación de un entorno de prueba en una red delimitada. Las máquinas virtuales que se crean en modalidad de clonación también reciben nombres e identificadores exclusivos para evitar conflictos dentro del entorno de producción. Con la modalidad de clonación, debe tener en cuenta el consumo de recursos porque la modalidad de clonación crea máquinas virtuales permanentes o a largo plazo.

Modalidad de producción
La modalidad de producción permite la recuperación tras desastre en el sitio local desde el almacenamiento primario o un sitio remoto de recuperación tras desastre, sustituyendo las imágenes de máquina originales por las imágenes de recuperación. Todas las configuraciones se llevan a cabo como parte de la recuperación, incluidos los nombres e identificadores, y todos los trabajos de datos de copia asociados a la máquina virtual continúan ejecutándose.

Restricción: El paso de la modalidad de prueba a la modalidad de producción no está soportado en Hyper-V.

Procedimiento

Para definir un trabajo de restauración de Hyper-V, complete los pasos siguientes:

1. En el panel de navegación, pulse **Gestionar protección** > **Hipervisores** > **Hyper-V** > **Crear trabajo de restauración** para abrir el asistente "Restauración de instantáneas".

   Sugerencias:

   - También puede abrir el asistente "Restauración de instantáneas" pulsando **Trabajos y operaciones** > **Crear trabajo de restauración** > **Hyper-V**.
   - Para obtener un resumen en ejecución de las selecciones en el asistente "Restauración de instantáneas", mueva el cursor al icono de información en el panel de navegación del asistente.
   - Para omitir las páginas opcionales en el asistente, seleccione **Omitir pasos opcionales**.

2. En la página **Selección de origen**, lleve a cabo las acciones siguientes:
   a) Revise los orígenes disponibles, incluidas las máquinas virtuales (VM) y los discos virtuales (VDisks). Puede expandir un origen pulsando su nombre.

      También puede especificar todo o parte de un nombre en el recuadro **Buscar** para localizar las máquinas virtuales que coinciden con los criterios de búsqueda. Puede utilizar el carácter comodín (*) para representar todo o parte de un nombre. Por ejemplo, `vm2*` representa todos los recursos que comienzan con "vm2".

   b) Pulse el icono de signo más situado junto al elemento que desea añadir a la lista de restauración al lado de la lista de orígenes. Puede añadir más de un elemento del mismo tipo (MV o disco virtual).

      Para eliminar un elemento de la lista de restauración, pulse el icono de signo menos situado junto al elemento.

   c) Pulse **Siguiente**.

3. En la página **Instantánea de origen** , especifique la instancia de la máquina virtual o del disco virtual que desea restaurar. Complete los siguientes campos y pulse **Siguiente** para continuar. Algunos campos no se visualizan hasta que se selecciona un campo relacionado.

Opción	Descripción
Tipo de restauración	Seleccione el tipo de trabajo de restauración: **Bajo demanda** Ejecuta una operación de restauración puntual. **Recurrente** Crea un trabajo de restauración de punto en el tiempo repetitivo que se ejecuta en una planificación.
Tipo de ubicación de restauración	Seleccione un tipo de ubicación desde donde se restauran los datos: **Sitio** El sitio en el que se hizo la copia de seguridad de las instantáneas. El sitio se define en el panel **Configuración del sistema** > **Sitio**. **Descarga de la nube** El servidor de nube en el que se han descargado las instantáneas. El servidor de nube se define en el panel **Configuración del sistema** > **Almacenamiento de copia de seguridad** > **Cloud**. **Descarga del repositorio** El servidor de repositorio donde se han descargado las instantáneas. El servidor de repositorio se define en el panel **Configuración del sistema** > **Almacenamiento de copia de seguridad** > **Servidor de repositorio**. **Archivado de nube** El servidor de nube en el que se han archivado las instantáneas. El servidor de nube se define en el panel **Configuración del sistema** > **Almacenamiento de copia de seguridad** > **Cloud**. **Archivado de repositorio** El servidor de repositorio en el que se han archivado las instantáneas. El servidor de repositorio se define en el panel **Configuración del sistema** > **Almacenamiento de copia de seguridad** > **Servidor de repositorio**.
Seleccionar una ubicación	Si está restaurando datos desde un sitio, seleccione una de las siguientes ubicaciones de restauración: **Demo** El sitio de demostración desde el que se restauran las instantáneas. **Primario** La ubicación del sitio primario desde la que se restauran las instantáneas. **Secundario** La ubicación del sitio secundario desde la que se restauran las instantáneas. Si está restaurando datos desde un servidor de nube o de repositorio, seleccione un servidor en el menú **Seleccionar una ubicación**.
Selector de fecha	Para las operaciones de restauración bajo demanda, especifique un rango de fechas para mostrar las instantáneas disponibles dentro de ese rango.
Punto de restauración	Para las operaciones de restauración bajo demanda, seleccione una instantánea en la lista de instantáneas disponibles en el rango de datos seleccionado.
Utilizar el servidor vSnap alternativo para el trabajo de restauración	Si está restaurando datos desde un recurso de nube o un servidor de repositorio, seleccione este recuadro para especificar un servidor de vSnap alternativo y, a continuación, seleccione un servidor en el menú **Seleccionar vSnap alternativo**.

Opción	Descripción
	Cuando restaura datos desde un punto de restauración que se ha descargado o archivado en un servidor de repositorio o de recursos de nube, se utiliza un servidor vSnap como pasarela para completar la operación. De forma predeterminada, el servidor vSnap que se utiliza para completar la operación de restauración es el mismo servidor vSnap que se utiliza para completar las operaciones de copia de seguridad y de descarga. Para reducir la carga en el servidor vSnap, puede seleccionar un servidor vSnap alternativo para que sirva como pasarela.

4. En la página **Establecer destino** , elija la instancia que se va a restaurar para el origen seleccionado y pulse **Siguiente**:

   Host o clúster de Hyper-V original
   Seleccione esta opción para restaurar los datos en el host o clúster original.

   Host o clúster de Hyper-V alternativo
   Seleccione esta opción para restaurar los datos en un destino local que sea distinto del host o clúster original y, a continuación, seleccione la ubicación alternativa de los recursos disponibles.

   En el campo **Destino de carpeta de MV**, especifique la vía de acceso a carpeta de la máquina virtual en el almacén de datos de destino. Tenga en cuenta que el directorio se creará si no existe. Utilice "/" como carpeta de máquina virtual raíz del almacén de datos de destino.

5. En la página **Establecer almacén de datos**, lleve a cabo las acciones siguientes:

   - Si está restaurando datos en un clúster o host de Hyper-V alternativo, seleccione el almacén de datos de destino y haga clic en **Siguiente**.
   - Si está restaurando datos en el host o clúster ESX original, no es necesario que establezca un almacén de datos. Simplemente, haga clic en **Siguiente**.

6. En la página **Establecer red**, especifique los valores de red que desea utilizar para cada origen elegido y pulse **Siguiente**.

   - Si está restaurando datos en el host o clúster de Hyper-V original, especifique los valores de red siguientes:

     Permitir que el sistema defina la configuración de IP
     Seleccione esta opción para permitir que el sistema operativo defina la dirección IP de destino. Durante una operación de restauración en modalidad de prueba, la máquina virtual de destino recibe una nueva dirección MAC junto con un NIC asociado. En función del sistema operativo, se puede asignar una nueva dirección IP basándose en el NIC original de la máquina virtual o bien se puede asignar mediante DHCP. Durante una restauración en modalidad de producción, la restauración dirección MAC no cambia; por lo tanto, la dirección IP debe mantenerse.

     Utilizar la configuración de IP original
     Seleccione esta opción para restaurar al host o clúster original utilizando la configuración de la dirección IP predefinida. Durante la operación de restauración, la máquina virtual de destino recibe una nueva dirección MAC, pero la dirección IP se conserva.

   - Si está restaurando datos en un host o clúster Hyper-V alternativo, complete los pasos siguientes:

     a. En los campos **Producción** y **Prueba**, establezca las redes virtuales para la ejecución de trabajos de restauración de prueba y producción. Los valores de red de destino para entornos de producción y de prueba deben apuntar a diferentes ubicaciones para crear una red delimitada, que impide a las máquinas virtuales utilizadas para la realización de pruebas interferir con máquinas virtuales utilizadas para la producción. Las redes asociadas con las modalidades de prueba y producción se utilizarán cuando el trabajo de restauración se ejecute en la modalidad asociada.

     b. Establezca una dirección IP o una máscara de subred para que las máquinas virtuales se vuelvan a dirigir para casos de desarrollo, de prueba o de recuperación tras desastre. Los tipos

de correlación soportados incluyen IP a IP, IP a DHCP y subred a subred. Las máquinas virtuales que contienen múltiples NIC están soportadas.

Realice una de las acciones siguientes:

– Para permitir que el sistema operativo defina las subredes de destino y las direcciones IP, pulse **Utilizar direcciones IP y subredes definidas por el sistema para el SO invitado de máquina virtual en el destino**.

– Para utilizar las direcciones IP y subredes predefinidas, pulse **Utilizar direcciones IP y subredes originales para el SO invitado de máquina virtual en el destino**.

– Para crear una nueva configuración de correlación, seleccione **Añadir correlaciones para subredes y direcciones IP para el SO invitado de máquina virtual en el destino**, pulse **Añadir correlación** y especifique una subred o una dirección IP en el campo **Añadir dirección IP o subred de origen** .

Elija uno de los protocolos de red siguientes:

- Seleccione **DHCP** para seleccionar automáticamente una IP y la información de configuración relacionada si DHCP está disponible en el origen seleccionado.
- Seleccione **Estático** para especificar una subred o dirección IP específica, máscara de subred, pasarela y DNS. Los campos **Subred/Dirección IP**, **Máscara de subred** y **Pasarela** son campos necesarios. Si se especifica una subred como origen, también se debe especificar una subred como destino.

La reconfiguración de IP se omite para las máquinas virtuales si se utiliza una IP estática, pero no se encuentra ninguna correlación de subred adecuada, o si la máquina virtual de origen está apagada y hay más de un NIC asociado. En un entorno de Windows, si una máquina virtual utiliza solo DHCP, la recuperación de IP se omite para dicha máquina virtual. En un entorno de Linux, se presupone que todas las direcciones son estáticas y solo la correlación IP estará disponible.

7. En los **Métodos de restauración**, seleccione el método de restauración que se utilizará para las selecciones de origen. Establezca de forma predeterminada el trabajo de restauración de Hyper-V para que se ejecute en modalidad de prueba, producción o clonación. Una vez que se ha creado el trabajo, se puede ejecutar en modalidad de producción o clonación utilizando el panel **Sesiones de trabajo**. También puede cambiar el nombre de la máquina virtual restaurada especificando el nuevo nombre de máquina virtual en el campo **Renombrar VM (opcional)**. Pulse **Siguiente** para continuar.
8. Opcional: En la página **Opciones de trabajo (opcional)**, configure las opciones avanzadas y haga clic en **Siguiente**.

Hacer que el recurso de clonación de IA sea permanente
Habilite esta opción para mover el disco virtual a un almacenamiento permanente y para limpiar los recursos temporales. Esta acción se lleva a cabo iniciando una operación vMotion para los recursos en segundo plano. El destino de la operación vMotion es el almacén de datos de configuración de máquina virtual. El disco de Acceso instantáneo sigue estando disponible para las operaciones de lectura/escritura durante esta operación.

Encender después de la recuperación
Alterne el estado de alimentación de una máquina virtual después de que se ejecute una recuperación. Las máquinas virtuales se encienden en el orden en el que se recuperan, tal como se establece en el paso Origen.

Restricción: Las plantillas de máquina virtual restauradas no se pueden encender después de la recuperación.

Sobrescribir máquina virtual
Habilite esta opción para permitir que el trabajo de restauración sobrescriba la máquina virtual seleccionada. De forma predeterminada, esta opción está inhabilitada.

Continuar con la restauración incluso si falla
Alterne la recuperación de un recurso en una serie si falla la recuperación del recurso anterior. Si esta opción está inhabilitada, el trabajo de restauración se detiene en caso de que falle la recuperación de un recurso.

Ejecutar la limpieza inmediatamente en caso de anomalía del trabajo
Habilite esta opción para limpiar automáticamente los recursos asignados como parte de un trabajo de restauración si falla la recuperación de la máquina virtual.

Permitir sobrescribir y forzar la limpieza de las sesiones anteriores pendientes
Habilite esta opción para permitir que una sesión planificada de un trabajo de recuperación obligue a una sesión pendiente a limpiar los recursos asociados para que se pueda ejecutar la nueva sesión. Inhabilite esta opción para mantener en funcionamiento un entorno de prueba existente sin que se limpie.

Añadir sufijo al nombre de la máquina virtual
Escriba un sufijo para añadirlo a los nombres de las máquinas virtuales restauradas.

Agregar al principio el prefijo para el nombre de máquina virtual
Escriba un prefijo para añadirlo a los nombres de las máquinas virtuales restauradas. Pulse Guardar para guardar las opciones de política.

9. Opcional: En la página **Aplicar scripts**, elija las opciones de script siguientes y haga clic en **Siguiente**.
   - Seleccione **Script anterior** para seleccionar un script cargado, y un servidor de aplicaciones o de scripts donde se ejecuta el script anterior. Para seleccionar un servidor de aplicaciones en el que se va a ejecutar el script, desmarque el recuadro de selección **Utilizar servidor de scripts**. Vaya a la página **Configuración del sistema** > **Script** para configurar los scripts y los servidores de scripts.
   - Seleccione **Script posterior** para seleccionar un script cargado, y un servidor de aplicaciones o de scripts donde se ejecuta el script posterior. Para seleccionar un servidor de aplicaciones en el que se ejecuta el script, desmarque el recuadro de selección **Utilizar servidor de scripts**. Vaya a la página **Configuración del sistema** > **Script** para configurar los scripts y los servidores de scripts.
   - Seleccione **Continuar trabajo/tarea en error de script** para seguir ejecutando el trabajo cuando falle el script asociado al trabajo. Cuando esta opción está habilitada y el script anterior se completa con un código de retorno distinto de cero, el trabajo de copia de seguridad o restauración sigue ejecutándose y el estado de la tarea del script anterior devuelve `COMPLETADO`. Si un script posterior se completa con un código de retorno distinto de cero, el estado de la tarea del script posterior devuelve `COMPLETADO`. Cuando esta opción no está seleccionada, el trabajo de copia de seguridad o restauración no se ejecuta, y el estado de la tarea del script anterior o el script posterior devuelve un estado `FALLIDO`.
10. Realice una de las acciones siguientes en la página **Planificación** :
    - Para ejecutar un trabajo bajo demanda, pulse **Siguiente**.
    - Para configurar un trabajo recurrente, especifique un nombre para la planificación de trabajos y especifique la frecuencia y el momento en que se inicia el trabajo de restauración. Pulse **Siguiente**.
11. En la página **Revisar**, revise los valores del trabajo de restauración y pulse **Enviar** para crear el trabajo.

    Los trabajos bajo demanda se iniciarán inmediatamente; los trabajos recurrentes se iniciarán a la hora de inicio planificada.

Qué hacer a continuación

Una vez completado el trabajo, seleccione una de las opciones siguientes del menú **Acciones** en las secciones **Sesiones de trabajos** o **Clones activos** en el panel **Restaurar** :

Limpieza
Destruye la máquina virtual y limpia todos los recursos asociados. Como se trata de una máquina virtual temporal que se va a utilizar para realizar pruebas, todos los datos se pierden cuando se destruye la máquina virtual.

Clonar (migrar)
Migra la máquina virtual al almacén de datos y a la red virtual que se definen como la red de prueba.

Tareas relacionadas

"Copia de seguridad de datos de Hyper-V" en la página 128
Utilice un trabajo de copia de seguridad para realizar copias de seguridad de datos de Hyper-V con instantáneas.

"Adición de un servidor Hyper-V" en la página 126
Cuando se añade un servidor Hyper-V a IBM Spectrum Protect Plus, se captura un inventario del servidor, lo que permite completar los trabajos de copia de seguridad y restauración, así como los informes de ejecución.

Restauración de archivos

Recupere los archivos de las instantáneas creadas con los trabajos de copia de seguridad de IBM Spectrum Protect Plus. Los archivos se pueden restaurar a su ubicación original o a una ubicación alternativa.

Antes de empezar
Tenga en cuenta los procedimientos y consideraciones siguientes antes de restaurar un archivo:

- Revise los requisitos de almacenamiento e indexación de archivos en "Requisitos de indexación y restauración de archivos" en la página 27.
- Ejecute un trabajo de copia de seguridad con los metadatos de archivo de catálogo habilitados. Siga estas directrices:
  - Asegúrese de que las credenciales se establecen para la máquina virtual asociada, así como el destino de la máquina virtual alternativa mediante la opción Nombre de usuario de SO invitado y Contraseña de SO invitado en la definición de trabajo de copia de seguridad.
  - Asegúrese de que puede acceder a la máquina virtual desde el dispositivo de IBM Spectrum Protect Plus utilizando el DNS o el nombre de host. En un entorno Windows, la política de seguridad predeterminada utiliza el protocolo NTLM de Windows y la identidad de usuario respeta el formato *dominio\nombre* predeterminado si la máquina virtual Hyper-V está conectada a un dominio. El formato *administrador_local* se utiliza si el usuario es un administrador local.
  - Para que una restauración de archivos se complete correctamente, asegúrese de que el ID de usuario que se encuentra en la máquina de destino dispone de los permisos de propiedad necesarios para el archivo que se está restaurando. Si un archivo lo ha creado un usuario que es diferente del ID de usuario que está restaurando el archivo según las credenciales de seguridad de Windows, el trabajo de restauración de archivo no se ejecutará correctamente.

Acerca de esta tarea

Restricciones:

- Los sistemas de archivos de Windows cifrados no están soportados para la catalogación de archivos o la restauración de archivos.
- La indexación de archivos y la restauración de archivos no están soportadas en los puntos de restauración descargados en los recursos de nube o servidores de repositorio.
- Cuando se restauran archivos en un entorno ReFS (sistema de archivos resistente), las restauraciones de versiones más recientes de Windows Server a versiones anteriores no están soportadas. Por ejemplo, la restauración de un archivo de Windows Server 2016 a Windows Server 2012.
- La catalogación de archivos, restauraciones de copia de seguridad, en un momento específico y otras operaciones que invocan el agente de Windows no se ejecutarán correctamente si un administrador local no predeterminado se especifica como el **Nombre de usuario del SO invitado** cuando se define un trabajo de copia de seguridad. Un administrador local que no es el predeterminado es cualquier usuario que se haya creado en el sistema operativo invitado y al que se le haya otorgado el rol de administrador.

Esto ocurre si la clave de registro `LocalAccountTokenFilterPolicy` en `[HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System]` se establece en 0 o no se establece. Si el parámetro se establece en 0 o no se establece, un administrador no predeterminado local no puede interactuar con WinRM, que es el protocolo que IBM Spectrum Protect Plus utiliza para instalar el agente de Windows para la catalogación de archivos, enviar mandatos a este agente y obtener resultados de él.

Establezca la clave de registro de `LocalAccountTokenFilterPolicy` en 1 en el invitado de Windows el que se está realizado la copia de seguridad con la opción `Metadatos del archivo de catálogo` habilitada. Si la clave no existe, vaya a `[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System]` y añada una clave de registro de DWord llamada `LocalAccountTokenFilterPolicy` con un valor de 1.

Como ayuda para evitar problemas que pueden producirse por las diferencias de huso horario, utilice un servidor NTP para sincronizar los husos horarios entre recursos. Por ejemplo, puede sincronizar los husos horarios de las matrices de almacenamiento, de los hipervisores y los servidores de aplicaciones que están en el entorno.

Si los husos horarios no están sincronizados, podrían detectarse errores durante el registro de aplicaciones, la catalogación de metadatos, el inventario, la copia de seguridad o restauración o bien en trabajos de restauración de archivos. Para obtener más información sobre la identificación y la resolución problemas de desviación del temporizador, consulte Tiempo en derivaciones de máquina virtual debido a la derivación del temporizador de hardware

Consideraciones sobre Hyper-V

Solo los volúmenes de los discos SCSI son aptos para la catalogación de archivos y la restauración de archivos.

Consideraciones sobre Linux

Si los datos se encuentran en volúmenes LVM, el servicio *lvm2-lvmetad* debe estar inhabilitado porque puede interferir con la posibilidad de que IBM Spectrum Protect Plus monte y vuelva a firmar instantáneas de grupo de volúmenes o clones. Para inhabilitar el servicio, complete los pasos siguientes:

1. Ejecute los mandatos siguientes:

```
systemctl stop lvm2-lvmetad
```

```
systemctl disable lvm2-lvmetad
```

2. Edite `/etc/lvm/lvm.conf` y especifique el valor siguiente:

```
use_lvmetad = 0
```

Si los datos residen en sistemas de archivos XFS y la versión del paquete xfsprogs está entre 3.2.0 y 4.1.9, la restauración de archivos puede fallar por un problema conocido en xfsprogs que produce daños en un clon o un sistema de archivos de instantánea cuando se modifica su UUID. Para resolver este problema, actualice xfsprogs a la versión 4.2.0 o una superior. Para obtener más información, consulte Registros de informes de error Debian.

Procedimiento

Para restaurar un archivo, complete los pasos siguientes:

1. En el panel de navegación, pulse **Gestionar protección** > **Restauración de archivos**.
2. Escriba una serie de búsqueda para buscar un archivo por el nombre y, a continuación, pulse el icono de búsqueda  . Para obtener más información sobre el uso de la función de búsqueda, consulte Apéndice A, “Directrices de búsqueda”, en la página 321.
3. Opcional: Puede utilizar filtros para ajustar la búsqueda entre máquinas virtuales específicas, el rango de fechas en el que se ha protegido el archivo y los tipos de sistemas operativos de la máquina virtual.

Las búsquedas también se pueden limitar a una carpeta específica con el campo **Vía de acceso a carpeta**. El campo **Vía de acceso a carpeta** admite comodines. Escriba comodines al principio, en medio o al final de una serie. Por ejemplo, escriba `*Descargas` para buscar dentro de la carpeta `Descargas` sin escribir la vía de acceso anterior.

4. Para restaurar el archivo utilizando las opciones predeterminadas, pulse **Restaurar**. El archivo se restaura a su ubicación original.
5. Para editar las opciones antes de restaurar el archivo, pulse **Opciones**. Establezca las opciones de restauración de archivo.

   Sobrescribir archivo/carpeta existente

   Sustituya el archivo o la carpeta existente por el archivo o la carpeta restaurados.

   Destino

   Seleccione esta opción para sustituir el archivo o la carpeta existente por el archivo o la carpeta restaurados.

   Para restaurar el archivo a su ubicación original, seleccione **Restaurar archivos en la ubicación original**.

   Para restaurar a un destino local diferente de la ubicación original, seleccione **Restaurar archivos en la ubicación alternativa**. A continuación, seleccione la ubicación alternativa entre los recursos disponibles utilizando el menú de navegación o la función de búsqueda.

   Restricción: Un archivo se puede restaurar a una ubicación alternativa únicamente si se han establecido las credenciales para la máquina virtual alternativa con la opción **Nombre de usuario/ Contraseña del SO invitado** en la definición de trabajo de copia de seguridad.

   Especifique la vía de acceso a la carpeta de la máquina virtual del destino alternativo en el campo **Carpeta de destino**. Si el directorio no existe, se creará.

   Pulse **Guardar** para guardar las opciones.
6. Para restaurar el archivo mediante las opciones definidas, pulse **Restaurar**.

Tareas relacionadas

“Copia de seguridad de datos de VMware” en la página 107
Utilice un trabajo de copia de seguridad para realizar una copia de seguridad de recursos de VMware, tales como máquinas virtuales, almacenes de datos, carpetas, vApps y centros de datos con instantáneas.

“Restauración de datos de VMware” en la página 116
Los trabajos de restauración de VMware admiten los casos de ejemplo de Restauración de máquina virtual instantánea y Restauración de disco instantánea, que se crean automáticamente basándose en el origen seleccionado.

Capítulo 8. Protección de aplicaciones

Debe registrar las aplicaciones de base de datos que desea proteger en IBM Spectrum Protect Plus y, a continuación, crear trabajos para realizar copias de seguridad de las bases de datos y de los recursos que están asociados con las aplicaciones y restaurarlos.

Nota: IBM Spectrum Protect Plus puede crear carpetas en servidores de aplicaciones cuando las aplicaciones están registradas en SPP. Las carpetas creadas por IBM Spectrum Protect Plus deberán permanecer para que el producto funcione correctamente y no se deben eliminar. Si es necesario eliminar una carpeta creada por SPP, elimine el registro de la aplicación de SPP. SPP realizará una limpieza de las carpetas asociadas con el registro.

Db2

Tras añadir correctamente las instancias de IBM Db2 a IBM Spectrum Protect Plus, puede empezar a proteger los datos de Db2. Cree políticas de acuerdos de nivel de servicio (SLA) para realizar copias de seguridad y mantener los datos Db2.

Asegúrese de que el entorno de Db2 cumple los requisitos del sistema. Para obtener más información, consulte “Requisitos de Db2” en la página 34.

Consejo: Si los datos de Db2 se almacenan en un entorno de varias particiones con varios host, puede proteger los datos de Db2 en cada host. Cada host del entorno multiparticionado se debe añadir a IBM Spectrum Protect Plus para que se detecten todas las instancias y bases de datos para la protección. Para obtener más información, consulte “Adición de un servidor de aplicaciones de Db2” en la página 144.

Requisitos previos para Db2

Se deben cumplir todos los requisitos previos para servidor de aplicaciones Db2 de IBM Spectrum Protect Plus antes de empezar a proteger los recursos de Db2 con IBM Spectrum Protect Plus.

Los requisitos para servidor de aplicaciones Db2 de IBM Spectrum Protect Plus están disponibles aquí, Requisitos de Db2.

Requisitos previos de espacio

Asegúrese de que tiene suficiente espacio en el sistema de gestión de bases de datos de Db2, en los grupos de volúmenes para la operación de copia de seguridad y en los volúmenes de destino para copiar archivos durante la operación de restauración. Para obtener más información sobre los requisitos de espacio, consulte Requisitos de espacio para la protección de Db2 . Cuando restaura datos a una ubicación alternativa, asigne volúmenes dedicados adicionales para los procesos de copia y restauración. Las vías de acceso a datos para espacios de tabla y registros en el host de destino son las mismas que las vías de acceso del host original. Esta configuración es necesaria para permitir la copia de datos desde el vSnap montado en el host de destino. Asegúrese de que se permiten directorios de base de datos locales dedicados para cada base de datos en la configuración de volumen.

Entornos multiparticionados de Db2

Para proteger las bases de datos multiparticionadas de Db2, la modalidad de copia de seguridad de ACS debe establecerse en modalidad paralela. Para ejecutar el proceso de copia de seguridad en paralelo de las particiones del entorno de Db2, asegúrese de que se cumple uno de los requisitos previos siguientes:

- La variable de registro de Db2 **DB2_PARALLEL_ACS** está establecida en YES, por ejemplo: **db2set DB2_PARALLEL_ACS=**YES.
- La variable de registro de Db2 **DB2_WORKLOAD** está establecida en SAP.

Restricción: La variable de registro **DB2_PARALLEL_ACS** solo está disponible en determinados niveles de fixpack de Db2. Si **DB2_PARALLEL_ACS** no está disponible en su versión, puede optar por cambiar **DB2_WORKLOAD** a SAP.

Más requisitos de configuración

Asegúrese de que el entorno de Db2 esté configurado para cumplir los criterios siguientes:

- El registro de archivado de Db2 se ha activado y Db2 está en modalidad recuperable.
- Asegúrese de que el tamaño de archivo efectivo **`ulimit`** -f para el usuario del agente de IBM Spectrum Protect Plus y el usuario de instancia de Db2 , esté establecido en unlimited. De forma alternativa, establezca el valor en un valor suficientemente alto para permitir la copia de los archivos de base de datos más grandes en los trabajos de copia de seguridad y restauración. Si cambia el valor de **`ulimit`**, reinicie la instancia de Db2 para finalizar la configuración.
- Si está ejecutando IBM Spectrum Protect Plus en un entorno de AIX o Linux, asegúrese de que la versión de sudo instalada esté en el nivel recomendado. Para obtener más información, consulte la nota técnica 2013790. A continuación, establezca privilegios sudo tal como se describe en "Establecimiento de privilegios sudo para Db2" en la página 144.
- En un entorno Linux, asegúrese de que el paquete del programa de utilidad de Linux `util-linux-ng` o el paquete `util-linux` es actual.
- Los caracteres Unicode en los nombres de vía de acceso al archivo no pueden ser manejados por IBM Spectrum Protect Plus. Todos los nombres deben estar en ASCII.
- Los espacios de tablas de base de datos, los registros en línea y el directorio de bases de datos local pueden estar en uno o varios volúmenes lógicos dedicados gestionados por LVM2 o por JFS2. Para ver los dos ejemplos de diseño, consulte las imágenes siguientes. En la primera imagen, se muestran dos tipos de grupos de volúmenes. En la segunda imagen, todos los volúmenes para datos y registros se encuentran en un grupo de volúmenes.

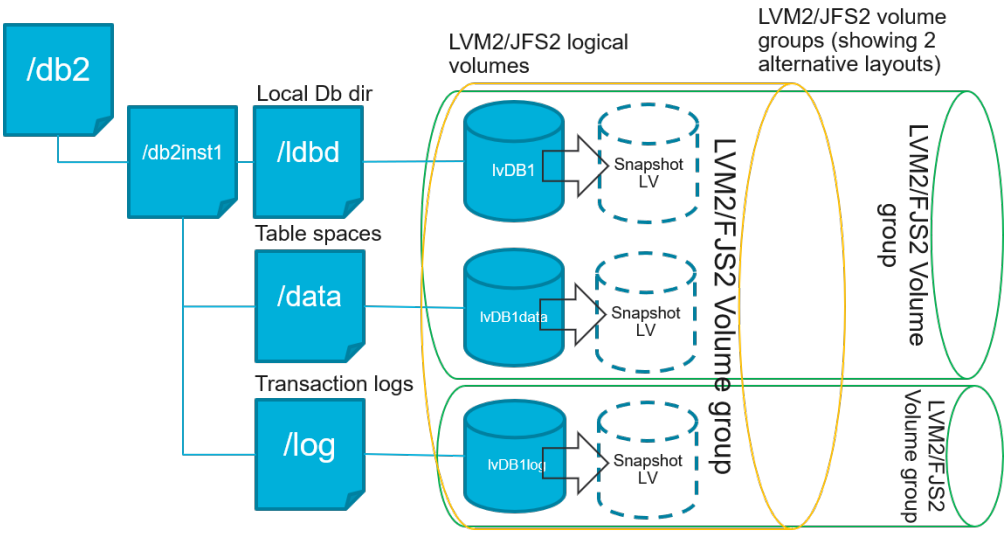


Figura 13. Ejemplos de diseño de volúmenes lógicos

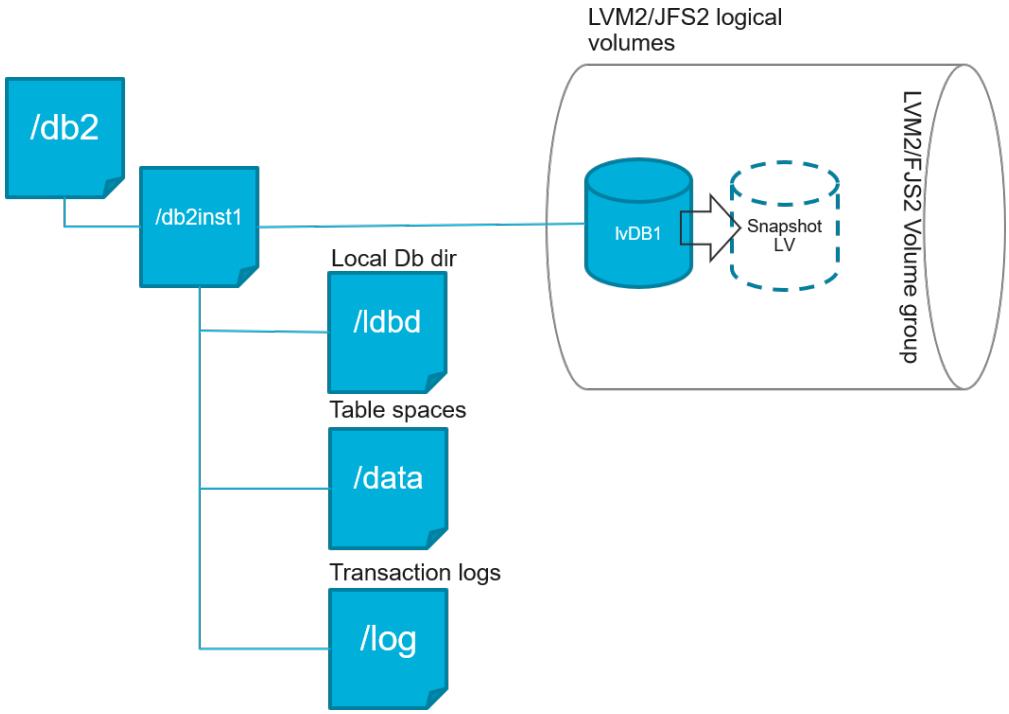


Figura 14. Ejemplo de diseño de volumen lógico único

- Asegúrese de que la configuración del volumen lógico de Db2 no incluya puntos de montaje anidados.

Requisitos de espacio para la protección de Db2

Antes de empezar a hacer una copia de seguridad de las bases de datos de Db2, asegúrese de tener suficiente espacio de disco libre en los hosts de destino y de origen y en el repositorio de vSnap. Se necesita espacio de disco libre adicional en los grupos de volúmenes en el host de origen para crear instantáneas temporales del Gestor de volúmenes lógicos (LVM) de los volúmenes lógicos en los que se almacenan los archivos de base de datos y de registro de Db2. Para crear instantáneas de LVM de una base de datos Db2 protegida, asegúrese de que los grupos de volúmenes con los datos de Db2 tengan suficiente espacio libre.

Instantáneas de LVM

Las instantáneas de LVM son copias de un punto en el tiempo específico de los volúmenes lógicos de LVM. Son instantáneas de espacio eficiente con las actualizaciones de datos cambiadas del volumen lógico de origen. Las instantáneas de LVM se crean en el mismo grupo de volúmenes que el volumen lógico de origen. El agente de IBM Spectrum Protect Plus Db2 utiliza instantáneas de LVM para crear una copia coherente y puntual de la base de datos de Db2.

El agente de IBM Spectrum Protect Plus Db2 crea una instantánea de LVM que, a continuación, se monta y se copia en el repositorio de vSnap. La duración de la operación de copia de archivos depende del tamaño de la base de datos de Db2. Durante la copia de archivos, la aplicación de Db2 permanece totalmente en línea. Después de que finalice la operación de copia de archivos, el agente de IBM Spectrum Protect Plus Db2 elimina las instantáneas de LVM en una operación de limpieza.

En el caso de AIX , no pueden existir más de 15 instantáneas para cada sistema de archivos JFS2. Las instantáneas de JFS2 internas y externas no pueden existir simultáneamente para el mismo sistema de archivos. Asegúrese de que no existen instantáneas internas en los volúmenes de JFS2 ya que estas instantáneas pueden provocar problemas cuando el agente de IBM Spectrum Protect Plus Db2 está creando instantáneas externas.

Para cada volumen lógico de instantánea LVM o JFS2 que contiene datos, permita al menos un 10 por ciento de su tamaño como espacio de disco libre en el grupo de volúmenes. Si el grupo de volúmenes

tiene suficiente espacio libre de disco, el agente de IBM Spectrum Protect Plus Db2 reserva hasta el 25 por ciento del tamaño de volumen lógico de origen para el volumen lógico de la instantánea.

LVM2 y JFS2
Cuando se ejecuta una operación de copia de seguridad de Db2, Db2 solicita una instantánea. Esta instantánea se crea en un sistema de gestión de volúmenes lógicos (LVM) o en un sistema de archivos de diario (JFS) para cada volumen lógico con datos o registros para la base de datos seleccionada. En sistemas Linux, los volúmenes lógicos se gestionan en LVM2 con mandatos `lvm2`. En AIX, los volúmenes lógicos se gestionan en JFS2 y se crean con el mandato de instantánea JFS2 como instantáneas externas.

Una instantánea de LVM2 o JFS2 basada en software se toma como un nuevo volumen lógico en el mismo grupo de volúmenes. Los volúmenes de instantánea se montan temporalmente en la misma máquina que ejecuta la instancia de Db2 de modo que se puedan transferir al repositorio de vSnap.

En el sistema operativo Linux el gestor de volúmenes LVM2 almacena la instantánea de un volumen lógico dentro del mismo grupo de volúmenes. En el sistema operativo AIX el gestor de volúmenes JFS2 almacena la instantánea de un volumen lógico dentro del mismo grupo de volúmenes. Para ambos, debe haber suficiente espacio en la máquina para almacenar el volumen lógico. El volumen lógico crece en tamaño a medida que los datos cambian en el volumen de origen mientras existe la instantánea. En entornos multiparticionados, cuando varias particiones comparten el mismo volumen, se crea una instantánea adicional del volumen para cada partición. Asegúrese de que el grupo de volúmenes tenga suficiente espacio libre para las instantáneas necesarias.

Establecimiento de privilegios sudo para Db2
Para utilizar IBM Spectrum Protect Plus para proteger los datos, debe instalar la versión necesaria del programa sudo. Para el servidor de aplicaciones de Db2, debe configurar sudo de una forma específica que pueda ser distinta de otros servidores de aplicaciones.

Antes de empezar

Para determinar la versión correcta de sudo que se va a instalar, consulte la nota técnica 2013790.

Acerca de esta tarea

Configure un usuario agente de IBM Spectrum Protect Plus dedicado con los privilegios de superusuario necesarios para sudo. Esta configuración permite que el usuario agente ejecute mandatos sin una contraseña.

Procedimiento

1. Cree un usuario de servidor de aplicaciones emitiendo el mandato siguiente:

   ```
   useradd -m <agent>
   ```

   donde `agent` especifica el nombre del usuario agente de IBM Spectrum Protect Plus.
2. Establezca una contraseña para el nuevo usuario emitiendo el mandato siguiente:

   ```
   passwd <agent>
   ```
3. Para habilitar privilegios de superusuario para el usuario agente, establezca el valor `!requiretty`. Al final del archivo de configuración sudo, añada las líneas siguientes:

   ```
   Defaults:<agent> !requiretty

   <agent> ALL=(ALL) NOPASSWD:ALL
   ```

   Si el archivo sudoers está configurado para importar configuraciones de otro directorio, por ejemplo, `/etc/sudoers.d`, puede añadir las líneas en el archivo adecuado de ese directorio.

Adición de un servidor de aplicaciones de Db2

Para empezar a proteger los datos de Db2, debe añadir la dirección de host en la que se encuentran las instancias de Db2. Puede repetir el procedimiento para añadir cada host que desee proteger con IBM

Spectrum Protect Plus. Si el entorno de Db2 es multiparticionado con varios hosts, debe añadir cada host a IBM Spectrum Protect Plus.

Acerca de esta tarea

Para añadir un servidor de aplicaciones de Db2 a IBM Spectrum Protect Plus, debe tener la dirección host de la máquina.

Procedimiento

1. En la navegación, expanda **Gestionar protección** > **Aplicaciones** > **Db2**.
2. En la ventana **Db2**, haga clic en **Gestionar servidores de aplicaciones** y pulse **Añadir servidor de aplicaciones** para añadir la máquina host.

Figura 15. Adición de un agente de Db2

3. En la sección **Propiedades de aplicación**, especifique la dirección de host.
4. Elija si desea especificar un usuario o bien utilice una clave SSH.
   - Si ha seleccionado especificar un usuario, seleccione un usuario existente o especifique un ID de usuario y una contraseña.
   - Si utiliza una clave SSH, elija la clave del menú.

Nota: El usuario debe disponer de privilegios sudo configurados.

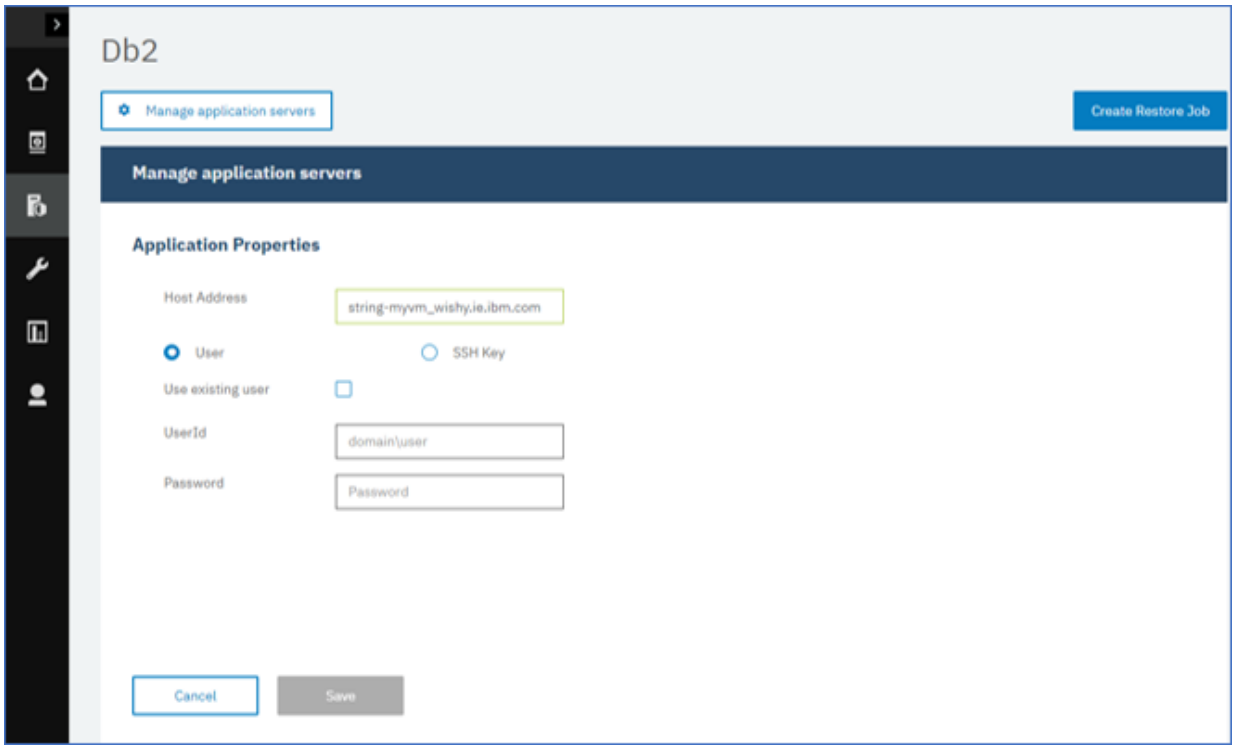


Figura 16. Gestión de usuarios agentes

Consejo:

Las instancias de Db2 encontradas se listan para cada host. Si la instancia de Db2 está particionada, esta información se lista con la máquina host y los números de las particiones. Para una Característica

de particionamiento de base de datos (DPF) de varios hosts, la instancia de Db2 se visualiza como una única unidad.

5. Guarde el formulario, repita los pasos para añadir otros servidores de aplicaciones de Db2 a IBM Spectrum Protect Plus.

   Si los datos de Db2 están en un entorno multiparticionado con varios hosts, debe añadir cada host. Repita el procedimiento para cada host de Db2.

Qué hacer a continuación

Después de añadir los servidores de aplicaciones de Db2 a IBM Spectrum Protect Plus, se ejecuta automáticamente un inventario en cada servidor de aplicaciones para detectar las bases de datos relevantes en esas instancias.

Para verificar si se han añadido las bases de datos, revise el registro de trabajo. Vaya a **Trabajos y operaciones**. Pulse la pestaña **Trabajos en ejecución** y busque la entrada de registro Inventario de servidor de aplicaciones más reciente.

Los trabajos completados se muestran en la pestaña **Historial de trabajos**. Puede utilizar la lista **Ordenar por** para ordenar los trabajos en función de la hora de inicio, el tipo, el estado, el nombre del trabajo o la duración. Utilice el campo **Buscar por nombre** para buscar trabajos por nombre. Puede utilizar asteriscos como caracteres comodín en el nombre.

Deben detectarse bases de datos para asegurarse de que se pueden proteger. Para obtener instrucciones sobre cómo ejecutar un inventario, consulte Detección de recursos de Db2.

Detección de recursos de Db2

Después de añadir servidores de aplicaciones de IBM Db2 a IBM Spectrum Protect Plus, se ejecuta automáticamente un inventario para detectar todas las instancias y bases de datos de Db2. El inventario detecta, enumera y almacena todas las bases de datos de Db2 para el host seleccionado, y hace que las bases de datos estén disponibles para la protección con IBM Spectrum Protect Plus.

Antes de empezar

Asegúrese de que ha añadido los servidores de aplicaciones de Db2 a IBM Spectrum Protect Plus. Para obtener instrucciones, consulte Adición de un servidor de aplicaciones de Db2.

Acerca de esta tarea

Se listan todas las particiones de Db2 que se encuentran en el inventario para la instancia de Db2. Las particiones se listan por el número de partición para cada host añadido al nombre de host de la tabla **Instancias**.

Procedimiento

1. En el panel de navegación, expanda **Gestionar protección** > **Aplicaciones** > **Db2**

   Consejo: Para añadir más instancias de Db2 al panel **Instancias**, siga las instrucciones que se indican en Adición de un servidor de aplicaciones de Db2.
2. Pulse **Ejecutar inventario**.

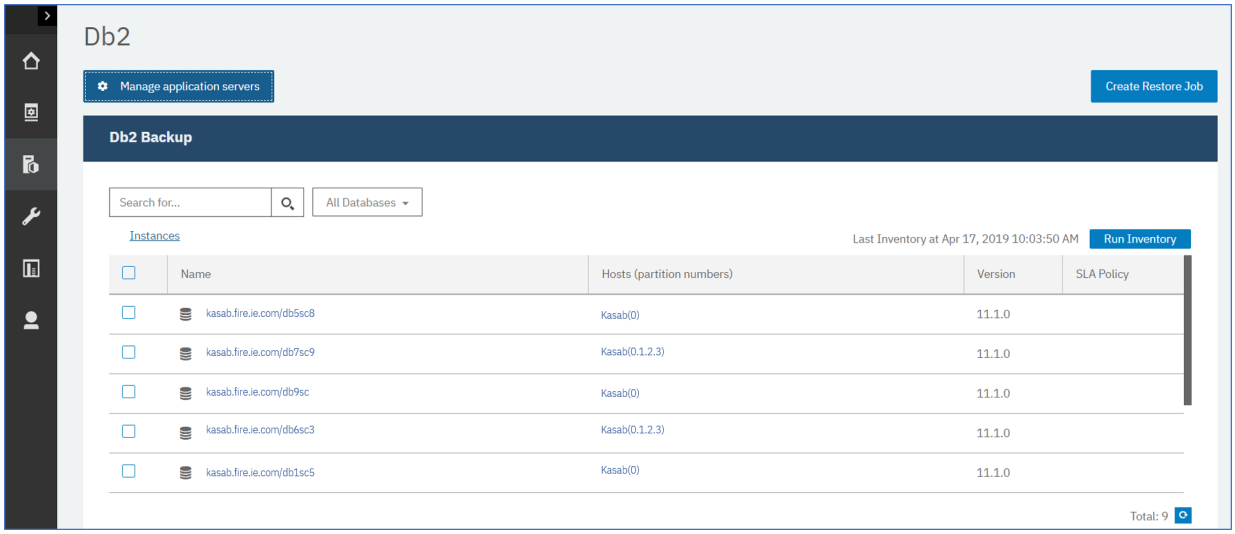


Figura 17. Detección de recursos de Db2

Cuando se ejecuta el inventario, el botón cambia para mostrar **Inventario en curso**. Puede ejecutar un inventario en cualquier servidor de aplicaciones disponible, pero solo puede ejecutar un proceso de inventario a la vez.

Para ver el registro de trabajo, vaya a **Trabajos y operaciones**. Pulse la pestaña **Trabajos en ejecución** y busque la entrada de registro Inventario de servidor de aplicaciones más reciente.

Los trabajos completados se muestran en la pestaña **Historial de trabajos**. Puede utilizar la lista **Ordenar por** para ordenar los trabajos en función de la hora de inicio, el tipo, el estado, el nombre del trabajo o la duración. Utilice el campo **Buscar por nombre** para buscar trabajos por nombre. Puede utilizar asteriscos como caracteres comodín en el nombre.

3. Pulse en una instancia para abrir una vista que muestre las bases de datos que se han detectado para dicha instancia. Si falta alguna de las bases de datos en la lista **Instancias**, compruebe el servidor de aplicaciones de Db2 y vuelva a ejecutar el inventario. En algunos casos, determinadas bases de datos se marcan como no admisibles para la copia de seguridad; pase el cursor por encima de la base de datos para desvelar la razón.

   Consejo: Para volver a la lista de instancias, pulse el hipertexto **Instancias** en el panel **Copia de seguridad de Db2**.

Qué hacer a continuación

Para empezar a proteger las bases de datos de Db2 que están catalogadas en la instancia seleccionada, aplique una política de acuerdo de nivel de servicio (SLA) a la instancia. Para obtener instrucciones sobre cómo establecer una política de SLA, consulte Definición de una política de SLA.

Prueba de conexión de Db2

Después de añadir un servidor de aplicaciones de Db2, puede probar la conexión. La prueba verifica la comunicación con los valores del servidor y de DNS entre IBM Spectrum Protect Plus y el servidor de Db2. También comprueba los permisos sudo para el usuario.

Procedimiento

1. En el panel de navegación, pulse **Gestionar protección** > **Aplicaciones** > **Db2**.
2. En la ventana **Db2** , pulse **Gestionar servidores de aplicaciones** y seleccione la **Dirección de host** que desea probar.

   Se muestra una lista de los servidores de aplicaciones de Db2 que están disponibles.
3. Pulse **Acciones** y seleccione **Probar** para iniciar las pruebas de verificación de las conexiones y los valores físicos, remotos y operativos del sistema.

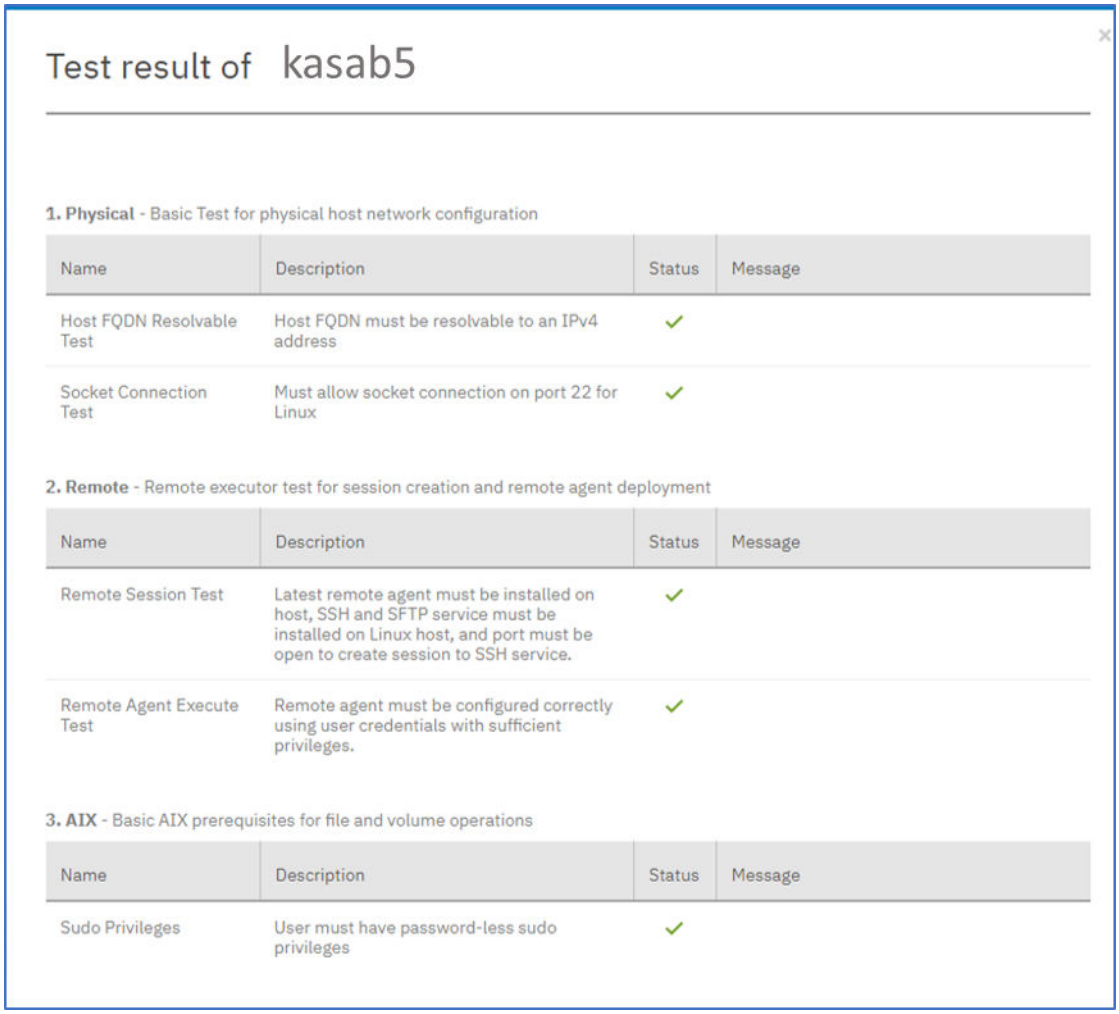


Figura 18. Probar la conexión

El informe de prueba muestra una lista de las pruebas. Consta de una prueba de la configuración de red de host física y pruebas de instalación del servidor remoto en el host, que comprueba el SSH y SFTP en el host. La tercera prueba comprueba los requisitos previos del sistema operativo y los privilegios sudo correctos.

4. Pulse **Aceptar** para cerrar la prueba y elija volver a ejecutar la prueba después de arreglar las pruebas fallidas.

Copia de seguridad de datos de Db2

Defina trabajos de copia de seguridad de Db2 regulares con opciones para ejecutar y crear copias de seguridad para proteger los datos. Puede habilitar la copia de seguridad continua de los registros de archivado para que pueda restaurar una copia puntual con opciones de recuperación en avance si es necesario.

Antes de empezar

Durante la copia de seguridad inicial, IBM Spectrum Protect Plus crea un nuevo volumen de vSnap y una unidad compartida de NFS. Durante las copias de seguridad incrementales, se reutiliza el volumen creado previamente. El agente Db2 de IBM Spectrum Protect Plus monta la unidad compartida en el servidor de Db2 donde se va a completar la copia de seguridad.

Revise los procedimientos y las consideraciones siguientes antes de crear una definición de trabajo de copia de seguridad:

- Añada los servidores de aplicaciones de los que desea realizar una copia de seguridad. Para obtener información sobre el procedimiento, consulte Adición de un servidor de aplicaciones de Db2.
- Configure una política de acuerdo de nivel de servicio (SLA). Para obtener información sobre el procedimiento, consulte Definición de un trabajo de copia de seguridad de Acuerdo de nivel de servicio.
- Para que un usuario pueda implementar operaciones de copia de seguridad y restauración de IBM Spectrum Protect Plus, deben asignarse roles y grupos de recursos al usuario. Otorgue a los usuarios acceso a los recursos y a las operaciones de copia de seguridad y restauración mediante el panel **Cuentas**. Para obtener más información, consulte Gestión del acceso de usuario.
- Los trabajos de inventario no se deben planificar para ejecutarse al mismo tiempo que los trabajos de copia de seguridad.
- Evite configurar copias de seguridad de registros para una única base de datos de Db2 con muchos trabajos de copia de seguridad. Si se añade una sola base de datos de Db2 a varias definiciones de trabajo con la copia de seguridad de registro habilitada, una copia de seguridad de registro de un trabajo puede truncar un registro antes de que se realice una copia de seguridad de él en el siguiente trabajo. Esto puede provocar que fallen los trabajos de restauración de un momento específico.

Procedimiento

1. En el menú de navegación, expanda **Gestionar protección** > **Aplicaciones** > **Db2**.
2. Seleccione una instancia o base de datos para realizar la copia de seguridad eligiendo una de las acciones siguientes:
   - Seleccione una instancia completa en el panel **Instancias** pulsando el recuadro de selección situado junto al nombre de instancia. Cualquier base de datos añadida a esta instancia se asigna automáticamente a la política de SLA que elija.
   - Seleccione una base de datos específica en una instancia pulsando el nombre de la instancia y eligiendo una base de datos de la lista de bases de datos de dicha instancia.

   Cada elemento del panel **Instancias** aparece listado por la instancia o el nombre de base de datos, la política de SLA aplicada y la elegibilidad de la copia de seguridad de registro.
3. Pulse **Seleccionar opciones** para habilitar o inhabilitar la copia de seguridad de registro y para especificar los streams paralelos para minimizar el tiempo que se tarda para el traslado de datos de gran tamaño en la operación de copia de seguridad. Pulse **Guardar** para confirmar las opciones.

   Seleccione **Habilitar copia de seguridad del registro** para realizar una copia de seguridad de los registros de archivado, lo que permite opciones de restauración de punto en el tiempo y opciones de recuperación. Para obtener información sobre los valores de copia de seguridad de registro de Db2, consulte Copias de seguridad de registro.

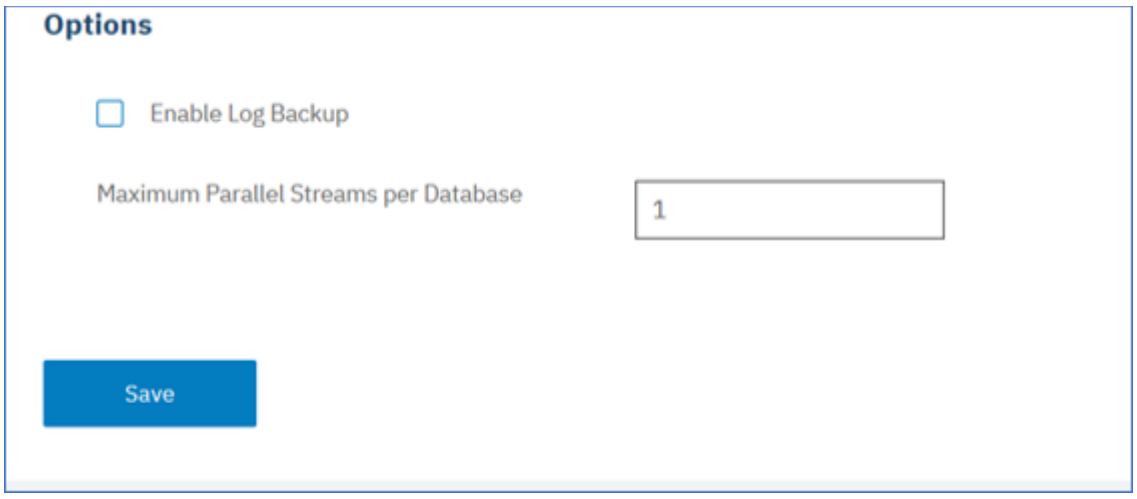


Figura 19. Panel Copia de seguridad con la opción Habilitar copia de seguridad de registro

Cuando se guardan las opciones, estas opciones se utilizan para todos los trabajos de copia de seguridad de esta base de datos o de esta instancia tal como se ha seleccionado.

4. Vuelva a seleccionar la base de datos o la instancia y pulse **Seleccionar política de SLA** para elegir una política de SLA para dicha base de datos o instancia.
5. Guarde las opciones de SLA.

   Para definir un nuevo SLA para editar una política existente con las tasas de retención y frecuencia personalizadas, seleccione **Gestionar protección** > **Descripción general de política**. En el panel **Políticas de SLA**, pulse **Añadir política de SLA** y defina las preferencias de política.

Qué hacer a continuación

Cuando se guarda la política de SLA, si lo desea, puede ejecutar una copia de seguridad bajo demanda en cualquier momento pulsando **Acciones** junto al nombre de la política y seleccionando **Iniciar**. El estado del registro cambia para mostrar que la copia de seguridad es En `ejecución`.

Definición de un trabajo de copia de seguridad de acuerdo de nivel de servicio

Después de que las bases de datos de Db2 se listen para cada una de las instancias de Db2, seleccione y aplique una política de acuerdo de nivel de servicio (SLA) para empezar a proteger los datos.

Procedimiento

1. En el menú de navegación, expanda **Gestionar protección** > **Aplicaciones** > **Db2**.
2. Seleccione una instancia de Db2 para realizar una copia de seguridad de todos los datos de dicha instancia o haga clic en el nombre de instancia para ver las bases de datos disponibles para realizar la copia de seguridad. A continuación, puede seleccionar bases de datos individuales en la instancia de Db2 a la que desea hacer copia de seguridad.

   Elija realizar una copia de seguridad de una instancia completa con todos los datos asociados, o bien puede elegir realizar una copia de seguridad de una o varias bases de datos.

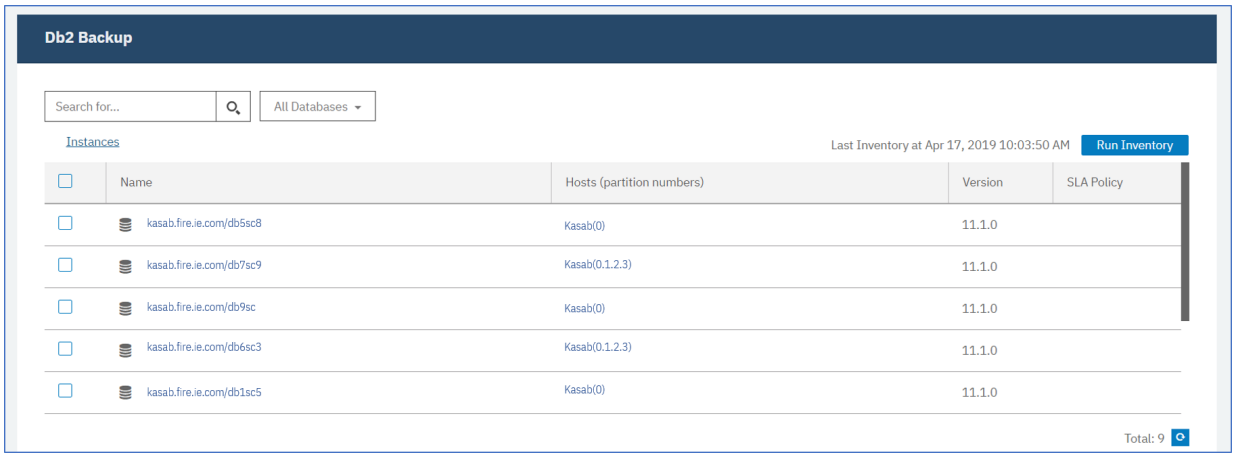


Figura 20. Panel de copia de seguridad de Db2 que instancias

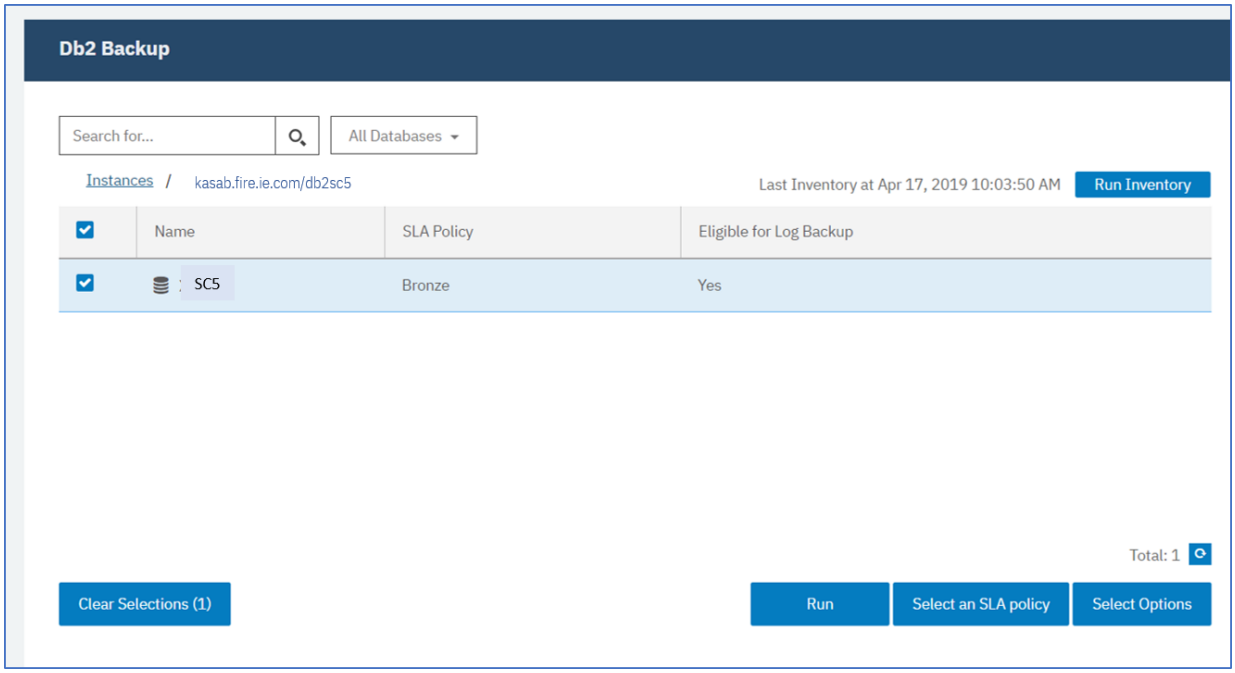


Figura 21. Panel de copia de seguridad de Db2 que muestra bases de datos en una instancia

3. Pulse **Seleccionar política de SLA** y elija una política de SLA, **Oro**, **Plata** o **Bronce**. Guarde su selección.

   Las opciones predefinidas de Oro, Plata y Bronce tienen cada una frecuencias diferentes y velocidades de retención diferentes. Puede crear una política de SLA personalizada o editar una política existente, desplazándose hasta **Descripción general de política** > **Políticas de SLA**.
4. Pulse **Seleccionar opciones** para definir opciones para la copia de seguridad, como por ejemplo, habilitar las copias de seguridad de registro para futuras opciones de recuperación y especificar los streams paralelos para reducir el tiempo que se tarda en realizar copias de seguridad de bases de datos grandes. Guarde los cambios.

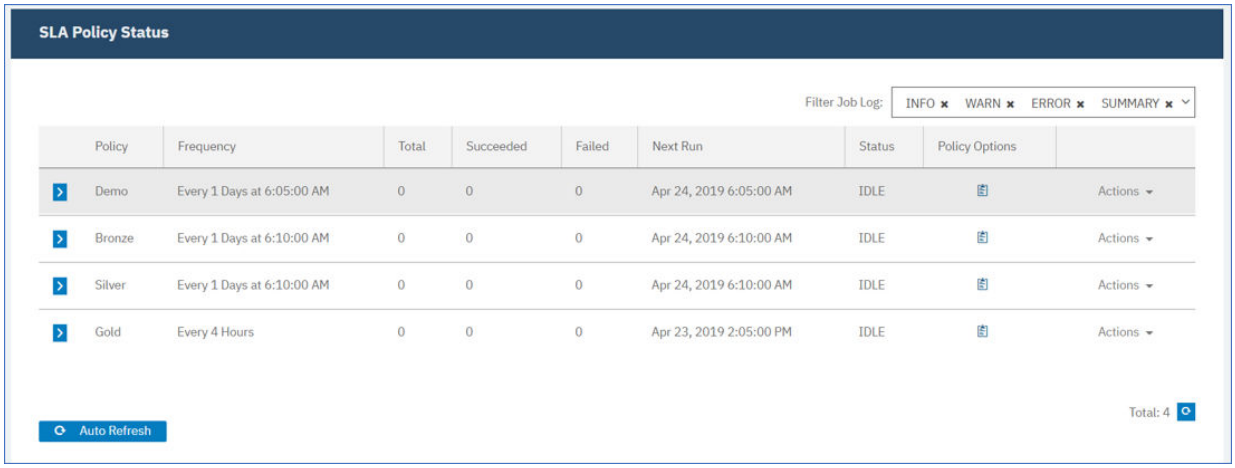


Figura 22. Opciones de copia de seguridad y políticas de SLA

5. Configure la política de SLA pulsando el icono de la columna **Opciones de política** de la tabla **Estado de política de SLA**.

   Para obtener más información sobre las opciones de configuración de SLA, consulte "Establecimiento de opciones de configuración de SLA para un trabajo de copia de seguridad" en la página 152.
6. Si desea ejecutar el exterior de la política del trabajo planificado, seleccione la instancia o la base de datos. Pulse **Acciones** y seleccione **Iniciar**.

El estado cambia a **En ejecución** para el SLA elegido y puede seguir el progreso del trabajo en el registro de trabajo mostrado.

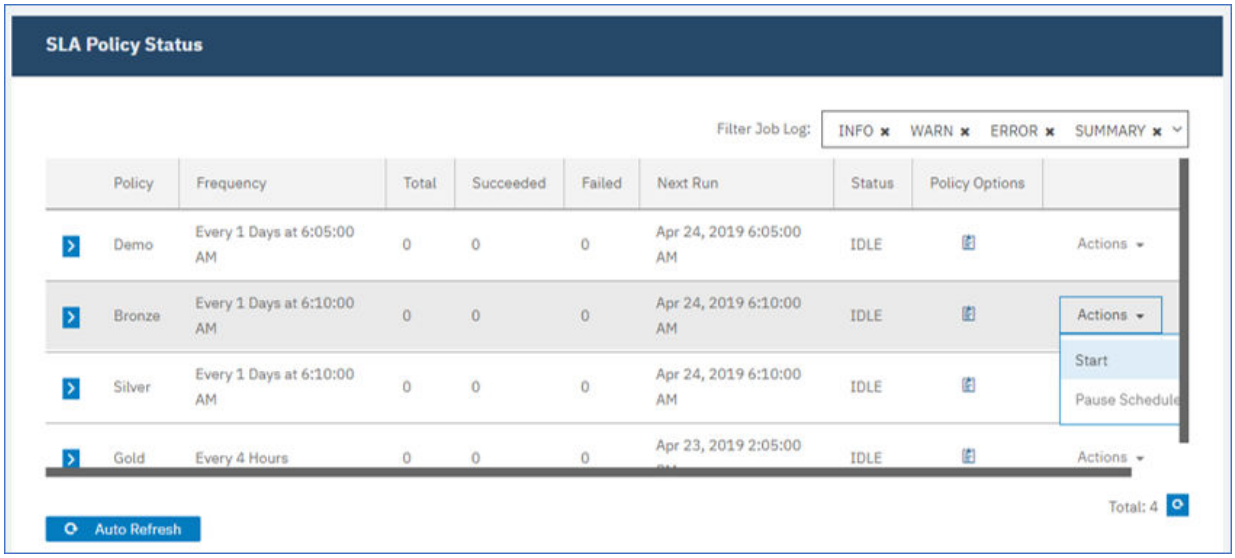


Figura 23. Políticas de SLA

Para poner en pausa la planificación de un SLA, pulse **Acciones** y seleccione **Pausar planificación**.

Para cancelar un trabajo una vez que se haya iniciado, pulse **Acciones** > **Cancelar**.

Establecimiento de opciones de configuración de SLA para un trabajo de copia de seguridad

Después de configurar un acuerdo de nivel de servicio (SLA) para el trabajo de copia de seguridad, puede optar por configurar más opciones para ese trabajo. Puede ejecutar scripts, excluir recursos de la operación de copia de seguridad y forzar una copia de seguridad base completa de una base de datos si es necesario.

Procedimiento

1. En la columna **Opciones de política** de la tabla **Estado de política de SLA** para el trabajo que está configurando, pulse el icono del portapapeles para especificar opciones de configuración adicionales.

   Si el trabajo ya está configurado, pulse en el icono para editar la configuración.

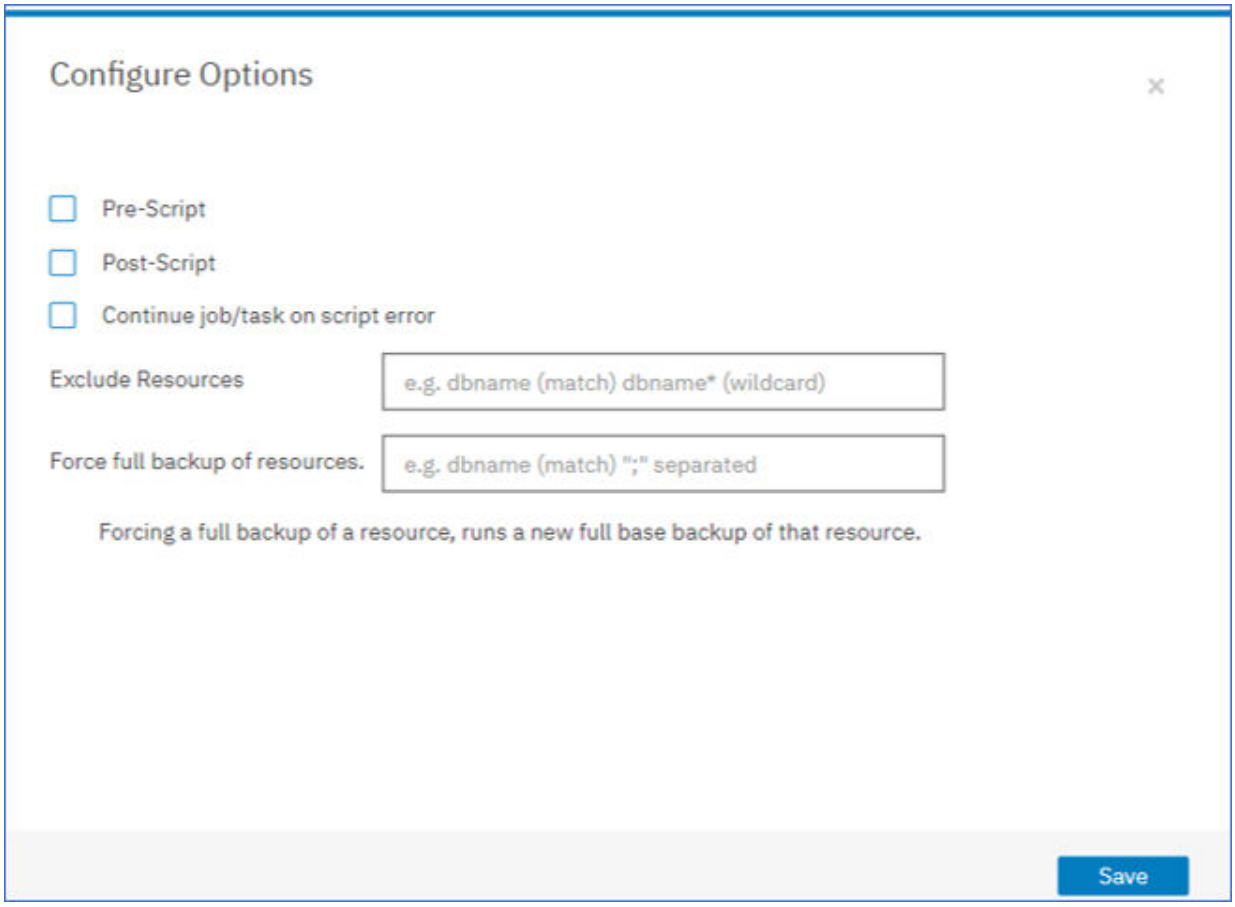


Figura 24. Especificación de opciones de configuración de SLA

2. Pulse **Script anterior** y defina la configuración del script anterior eligiendo una de las opciones siguientes:
   - Pulse **Utilizar servidor de scripts** y seleccione un script cargado en el menú.
   - No pulse **Utilizar servidor de scripts**. Seleccione un servidor de aplicaciones en la lista para ejecutar el script en dicha ubicación.
3. Pulse **Script posterior** y defina la configuración posterior al script eligiendo una de las opciones siguientes:
   - Pulse **Utilizar servidor de scripts** y seleccione un script cargado en el menú.
   - No pulse **Utilizar servidor de scripts**. Seleccione un servidor de aplicaciones en la lista para ejecutar el script en dicha ubicación.

   Los scripts y los servidores de scripts se configuran en la página **Configuración del sistema** > **Script**. Para obtener más información sobre cómo trabajar con scripts, consulte Configuración de scripts.
4. Para continuar ejecutando el trabajo cuando falle el script asociado con el trabajo, seleccione **Continuar trabajo/tarea en error de script**.

   Si se selecciona esta opción, se reintentará la operación de copia de seguridad o restauración y el estado de la tarea de script se notificará como COMPLETADO cuando el script finalice el proceso con un código de retorno distinto de cero. Si no se selecciona esta opción, no se reintentará la operación de copia de seguridad o restauración y el estado de la tarea de script se notificará como FALLIDO.
5. Para excluir recursos de un trabajo de copia de seguridad, especifique los recursos que desea ejecutar del trabajo. Escriba un nombre de recurso exacto en el campo **Excluir recursos**. Si no está seguro de alguno de los nombres, utilice los asteriscos de comodín especificados delante del patrón (**texto*) o después del patrón (*texto**). Se pueden escribir varios comodines con caracteres alfanuméricos estándar y con los siguientes caracteres especiales:-_ y *. Separe las entradas con un punto y coma.

6. Para crear una copia de seguridad completa de un recurso, especifique el nombre de dicho recurso en el campo **Forzar copia de seguridad completa de recursos**. Separe varios recursos con un punto y coma.

   La copia de seguridad completa crea una nueva copia de seguridad completa de ese recurso y sustituye la copia de seguridad existente de dicho recurso por una sola aparición. Una vez completada la copia de seguridad completa, se realiza una copia de seguridad del recurso de forma incremental como antes.

Copias de seguridad de registros

Los registros archivados para bases de datos contienen datos de transacciones comprometidas. Estos datos de transacciones se pueden utilizar para ejecutar una recuperación de datos de avance al ejecutar una operación de restauración. El uso de copias de seguridad de registros de archivado mejora el objetivo de punto de recuperación para los datos.

Asegúrese de seleccionar la opción **Habilitar copias de seguridad de registros** para permitir la recuperación en avance cuando configura un trabajo de copia de seguridad cuando configura un trabajo de copia de seguridad o una política de acuerdo de nivel de servicio (SLA). Cuando se selecciona por primera vez, debe ejecutar un trabajo de copia de seguridad para que la política de SLA active el archivado de registro en IBM Spectrum Protect Plus en la base de datos. Esta copia de seguridad crea un volumen aparte en el repositorio de vSnap, que se monta de manera persistente en el servidor de aplicaciones de Db2. El proceso de copia de seguridad actualiza los parámetros **LOGARCHMETH1** o **LOGARCHMETH2** para que apunten a ese volumen con fines de archivado de registro. El volumen se mantiene montado en el servidor de aplicaciones de Db2, a menos que se deseleccione la opción **Habilitar copia de seguridad de registro** y se ejecute un nuevo trabajo de copia de seguridad.

Restricción: En entornos multiparticionados de Db2, los parámetros **LOGARCHMETH** entre las particiones deben coincidir.

Cuando los parámetros **LOGARCHMETH1** o **LOGARCHMETH2** están establecidos con un valor que no sea OFF, puede utilizar registros archivados para la recuperación en avance. Puede cancelar los trabajos de copia de seguridad de registros en cualquier momento desactivando la opción **Habilitar copias de seguridad de registros**: vaya a **Gestionar protección** > **Aplicaciones** > **Db2**, seleccione la instancia y pulse **Seleccionar opciones**. Este cambio entra en vigor después de que se complete el siguiente trabajo de copia de seguridad correcto y el valor del parámetro **LOGARCHMETH** cambie por su valor original.

Importante: IBM Spectrum Protect Plus solo puede habilitar trabajos de copias de seguridad de registros cuando el parámetro **LOGARCHMETH1** está establecido en LOGRETAIN o si uno de los parámetros **LOGARCHMETH** está establecido en OFF.

Si el parámetro LOGARCHMETH1 está establecido en LOGRETAIN.

IBM Spectrum Protect Plus cambia el valor del parámetro **LOGARCHMETH1** para habilitar copias de seguridad de registros.

Si uno de los parámetros LOGARCHMETH1 o LOGARCHMETH2 está establecido en OFF y el otro está establecido en DISK, TSM o VENDOR.

IBM Spectrum Protect Plus utiliza el parámetro **LOGARCHMETH** que está establecido en off para habilitar copias de seguridad de registros.

Si ambos parámetros LOGARCHMETH están establecidos en DISK, TSM o VENDOR.

Esta combinación de valores hace que se produzca un error cuando IBM Spectrum Protect Plus intenta habilitar las copias de seguridad de registros. Para resolver el error, establezca uno de los parámetros en OFF y ejecute el trabajo de copia de seguridad con la opción **Habilitar copias de seguridad de registros** seleccionada.

Truncado de copias de seguridad de registros de archivado

IBM Spectrum Protect Plus suprime automáticamente los registros transaccionales después de una copia de seguridad de base de datos correcta. Esta acción garantiza que la capacidad del volumen de archivado de registros no se vea comprometida por la retención de los archivos de registro anteriores. Estos archivos de registro truncados se almacenan en el repositorio de vSnap hasta que caduca la copia de

seguridad correspondiente y se suprime. La retención de copias de seguridad de base de datos está definida en la política de SLA que seleccione. Para obtener más información sobre las políticas de SLA, consulte “Definición de un trabajo de copia de seguridad de acuerdo de nivel de servicio” en la página 150.

IBM Spectrum Protect Plus no gestiona la retención de otras ubicaciones de registros archivados.

Para obtener más información sobre los valores de Db2, consulte la página de bienvenida de IBM Db2.

Restauración de datos de Db2

Para restaurar los datos de Db2 desde el repositorio de vSnap, defina un trabajo que restaure los datos desde la copia de seguridad más reciente o desde una copia de seguridad anterior. Puede elegir restaurar datos en la instancia original o en una instancia alternativa en una máquina distinta, especificar opciones de recuperación y guardar el trabajo.

Antes de empezar

Importante: Para todas las operaciones de restauración, Db2 debe tener el mismo nivel de versión en los hosts de origen y destino. Además de este requisito, debe asegurarse de que exista en cada host una instancia con el mismo nombre que la instancia que se está restaurando. Este requisito se aplica cuando la instancia de destino tiene el mismo nombre y cuando los nombres son diferentes. Para que la operación de restauración sea satisfactoria, deben suministrarse ambas instancias: una con el nombre original y la otra con un nuevo nombre.

Si el entorno de Db2 incluye bases de datos particionadas, se hace copia de seguridad de los datos de todas las particiones durante los trabajos de copia de seguridad regulares. Todas las instancias se listan en el panel de copia de seguridad. Las instancias multiparticionadas se muestran con los números de partición y los nombres de host.

Antes de crear un trabajo de restauración para Db2, asegúrese de que se cumplen los requisitos siguientes:

- Se ha configurado como mínimo un trabajo de copia de seguridad de Db2 y se está ejecutando correctamente. Para obtener instrucciones sobre la configuración de un trabajo de copia de seguridad, consulte “Copia de seguridad de datos de Db2” en la página 148.
- Se han asignado roles y grupos de recursos de IBM Spectrum Protect Plus al usuario que configura el trabajo de restauración. Para obtener más información sobre la asignación de roles, consulte Capítulo 13, “Gestión del acceso de usuarios”, en la página 303.
- Cuando se realiza una restauración desde un archivado de IBM Spectrum Protect, los archivos se migrarán a una agrupación de transferencia desde la cinta antes del inicio del trabajo. Dependiendo del tamaño de la restauración, este proceso puede tardar varias horas.

Nota: Cuando restaure bases de datos multiparticionadas en una ubicación alternativa, asegúrese de que la instancia de destino esté configurada con los mismos números de partición que la instancia original. Todas estas particiones deben estar en un solo host. Cuando restaura datos en una nueva instancia a la que se le ha cambiado el nombre, ambas instancias necesarias para la operación de restauración deben configurarse con el mismo número de particiones.

Antes de iniciar una operación de restauración en una instancia alternativa, asegúrese de que la estructura del sistema de archivos de la máquina de origen coincide en la máquina de destino. Esta estructura de sistema de archivos incluye espacios de tabla, registros en línea y el directorio de bases de datos local. Asegúrese de que los volúmenes dedicados con espacio suficiente se asignan a la estructura del sistema de archivos. Db2 debe tener el mismo nivel de versión en los hosts de origen y destino para todas las operaciones de restauración, y debe haber una instancia con el mismo nombre en cada host. Para obtener más información sobre los requisitos de espacio, consulte Requisitos de espacio para la protección de Db2. Para obtener más información sobre los requisitos previos y la configuración, consulte Requisitos previos para Db2.

Procedimiento

1. En el panel de navegación, expanda **Gestionar protección** > **Aplicaciones** > **Db2** y haga clic en **Crear trabajo de restauración**.

   Se abre el asistente de restauración de instantáneas.
2. Opcional: Si ha iniciado el asistente de restauración desde la página **Trabajos y operaciones**, seleccione Db2 como tipo de origen y haga clic en **Siguiente**.

   Consejo: Para obtener un resumen de las selecciones en el asistente de restauración, mueva el cursor al icono de información en el panel de navegación del asistente.
3. En la página **Selección de origen** , pulse en una instancia de Db2 para mostrar las bases de datos en dicha instancia. Elija una base de datos pulsando el icono de signo más junto al nombre de la base de datos. Pulse **Siguiente** para continuar.
4. En la página **Instantánea de origen** , seleccione el tipo de operación de restauración necesaria.
   - **Bajo demanda: instantánea**: crea una única operación de restauración desde una instantánea de base de datos. El trabajo no se ha configurado para repetirse.
   - **Bajo demanda: punto en el tiempo**: crea una única operación de restauración a partir de una copia de seguridad de punto en el tiempo de la base de datos. El trabajo no se ha configurado para repetirse.
   - **Recurrente**: crea un trabajo recurrente que se ejecuta en una planificación y se repite.

   Consejo:

   Para **Bajo demanda: instantánea**, no puede seleccionar ninguna recuperación ni recuperar hasta que finalice la copia de seguridad. Para un trabajo de restauración **Bajo demanda: punto en el tiempo**, puede seleccionar recuperarse hasta el final de los registros disponibles o recuperarse hasta un punto en el tiempo específico.
5. En la misma página, seleccione un **Tipo de ubicación de restauración** como se indica a continuación:

Ubicación	Instrucciones
Sitio	Seleccione esta opción para restaurar los datos desde el sitio primario o secundario. El sitio es la única opción para los trabajos de restauración de punto en el tiempo bajo demanda.
Descarga de la nube	Seleccione esta opción para restaurar los datos desde el almacenamiento en la nube. Especifique el punto de restauración que se utilizará para la instantánea.
Descarga del repositorio	Seleccione esta opción para restaurar los datos desde un repositorio de vSnap. Especifique el punto de restauración que se utilizará para la instantánea.
Archivado de nube	Seleccione esta opción para restaurar los datos que están archivados en la nube. Especifique el punto de restauración que se utilizará para la instantánea.
Archivado de repositorio	Seleccione esta opción para restaurar los datos que están archivados en el repositorio de vSnap. Especifique el punto de restauración que se utilizará para la instantánea.

   Cuando está creando una instantánea bajo demanda, puede especificar un espacio de tiempo en la instantánea que está buscando. Donde sea aplicable, puede utilizar un servidor de vSnap diferente para la operación.

6. Seleccione una ubicación para la operación de restauración. Seleccione una de las siguientes opciones de ubicación y haga clic en **Siguiente**.

Opción	Descripción
Demo	Seleccione esta opción para restaurar los datos desde el servidor de vSnap de demostración. Esta opción sólo está disponible en determinadas configuraciones.
Primario	Seleccione esta opción para restaurar datos del servidor vSnap primario en el destino. Esta ubicación está disponible para el tipo de ubicación de restauración Sitio.
Secundario	Seleccione esta opción para restaurar datos del servidor vSnap secundario en el destino. Esta ubicación está disponible para el tipo de ubicación de restauración Sitio.

   Los puntos de restauración están disponibles desde el menú **Punto de restauración**.
7. Elija un **método de restauración** adecuado para el destino elegido para la operación de restauración. Pulse **Siguiente** para continuar.
   - **Acceso instantáneo**: En esta modalidad, no se emprende ninguna acción adicional después de que IBM Spectrum Protect Plus monte el volumen desde el repositorio de vSnap. Utilice los datos para la recuperación personalizada de los archivos en el volumen montado.
   - **Producción**: en este modalidad, el servidor de aplicaciones de Db2 copia primero los archivos del volumen de repositorio de vSnap en el host de destino, que es una ubicación alternativa o la instancia original. A continuación, los datos copiados se utilizan para iniciar la base de datos.
   - **Probar**: en esta modalidad, el agente crea una nueva base de datos utilizando directamente los archivos del repositorio vSnap.
   - Añada un nombre de base de datos cuando esté restaurando la base de datos en una ubicación distinta y desee cambiar el nombre de la base de datos.

   Consejo:

   La producción es el único **método de restauración** que está disponible para las operaciones de restauración en la ubicación original. Las opciones que no son adecuadas para la operación de restauración que ha seleccionado no son seleccionables.

   Para restaurar los datos a la instancia original, siga las instrucciones que se indican en Restauración a la instancia original. Para restaurar los datos a una instancia alternativa, siga las instrucciones que se indican en Restauración a una instancia alternativa.
8. Establezca el destino de la operación de restauración eligiendo una de las opciones siguientes. Pulse **Siguiente** para continuar.
   - **Restaurar a instancia original**: esta opción restaura los datos en el servidor original y en la instancia original.
   - **Restaurar a la instancia alternativa**: esta opción restaura los datos a una ubicación especificada diferente, creando una copia de los datos en dicha ubicación.

   Si está restaurando datos en una ubicación alternativa, elija una instancia en la tabla **Instancia** antes de hacer clic en **Siguiente**. La instancia alternativa debe estar en una máquina distinta; las instancias no adecuadas no están disponibles para la selección. Para las bases de datos multiparticionadas, la instancia de destino debe tener el mismo conjunto de particiones en una misma máquina.
9. En la página **Opciones de trabajo**, seleccione las opciones de recuperación, aplicación y avanzadas para la operación de restauración que está definiendo.

   Consejo:

Las opciones de recuperación no están disponibles para los trabajos de restauración de acceso instantáneo.

- **Sin recuperación**. Esta opción pasa por alto cualquier recuperación en avance después de la operación de restauración. La base de datos permanece en un estado `Avance pendiente` hasta que decida si desea ejecutar manualmente la operación de la recuperación en avance.
- **Recuperar hasta el final de la copia de seguridad**. Esta opción recupera la base de datos seleccionada a su estado en el momento en que se creó la copia de seguridad. El proceso de recuperación utiliza los archivos de registro que se incluyen en la copia de seguridad de la base de datos de Db2.
- **Recuperar hasta el final de los registros disponibles**. Esta opción solo está disponible si se realiza una copia de seguridad de los registros en la definición del trabajo de copia de seguridad de Db2. IBM Spectrum Protect Plus utiliza el punto de restauración más reciente. Se crea automáticamente una restauración temporal para que la base de datos de Db2 se pueda retrotraer hasta el final de los registros. Esta opción de recuperación no está disponible si ha seleccionado un punto de restauración específico en la lista. Esta opción solo está disponible cuando se está ejecutando un trabajo de restauración de punto en el tiempo bajo demanda que utiliza la última copia de seguridad.
- **Recuperar hasta un momento específico**. Esta opción incluye todos los datos de copia de seguridad hasta un punto en el tiempo específico. Esta opción solo está disponible si habilitó las copias de seguridad de los registros en la definición del trabajo de copia de seguridad de Db2. Configure una recuperación de un punto en el tiempo mediante una fecha y hora específicas, por ejemplo, `1 de enero de 2019 12:18:00 AM`. IBM Spectrum Protect Plus busca directamente los puntos de restauración antes y después del punto en el tiempo específico elegido. Durante el proceso de recuperación, se montan el volumen de copia de seguridad de datos más antiguo y el volumen de copia de seguridad de registro más reciente. Si el punto en el tiempo es después de la última copia de seguridad, se crea un punto de restauración temporal. Esta opción de recuperación no está disponible si ha seleccionado un punto de restauración específico en la lista. Esta opción solo está disponible cuando ejecuta un trabajo de restauración de punto en el tiempo bajo demanda que utiliza la copia de seguridad más reciente.

Consejo: Para omitir los pasos opcionales en el asistente de restauración, seleccione **Omitir pasos opcionales** y haga clic en **Siguiente**.

10. Opcional: En la página **Opciones de trabajo** , seleccione las opciones de aplicación para la operación de restauración que está definiendo.

    Consejo:

    Las opciones de aplicación no están disponibles para los trabajos de restauración de acceso instantáneo.

    - **Sobrescribir bases de datos existentes**. Elija esta opción para sustituir las bases de datos existentes que tengan los mismos nombres durante el proceso de restauración de restauración. Si esta opción no está seleccionada, el trabajo de restauración falla cuando las bases de datos con el mismo nombre se encuentran durante la operación de restauración. Si selecciona esta opción, asegúrese de que el directorio de registros de Db2 y el directorio de registro de duplicación de Db2 no tengan datos.

      Atención: Asegúrese de que ninguna otra base de datos comparta el directorio de bases de datos local como la base de datos original o de que los datos se sobrescriben cuando se selecciona esta opción.
    - **Número máximo de streams paralelos por base de datos**. Puede optar por ejecutar la operación de restauración de datos en streams paralelos. Esta opción es útil si está restaurando una base de datos grande.
    - **Especifique el tamaño de la memoria de base de datos Db2 establecida en KB**. Especifique la memoria, en KB, que se debe asignar para la restauración de la base de datos en la máquina de destino. Este valor se utiliza para modificar el tamaño de memoria compartida de la base de datos

de Db2 en el servidor de destino. Para utilizar el mismo tamaño de memoria compartida en el servidor de origen y en el servidor de destino, establezca el valor en cero.

11. Opcional: En la página **Opciones de trabajo** , seleccione las opciones avanzadas para la operación de restauración que está definiendo.
    - **Ejecute la limpieza inmediatamente en caso de anomalía del trabajo**. Esta opción se selecciona de forma predeterminada para limpiar automáticamente los recursos asignados como parte de una operación de restauración cuando falla la recuperación.
    - **Continuar con las restauraciones de otras bases de datos seleccionadas incluso si una falla**. Esta opción continúa la operación de restauración si una base de datos de la instancia no se puede restaurar satisfactoriamente. El proceso continúa para todas las demás bases de datos que se están restaurando. Cuando esta opción no está seleccionada, el trabajo de restauración se detiene cuando falla la recuperación de un recurso.
    - **Prefijo de punto de montaje**. Para las operaciones de restauración de acceso instantáneo, especifique el prefijo de la vía de acceso donde se va a dirigir el punto de montaje.
12. Elija las opciones de script en la página **Aplicar scripts** y pulse **Siguiente** para continuar.
    - Seleccione **Script anterior** para seleccionar un script cargado, y un servidor de aplicaciones o de scripts donde se ejecuta el script anterior. Para seleccionar un servidor de aplicaciones en el que se ejecuta el script, desmarque el recuadro de selección **Utilizar servidor de scripts**. Vaya a la página **Configuración del sistema** > **Script** para configurar los scripts y los servidores de scripts.
    - Seleccione **Script posterior** para seleccionar un script cargado, y un servidor de aplicaciones o de scripts donde se ejecuta el script posterior. Para seleccionar un servidor de aplicaciones en el que se ejecuta el script, desmarque el recuadro de selección **Utilizar servidor de scripts**. Vaya a la página **Configuración del sistema** > **Script** para configurar los scripts y los servidores de scripts.
    - Seleccione **Continuar trabajo/tarea en error de script** para seguir ejecutando el trabajo cuando falle el script asociado al trabajo. Cuando esta opción está habilitada y el script anterior se completa con un código de retorno distinto de cero, el trabajo de copia de seguridad o restauración sigue ejecutándose y el estado de la tarea del script anterior devuelve `COMPLETADO`. Si un script posterior se completa con un código de retorno distinto de cero, el estado de la tarea del script posterior devuelve `COMPLETADO`. Cuando esta opción no está seleccionada, el trabajo de copia de seguridad o restauración no se ejecuta, y el estado de la tarea del script anterior o el script posterior devuelve un estado `FALLIDO`.
13. En la página **Planificación**, ponga nombre al trabajo de restauración y elija la frecuencia con la que se ejecutará el trabajo. Planifique la hora de inicio y haga clic en **Siguiente** para continuar.

    Si el trabajo de restauración que está especificando es un trabajo bajo demanda, no hay ninguna opción para especificar una planificación. Especifique una planificación solo para los trabajos de restauración recurrentes.
14. En la página **Revisar** , revise las selecciones para el trabajo de restauración. Si todos los detalles son correctos para el trabajo de restauración, haga clic en **Enviar** o haga clic en **Atrás** para realizar las modificaciones.

Resultados

Unos momentos después de pulsar **Enviar**, el registro **onDemandRestore** se añade al panel **Sesiones de trabajo**. Para ver el progreso de la operación de restauración, expanda el trabajo. También puede descargar el archivo de registro pulsando descarga  . Todos los trabajos en ejecución se pueden visualizar en la página **Trabajos y operacionesEjecución de trabajos** .

Para restaurar los datos a la instancia original, siga las instrucciones que se indican en Restauración a la instancia original. Para restaurar los datos a una instancia alternativa, siga las instrucciones que se indican en Restauración a una instancia alternativa.

Restauración de datos de Db2 a la instancia original

Puede restaurar una copia de seguridad de base de datos a su instancia original en el host original. Puede restaurar a la última copia de seguridad o a una versión de copia de seguridad de base de datos de Db2

anterior. Cuando se restaura una base de datos a su instancia original, no se puede cambiar su nombre. Esta opción de restauración ejecuta una restauración de producción completa y los datos existentes se sobrescriben en el sitio de destino si la opción **Sobrescribir bases de datos existentes** está seleccionada.

Antes de empezar

Si el entorno de Db2 incluye bases de datos particionadas, se hace copia de seguridad de los datos de todas las particiones durante los trabajos de copia de seguridad regulares. Todas las instancias se listan en el panel de copia de seguridad. Las instancias multiparticionadas se muestran con los números de partición y los nombres de host.

Antes de crear un trabajo de restauración para Db2, asegúrese de que se cumplen los requisitos siguientes:

- Se ha configurado como mínimo un trabajo de copia de seguridad de Db2 y se está ejecutando correctamente. Para obtener instrucciones sobre la configuración de un trabajo de copia de seguridad, consulte "Copia de seguridad de datos de Db2" en la página 148.
- Se han asignado roles y grupos de recursos de IBM Spectrum Protect Plus al usuario que configura el trabajo de restauración. Para obtener más información sobre la asignación de roles, consulte Capítulo 13, "Gestión del acceso de usuarios", en la página 303.
- Cuando se realiza una restauración desde un archivado de IBM Spectrum Protect, los archivos se migrarán a una agrupación de transferencia desde la cinta antes del inicio del trabajo. Dependiendo del tamaño de la restauración, este proceso puede tardar varias horas.

Procedimiento

1. En el panel de navegación, expanda **Gestionar protección** > **Aplicaciones** > **Db2** y haga clic en **Crear trabajo de restauración**.

   Se abre el asistente de restauración de instantáneas.
2. Opcional: Si ha iniciado el asistente de restauración desde la página **Trabajos y operaciones**, seleccione Db2 como tipo de origen y haga clic en **Siguiente**.

   Consejo: Para obtener un resumen de las selecciones en el asistente de restauración, mueva el cursor al icono de información en el panel de navegación del asistente.
3. En la página **Selección de origen** , pulse en una instancia de Db2 para mostrar las bases de datos en dicha instancia. Elija una base de datos pulsando el icono de signo más junto al nombre de la base de datos. Pulse **Siguiente** para continuar.
4. En la página **Instantánea de origen** , seleccione el tipo de operación de restauración necesaria.
   - **Bajo demanda: instantánea**: crea una única operación de restauración desde una instantánea de base de datos. El trabajo no se ha configurado para repetirse.
   - **Bajo demanda: punto en el tiempo**: crea una única operación de restauración a partir de una copia de seguridad de punto en el tiempo de la base de datos. El trabajo no se ha configurado para repetirse.
   - **Recurrente**: crea un trabajo recurrente que se ejecuta en una planificación y se repite.

   Consejo:

   Para **Bajo demanda: instantánea**, no puede seleccionar ninguna recuperación ni recuperar hasta que finalice la copia de seguridad. Para un trabajo de restauración **Bajo demanda: punto en el tiempo**, puede seleccionar recuperarse hasta el final de los registros disponibles o recuperarse hasta un punto en el tiempo específico.
5. En la misma página, seleccione un **Tipo de ubicación de restauración** como se indica a continuación:

Ubicación	Instrucciones
Sitio	Seleccione esta opción para restaurar los datos desde el sitio primario o secundario. El sitio es la única opción para los trabajos de restauración de punto en el tiempo bajo demanda.
Descarga de la nube	Seleccione esta opción para restaurar los datos desde el almacenamiento en la nube. Especifique el punto de restauración que se utilizará para la instantánea.
Descarga del repositorio	Seleccione esta opción para restaurar los datos desde un repositorio de vSnap. Especifique el punto de restauración que se utilizará para la instantánea.
Archivado de nube	Seleccione esta opción para restaurar los datos que están archivados en la nube. Especifique el punto de restauración que se utilizará para la instantánea.
Archivado de repositorio	Seleccione esta opción para restaurar los datos que están archivados en el repositorio de vSnap. Especifique el punto de restauración que se utilizará para la instantánea.

Cuando está creando una instantánea bajo demanda, puede especificar un espacio de tiempo en la instantánea que está buscando. Donde sea aplicable, puede utilizar un servidor de vSnap diferente para la operación.

6. Seleccione una ubicación para la operación de restauración. Seleccione una de las siguientes opciones de ubicación y haga clic en **Siguiente**.

Opción	Descripción
Demo	Seleccione esta opción para restaurar los datos desde el servidor de vSnap de demostración. Esta opción sólo está disponible en determinadas configuraciones.
Primario	Seleccione esta opción para restaurar datos del servidor vSnap primario en el destino. Esta ubicación está disponible para el tipo de ubicación de restauración Sitio.
Secundario	Seleccione esta opción para restaurar datos del servidor vSnap secundario en el destino. Esta ubicación está disponible para el tipo de ubicación de restauración Sitio.

Los puntos de restauración están disponibles desde el menú **Punto de restauración**.

7. En la página **Método de restauración**, elija **Producción** para la operación de restauración.

   En la modalidad de **Producción**, el servidor de aplicaciones de Db2 copia primero los archivos del volumen de repositorio de vSnap en el host de destino. A continuación, los datos copiados se utilizan para iniciar la base de datos.

   Consejo: Evite introducir un nuevo nombre de base de datos cuando restaure una operación de producción en la instancia original, ya que no se implementará.

8. Establezca el destino de la operación de restauración en **Restaurar a la instancia original** para restaurar los datos al servidor original. Pulse **Siguiente** para continuar.

9. Elija las opciones como se describe en “Restauración de datos de Db2 ” en la página 155.
10. En la página **Planificación**, ponga nombre al trabajo de restauración y elija la frecuencia con la que se ejecutará el trabajo. Planifique la hora de inicio y haga clic en **Siguiente** para continuar.

    Si el trabajo de restauración que está especificando es un trabajo bajo demanda, no hay ninguna opción para especificar una planificación. Especifique una planificación solo para los trabajos de restauración recurrentes.
11. En la página **Revisar** , revise las selecciones para el trabajo de restauración. Si todos los detalles son correctos para el trabajo de restauración, haga clic en **Enviar** o haga clic en **Atrás** para realizar las modificaciones.

Resultados

Unos momentos después de pulsar **Enviar**, el registro **onDemandRestore** se añade al panel **Sesiones de trabajo**. Para ver el progreso de la operación de restauración, expanda el trabajo. También puede descargar el archivo de registro pulsando descarga  . Todos los trabajos en ejecución se pueden visualizar en la página **Trabajos y operacionesEjecución de trabajos** .

Restauración de bases de datos de Db2 a una instancia alternativa

Puede restaurar una base de datos de Db2 a otra instancia de Db2 en un host alternativo. También puede elegir restaurar una base de datos a una instancia con un nombre distinto y cambiar el nombre de la base de datos. Este proceso crea una copia exacta de la base de datos sobre un host diferente en una instancia distinta. Si restaura un recurso a una ubicación alternativa, puede restaurar el mismo recurso varias veces sin especificar distintos hosts de destino.

Antes de empezar

Importante: Para todas las operaciones de restauración, Db2 debe tener el mismo nivel de versión en los hosts de origen y destino. Además de este requisito, debe asegurarse de que exista en cada host una instancia con el mismo nombre que la instancia que se está restaurando. Este requisito se aplica cuando la instancia de destino tiene el mismo nombre y cuando los nombres son diferentes. Para que la operación de restauración sea satisfactoria, deben suministrarse ambas instancias: una con el nombre original y la otra con un nuevo nombre.

Antes de crear un trabajo de restauración para Db2, asegúrese de que se cumplen los requisitos siguientes:

- Se ha configurado como mínimo un trabajo de copia de seguridad de Db2 y se está ejecutando correctamente. Para obtener instrucciones sobre la configuración de un trabajo de copia de seguridad, consulte “Copia de seguridad de datos de Db2” en la página 148.
- Se han asignado roles y grupos de recursos de IBM Spectrum Protect Plus al usuario que configura el trabajo de restauración. Para obtener más información sobre la asignación de roles, consulte Capítulo 13, “Gestión del acceso de usuarios”, en la página 303.
- Cuando se realiza una restauración desde un archivado de IBM Spectrum Protect, los archivos se migrarán a una agrupación de transferencia desde la cinta antes del inicio del trabajo. Dependiendo del tamaño de la restauración, este proceso puede tardar varias horas.

Antes de iniciar una operación de restauración en una instancia alternativa, asegúrese de que la estructura del sistema de archivos de la máquina de origen coincide en la máquina de destino. Esta estructura de sistema de archivos incluye espacios de tabla, registros en línea y el directorio de bases de datos local. Asegúrese de que los volúmenes dedicados con espacio suficiente se asignan a la estructura del sistema de archivos. Db2 debe tener el mismo nivel de versión en los hosts de origen y destino para todas las operaciones de restauración, y debe haber una instancia con el mismo nombre en cada host. Para obtener más información sobre los requisitos de espacio, consulte Requisitos de espacio para la protección de Db2. Para obtener más información sobre los requisitos previos y la configuración, consulte Requisitos previos para Db2.

Restricción: Si los datos existen en el directorio de bases de datos local al que está restaurando la copia de seguridad de la base de datos y la opción **Sobrescribir bases de datos existentes** no está

seleccionada, la operación de restauración no se ejecuta correctamente. Ningún otro dato puede compartir el directorio de bases de datos local donde se restaura la copia de seguridad. Cuando se selecciona la opción **Sobrescribir bases de datos existentes**, los datos existentes se eliminan y el directorio de bases de datos local en el host alternativo.

Nota: Cuando restaure bases de datos multiparticionadas en una ubicación alternativa, asegúrese de que la instancia de destino esté configurada con los mismos números de partición que la instancia original. Todas estas particiones deben estar en un solo host. Cuando restaura datos en una nueva instancia a la que se le ha cambiado el nombre, ambas instancias necesarias para la operación de restauración deben configurarse con el mismo número de particiones.

Acerca de esta tarea

Asegúrese de que las vías de acceso al disco para la operación de restauración redirigida incluyen el nombre de instancia y el nombre de base de datos. La información es necesaria para todos los tipos de vías de acceso: vías de acceso de base de datos, vías de acceso de contenedor, vías de acceso de almacenamiento y vías de acceso de registro y de registro de duplicación.

Procedimiento

1. En el panel de navegación, expanda **Gestionar protección** > **Aplicaciones** > **Db2** y haga clic en **Crear trabajo de restauración**.

   Se abre el asistente de restauración de instantáneas.
2. Opcional: Si ha iniciado el asistente de restauración desde la página **Trabajos y operaciones**, seleccione Db2 como tipo de origen y haga clic en **Siguiente**.

   Consejo: Para obtener un resumen de las selecciones en el asistente de restauración, mueva el cursor al icono de información en el panel de navegación del asistente.
3. En la página **Selección de origen** , pulse en una instancia de Db2 para mostrar las bases de datos en dicha instancia. Elija una base de datos pulsando el icono de signo más junto al nombre de la base de datos. Pulse **Siguiente** para continuar.
4. En la página **Instantánea de origen** , seleccione el tipo de operación de restauración necesaria.
   - **Bajo demanda: instantánea**: crea una única operación de restauración desde una instantánea de base de datos. El trabajo no se ha configurado para repetirse.
   - **Bajo demanda: punto en el tiempo**: crea una única operación de restauración a partir de una copia de seguridad de punto en el tiempo de la base de datos. El trabajo no se ha configurado para repetirse.
   - **Recurrente**: crea un trabajo recurrente que se ejecuta en una planificación y se repite.

   Consejo:

   Para **Bajo demanda: instantánea**, no puede seleccionar ninguna recuperación ni recuperar hasta que finalice la copia de seguridad. Para un trabajo de restauración **Bajo demanda: punto en el tiempo**, puede seleccionar recuperarse hasta el final de los registros disponibles o recuperarse hasta un punto en el tiempo específico.
5. En la misma página, seleccione un **Tipo de ubicación de restauración** como se indica a continuación:

Ubicación	Instrucciones
Sitio	Seleccione esta opción para restaurar los datos desde el sitio primario o secundario. El sitio es la única opción para los trabajos de restauración de punto en el tiempo bajo demanda.
Descarga de la nube	Seleccione esta opción para restaurar los datos desde el almacenamiento en la nube. Especifique el punto de restauración que se utilizará para la instantánea.

Ubicación	Instrucciones
Descarga del repositorio	Seleccione esta opción para restaurar los datos desde un repositorio de vSnap. Especifique el punto de restauración que se utilizará para la instantánea.
Archivado de nube	Seleccione esta opción para restaurar los datos que están archivados en la nube. Especifique el punto de restauración que se utilizará para la instantánea.
Archivado de repositorio	Seleccione esta opción para restaurar los datos que están archivados en el repositorio de vSnap. Especifique el punto de restauración que se utilizará para la instantánea.

Cuando está creando una instantánea bajo demanda, puede especificar un espacio de tiempo en la instantánea que está buscando. Donde sea aplicable, puede utilizar un servidor de vSnap diferente para la operación.

6. Seleccione una ubicación para la operación de restauración. Seleccione una de las siguientes opciones de ubicación y haga clic en **Siguiente**.

Opción	Descripción
Demo	Seleccione esta opción para restaurar los datos desde el servidor de vSnap de demostración. Esta opción sólo está disponible en determinadas configuraciones.
Primario	Seleccione esta opción para restaurar datos del servidor vSnap primario en el destino. Esta ubicación está disponible para el tipo de ubicación de restauración Sitio.
Secundario	Seleccione esta opción para restaurar datos del servidor vSnap secundario en el destino. Esta ubicación está disponible para el tipo de ubicación de restauración Sitio.

Los puntos de restauración están disponibles desde el menú **Punto de restauración**.

7. Elija un **método de restauración** adecuado para el destino elegido para la operación de restauración. Pulse **Siguiente** para continuar.
   - **Producción**: en este modalidad, el servidor de aplicaciones de Db2 copia primero los archivos del volumen de repositorio de vSnap en el host de destino, que es una ubicación alternativa o la instancia original. A continuación, los datos copiados se utilizan para iniciar la base de datos.
   - **Probar**: en esta modalidad, el agente crea una nueva base de datos utilizando directamente los archivos del repositorio vSnap.
   - **Acceso instantáneo**: En esta modalidad, no se emprende ninguna acción adicional después de que IBM Spectrum Protect Plus monte el volumen desde el repositorio de vSnap. Utilice los datos para la recuperación personalizada de los archivos en el volumen montado.
   - Añada un nombre de base de datos cuando esté restaurando la base de datos en una ubicación distinta y desee cambiar el nombre de la base de datos.
8. Establezca el destino de la operación de restauración en **Restaurar a la instancia alternativa** para restaurar los datos a una ubicación distinta que puede seleccionar en las lista de ubicaciones elegibles. Pulse **Siguiente** para continuar.

Cuando realice la restauración en una ubicación alternativa, elija una instancia en la tabla **Instancia** antes de pulsar **Siguiente**. No se pueden seleccionar instancias de destino inadecuadas.

9. Elija las opciones como se describe en “Restauración de datos de Db2 ” en la página 155.
10. En la página **Planificación**, ponga nombre al trabajo de restauración y elija la frecuencia con la que se ejecutará el trabajo. Planifique la hora de inicio y haga clic en **Siguiente** para continuar.

    Si el trabajo de restauración que está especificando es un trabajo bajo demanda, no hay ninguna opción para especificar una planificación. Especifique una planificación solo para los trabajos de restauración recurrentes.
11. En la página **Revisar** , revise las selecciones para el trabajo de restauración. Si todos los detalles son correctos para el trabajo de restauración, haga clic en **Enviar** o haga clic en **Atrás** para realizar las modificaciones.

Resultados

Unos momentos después de pulsar **Enviar**, el registro **onDemandRestore** se añade al panel **Sesiones de trabajo**. Para ver el progreso de la operación de restauración, expanda el trabajo. También puede descargar el archivo de registro pulsando descarga . Todos los trabajos en ejecución se pueden visualizar en la página **Trabajos y operacionesEjecución de trabajos** .

Servidor de Microsoft Exchange.

Una vez que haya registrado correctamente un servidor de Microsoft Exchange, puede empezar a proteger datos de Microsoft Exchange con IBM Spectrum Protect Plus. Defina una política de acuerdo de nivel de servicio (SLA) para crear trabajos de copia de seguridad con planificaciones específicas con planificaciones específicas, políticas de retención y scripts.

Requisitos previos para Microsoft Exchange Server

Asegúrese de que todos los requisitos previos de la aplicación Microsoft Exchange se cumplan antes de empezar a proteger base de datos de Microsoft Exchange con IBM Spectrum Protect Plus.

Para obtener más información, consulte “Requisitos de Microsoft Exchange Server” en la página 31.

Soporte de virtualización

IBM Spectrum Protect Plus da soporte a Microsoft Exchange Server que se ejecuta en un servidor (bare metal) físico asó como en un entorno de virtualización. Se da soporte a los entornos de virtualización siguientes:

- Sistema operativo invitado VMware ESX
- Sistema operativo invitado Hyper-V de Microsoft Windows

Privilegios

Para asegurarse de que un agente de Microsoft Exchange puede funcionar en el entorno de IBM Spectrum Protect Plus, debe configurar privilegios adecuados.

Control de acceso basado en roles

Para la seguridad de IBM Spectrum Protect Plus, los usuarios que han iniciado sesión en Exchange Server deben tener permisos de control de acceso basado en roles (RBAC) para acceder a los buzones y para completar las tareas de restauración del buzón.

Debe asignar los siguientes roles de gestión a cada usuario de Exchange que realizará las tareas de restauración de buzón:

- Permisos de Active Directory
- ApplicationImpersonation

- Bases de datos
- Recuperación tras desastre
- Importación y exportación de buzón
- Carpetas públicas
- Configuración de solo vista
- Destinatarios de solo vista

Se recomienda colocar los usuarios que desea que realicen las tareas de restauración de buzón en un grupo de roles del servidor de Exchange que contiene los roles anteriores.

El servidor de Exchange incluye varios grupos de rol incorporados. El grupo de roles Gestión de organización de forma predeterminada contendrá la mayoría, si no todos los roles listados anteriormente.

Se recomienda colocar el usuario que desea que realice las tareas de restauración de buzón en el grupo de roles Gestión de la organización (asegurándose de que contiene todos los roles listados anteriormente).

De lo contrario, puede colocar el usuario en otro grupo de roles que haya creado o en cualquier otro grupo de roles incorporado que contenga los roles listados anteriormente.

Nota: Un usuario cuyo nombre no se encuentra en el grupo o subgrupos de roles de Exchange Organization Management puede experimentar un rendimiento más lento al completar las operaciones de restauración.

Nota: Podrá gestionar grupos de roles de Exchange utilizando Exchange Admin Center (EAC) o Exchange Powershell Cmdlets **solo** si el nombre de usuario está autorizado por la política de seguridad de su organización.

Ámbito del rol de gestión

Asegúrese de que los objetos de Exchange siguientes están en el ámbito de rol de gestión para el usuario de Exchange:

- El servidor de Exchange que contiene los datos necesarios.
- La base de datos de recuperación que ha creado IBM Spectrum Protect Plus.
- La base de datos que contiene el buzón activo.
- La base de datos que contiene el buzón activo del usuario que completa la operación de restauración.

Verifique que el nombre de usuario de Exchange sea miembro de un grupo Administrador y que tenga un buzón de Exchange activo en el dominio. De forma predeterminada, Windows añade el grupo Administradores de la organización de Exchange a otros grupos de seguridad, incluido el grupo de Administradores local. Para los usuarios de Exchange que no son miembros del grupo Exchange Organization Management, debe añadir manualmente la cuenta de usuario al grupo de Administradores locales utilizando la herramienta Usuarios y grupos locales en el sistema del miembro de dominio.

En el sistema del miembro de dominio, pulse **Herramientas administrativas > Gestión del sistema > Herramienta de usuarios y grupos locales**. En un sistema del controlador de dominios que no tenga un grupo de Administradores local o una herramienta Usuarios y grupos locales, añada manualmente la cuenta de usuario al grupo Administradores en el dominio pulsando **Herramientas administrativas > Herramienta Usuarios y sistemas de Active Directory**.

Sistema de cifrado de archivos

IBM Spectrum Protect Plus for Exchange requiere que el Sistema de archivos de cifrado (EFS) esté habilitado en la política de dominio local o de grupo y que esté disponible un certificado de agente de recuperación de datos de dominio (DRA) válido. Si se define una política de grupo personalizado y se enlaza con la unidad organizativa, asegúrese de que el servidor Exchange forme parte de la unidad organizativa.

Adición de un servidor de aplicaciones de Microsoft Exchange

Al registrar Microsoft Exchange Server, se añade un inventario de bases de datos de Exchange a IBM Spectrum Protect Plus. Cuando el inventario está disponible, puede iniciar la copia de seguridad y la restauración de las bases de datos de Exchange y ejecutar informes.

Acerca de esta tarea

Para registrar un servidor de aplicaciones de Microsoft Exchange, necesita la dirección IP o el nombre de host.

Procedimiento

Para añadir un servidor de aplicaciones de Microsoft Exchange, complete los pasos siguientes:

1. En el panel de navegación, expanda **Gestionar protección > Aplicaciones > Exchange**.
2. En la página **Exchange**, pulse **Gestionar servidores de aplicaciones** y, a continuación, pulse **Añadir servidor de aplicaciones** para añadir el sistema host.
3. En el formulario **Propiedades de la aplicación**, especifique la dirección IP o el host.
4. Escriba un ID de usuario en el formato del dominio de directorio y cuenta de usuario (domain\user) activos y de la contraseña asociada. Este usuario debe tener los roles y privilegios de Exchange correctos. Para obtener más información sobre los privilegios de Exchange, consulte “Privilegios ” en la página 165.
5. Pulse **Guardar** y repita los pasos para añadir otras instancias de Microsoft Exchange a IBM Spectrum Protect Plus.

   Importante: En un entorno de grupo de disponibilidad de base de datos (DAG), registre todos los servidores de aplicaciones de Microsoft Exchange en el DAG.

Qué hacer a continuación

Cuando se añade el servidor de aplicaciones Exchange a IBM Spectrum Protect Plus, se ejecuta automáticamente un inventario en cada instancia. Deben detectarse bases de datos para asegurarse de que se puede realizar copias de seguridad de ellas, y puede ejecutar un inventario manual en cualquier momento para detectar las actualizaciones. Para obtener instrucciones sobre la ejecución de un inventario manual, consulte “Detección de bases de datos de Microsoft Exchange mediante la ejecución de un inventario” en la página 167. Para obtener instrucciones sobre cómo configurar trabajos de copia de seguridad de base de datos de Exchange, consulte “Definición de un trabajo de copia de seguridad de Acuerdo de nivel de servicio” en la página 169.

Detección de bases de datos de Microsoft Exchange mediante la ejecución de un inventario

Cuando se añaden las instancias del servidor de Microsoft Exchange a IBM Spectrum Protect Plus, un inventario se ejecuta automáticamente. Sin embargo, puede ejecutar manualmente un inventario en un servidor de aplicaciones Exchange en cualquier momento para detectar actualizaciones y listar todas las bases de datos de Exchange de cada instancia.

Antes de empezar

Asegúrese de que ha añadido las instancias de Exchange a IBM Spectrum Protect Plus. Para obtener instrucciones sobre la adición de una instancia de Exchange, consulte “Adición de un servidor de aplicaciones de Microsoft Exchange” en la página 167.

Procedimiento

1. En el panel de navegación, expanda **Gestionar protección** > **Aplicaciones** > **Exchange**..
2. Pulse **Ejecutar inventario**.

   Cuando se ejecuta el inventario, la etiqueta de botón cambia a **Inventario en curso**. Puede ejecutar un inventario en cualquier servidor de aplicaciones disponible, pero solo puede ejecutar un proceso de inventario a la vez.

3. Para supervisar el trabajo de inventario, vaya a **Trabajos y operaciones**. Pulse la pestaña **Trabajos en ejecución** y busque la entrada de registro Inventario de servidor de aplicaciones más reciente.

   Los trabajos completados se muestran en la pestaña **Historial de trabajos**. Puede utilizar la lista **Ordenar por** para ordenar los trabajos en función de la hora de inicio, el tipo, el estado, el nombre del trabajo o la duración. Utilice el campo **Buscar por nombre** para buscar trabajos por nombre. Puede utilizar asteriscos como caracteres comodín en el nombre.
4. Cuando se haya completado el trabajo de inventario, en el panel **Copia de seguridad de Exchange**, pulse una instancia de Exchange para abrir una vista que muestre las bases de datos que se detectan para dicha instancia. Si falta alguna de las bases de datos en la lista **Instancias**, compruebe el servidor de aplicaciones de Microsoft Exchange y vuelva a ejecutar el inventario.

   Consejo: Para volver a la lista de instancias, pulse el hipertexto **Instancias** en el panel Copia de seguridad de Exchange.

Prueba de conexión de Microsoft Exchange

Una vez que haya registrado un servidor de aplicaciones de Microsoft Exchange y cuando lo haya añadido a la lista de servidores de aplicaciones, pruebe la conexión. La prueba verifica la comunicación entre IBM Spectrum Protect Plus y el servidor de aplicaciones de host.

Procedimiento

1. En el panel de navegación, expanda **Gestionar protección** > **Aplicaciones** > **Exchange**.
2. En la página **Exchange**, pulse **Gestionar servidores de aplicaciones**.

   Se muestran los servidores de aplicaciones de Microsoft Exchange que están disponibles.
3. Pulse **Acciones** para el servidor de aplicaciones de Microsoft Exchange que desea probar y, a continuación, pulse **Probar**.

   El informe de prueba muestra una lista de las pruebas que se han ejecutado y su estado. Cada procedimiento de prueba incluye una prueba de la configuración de red de host física, una prueba de sesión remota y los requisitos previos para una prueba de Windows, como por ejemplo, privilegios de administrador de usuario.
4. Pulse **Aceptar** para cerrar la prueba. Vuelva a ejecutarla cuando haya arreglado el o los problemas.

Copias de seguridad de bases de datos de Microsoft Exchange

Para proteger las bases de datos de Microsoft Exchange, puede definir un trabajo de copia de seguridad que se ejecuta continuamente para crear copias de seguridad incrementales. También puede ejecutar trabajos de copia de seguridad bajo demanda fuera de la planificación.

Antes de empezar

Asegúrese de que se añaden los servidores de aplicaciones que contienen las bases de datos de Exchange de las que desea realizar copia de seguridad. Para obtener más información, consulte “Adición de un servidor de aplicaciones de Microsoft Exchange” en la página 167.

Procedimiento

1. En el panel de navegación, expanda **Gestionar protección** > **Aplicaciones** > **Exchange**.
2. En el panel **Copia de seguridad de Exchange**, haga clic en la instancia de Microsoft Exchange y, a continuación, seleccione la base de datos de la que va ha realizar una copia de seguridad.

   Cada base de datos se lista por instancia o nombre de base de datos, la política de SLA aplicada y la elegibilidad para la copia de seguridad de registro.
3. Pulse **Ejecutar**.

   El trabajo de copia comienza y puede ver los detalles en **Trabajos y operaciones** > **Trabajos en ejecución**.

   Consejo: El botón **Ejecutar** solo está habilitado para una única copia de seguridad de base de datos, y la base de datos debe tener una política de SLA aplicada.

4. Para ejecutar trabajos de copia de seguridad para varias bases de datos, seleccione las bases de datos en el panel de copia de seguridad de Exchange y haga clic en **Seleccionar una política de SLA**.

   Para obtener más información sobre la definición de los trabajos de copia de seguridad de la política de SLA y de las opciones de trabajo de copia de seguridad, consulte "Definición de un trabajo de copia de seguridad de Acuerdo de nivel de servicio" en la página 169.

Definición de un trabajo de copia de seguridad de Acuerdo de nivel de servicio
Cuando las bases de datos de Microsoft Exchange se listan para cada una de las instancias de Exchange, seleccione y aplique una política de acuerdo de nivel de servicio (SLA) para empezar a proteger los datos.

Acerca de esta tarea

IBM Spectrum Protect Plus soporta bases de datos de Microsoft Exchange individuales o múltiples por cada trabajo de copia de seguridad de Exchange. Varios trabajos de copia de seguridad de base de datos se ejecutan secuencialmente.

Procedimiento

1. En el panel de navegación, expanda **Gestionar protección** > **Aplicaciones** > **Exchange**.
2. Seleccione una instancia de Exchange para realizar una copia de seguridad de todos los datos de dicha instancia, o pulse un nombre de instancia y, a continuación, seleccione las bases de datos individuales de la que desea realizar de copia de seguridad.
3. Pulse **Seleccionar una política de SLA** y elija una política SLA.

   Las opciones predefinidas son Oro, Plata y Bronce, cada una con frecuencias diferentes y velocidades de retención diferentes. Oro es la más frecuente con la velocidad de retención más corta. También puede crear una política de SLA personalizada o editar una política existente. Para obtener más información, consulte "Creación de una política de SLA" en la página 93.
4. Pulse **Seleccionar opciones** para definir opciones para la copia de seguridad, como por ejemplo, habilitar las copias de seguridad de registro para futuras opciones de recuperación y especificar los streams paralelos para reducir el tiempo que se tarda en realizar copias de seguridad de bases de datos grandes. Guarde los cambios.
5. Configure la política de SLA pulsando el icono de la columna **Opciones de política** de la tabla **Estado de política de SLA**.

   Para obtener más información sobre las opciones de configuración de SLA, consulte "Establecimiento de opciones de configuración de SLA para un trabajo de copia de seguridad" en la página 169.
6. Si desea ejecutar el exterior de la política del trabajo planificado, seleccione la instancia o la base de datos y a continuación, pulse **Acciones** > **Iniciar**.

   El estado cambia a **En ejecución** para el SLA elegido. Para poner en pausa en la planificación, pulse **Acciones** > **Pausar planificación** y para cancelar un trabajo después de que se haya iniciado, pulse **Acciones** > **Cancelar**.

Establecimiento de opciones de configuración de SLA para un trabajo de copia de seguridad
Después de configurar un acuerdo de nivel de servicio (SLA) para el trabajo de copia de seguridad, puede optar por configurar más opciones para ese trabajo. Las opciones adicionales de SLA incluyen la ejecución de scripts, excluyendo los recursos de la operación de copia de seguridad, y forzando una copia de seguridad base completa si es necesario.

Procedimiento

1. En la columna **Opciones de política** de la tabla **Estado de política de SLA** para el trabajo que está configurando, pulse el icono del portapapeles para especificar opciones adicionales de configuración.
2. Para definir de script anterior, seleccione **Script anterior** y lleve a cabo una de las acciones siguientes:
   - Para utilizar un servidor de script, seleccione **Utilizar servidor de scripts** y elija un script cargado en la lista **Script** o **Servidor de script**.

- Para ejecutar un script en un servidor de aplicaciones, desmarque el recuadro de selección **Utilizar servidor de scripts** y elija un servidor de aplicaciones en la lista **Servidor de aplicaciones**.

3. Para definir una configuración de script posterior, seleccione **Script posterior** y lleve a cabo una de las acciones siguientes:
   - Para utilizar un servidor de script, seleccione **Utilizar servidor de scripts** y elija un script cargado en la lista **Script** o **Servidor de script**.
   - Para ejecutar un script en un servidor de aplicaciones, desmarque el recuadro de selección **Utilizar servidor de scripts** y elija un servidor de aplicaciones en la lista **Servidor de aplicaciones**.

   Los scripts y los servidores de scripts se configuran en la página **Configuración del sistema** > **Script**. Para obtener más información sobre cómo trabajar con scripts, consulte Configuración de scripts.
4. Seleccione **Continuar trabajo/tarea en error de script** para seguir ejecutando el trabajo cuando falle el script asociado al trabajo.

   Si se selecciona esta opción, se intentará la operación de copia de seguridad o restauración y el estado de la tarea de script se notificará como COMPLETADO cuando un script complete el proceso con un código de retorno distinto de cero. Si no se selecciona esta opción, no se intentará la copia de seguridad o la restauración y el estado de la tarea de script se notificará como FALLIDO.
5. Especifique los recursos para excluirlos del trabajo de copia de seguridad. Escriba un nombre de recurso exacto en el campo **Excluir recursos**. Si no está seguro de alguno de los nombres, utilice los asteriscos de comodín especificados delante del patrón (**texto*) o después del patrón (*texto**). Se pueden escribir varios comodines con caracteres alfanuméricos estándar y con los siguientes caracteres especiales:-_ y *. Separe las entradas con un punto y coma.
6. Si desea crear una copia de seguridad completa de un recurso determinado, escriba el nombre de dicho recurso en el campo **Forzar copia de seguridad completa de los recursos**. Separe varios recursos con un punto y coma.

   Una copia de seguridad completa sustituye a la copia de seguridad existente de ese recurso solo para una aparición. Después de esto, se realizará una copia de seguridad del recurso de forma incremental como antes.
7. Pulse **Guardar**.

Copia de seguridad de los registros de base de datos de Microsoft Exchange

Puede realizar una copia de seguridad de los registros de transacciones de la base de datos para las bases de Microsoft Exchange. Las copias de seguridad de registro de Exchange se planifican utilizando el Programador de tareas de Windows. Cuando las copias de seguridad de registro están disponibles, puede ejecutar una recuperación de datos en avance durante una operación de restauración para asegurarse de que los datos se recuperan hasta el último punto posible en el tiempo.

Acerca de esta tarea

Cuando se habilitan las copias de seguridad de registro, se crea una tarea de Programador de tareas en el servidor de Exchange. La tarea ejecuta una operación de copia de seguridad de los archivos de registro de Exchange de acuerdo con la política de SLA.

Procedimiento

1. En el panel de navegación, expanda **Gestionar protección** > **Aplicaciones** > **Exchange**.
2. Pulse la instancia de Microsoft Exchange que desea proteger y, a continuación, seleccione las bases de datos de cuyos registros desea realizar una copia de seguridad.

   Consejo: La columna **Elegible para la copia de seguridad de registro** muestra las bases de datos de las cuales se pueden ejecutar copias de seguridad de registro. Si se registra una base de datos como no apta para la copia de seguridad de registro, se ofrece una explicación de ayuda contextual.
3. Pulse **Seleccionar opciones** y, a continuación, seleccione **Habilitar copia de seguridad de registro**.
4. Escriba la frecuencia de las copias de seguridad de registro en días, horas o minutos.
5. Elija la fecha de inicio, seleccione la hora de inicio de las copias de seguridad de registro y, a continuación, pulse **Guardar**.

Resultados
Se realiza una copia de seguridad de los registros de transacciones de la base de datos en el servidor vSnap de acuerdo con la frecuencia seleccionada.

Restricción: Solo se realiza una copia de seguridad de los registros de la base de datos en el nodo preferido. Solamente una instancia de Microsoft Exchange a la vez puede grabar copias de seguridad de registro en el servidor vSnap.

Los problemas de copia de seguridad de registro que surjan se muestran en las notificaciones de la alerta en IBM Spectrum Protect Plus.

Copia de seguridad de bases de datos de Exchange en un grupo de disponibilidad de base de datos
Puede realizar copia de seguridad de las bases de datos de buzón en un Grupo de disponibilidad de base de datos (DAG) de Microsoft Exchange y especificar si desea utilizar la copia activa o una copia pasiva de la base de datos para la copia de seguridad. Los servidores de Exchange en un entorno DAG sincronizan los datos entre las copias activas y pasivas para la alta disponibilidad.

Acerca de esta tarea

Con el uso de la información de un trabajo de inventario, IBM Spectrum Protect Plus proporciona una vista de DAG que muestra todas las bases de datos en un entorno DAG de Exchange. Cada base de datos tiene una copia activa en un servidor en el DAG, y una o más copias pasivas en los otros servidores. De forma predeterminada, las copias de seguridad planificadas se toman desde el servidor en el que está activa la base de datos, pero puede seleccionar un servidor distinto para realizar una copia de seguridad de una copia pasiva de la base de datos.

Procedimiento

1. En el panel de navegación, expanda **Gestionar protección** > **Aplicaciones** > **Exchange**..
2. En el panel **Copia de seguridad de Exchange**, pulse el menú **Ver** y seleccione **Grupos de disponibilidad de base de datos**.
3. Pulse el DAG de Microsoft Exchange que desea ver y, a continuación, seleccione las bases de datos de las que desea realizar la copia de seguridad.
4. Pulse **Seleccionar opciones**. En la lista **Realizar copia de seguridad del nodo preferido**, seleccione la instancia de la opción en la que se van a ejecutar las copias de seguridad.

   Con la opción **Copia de seguridad del nodo preferido**, puede seleccionar una copia pasiva de la base de datos para realizar la copia de seguridad.
5. Pulse **Seleccionar una política de SLA** y, a continuación, seleccione una política de SLA en la lista.
6. Para crear la definición de trabajo utilizando las opciones predeterminadas, pulse **Guardar**.

   Las bases de datos de DAG están programadas para los trabajos de copia de seguridad de acuerdo con las políticas de SLA seleccionadas y las opciones de nodo preferidas.
7. Para ejecutar la política seleccionada fuera de la planificación, en el panel **Estado de política de SLA**, pulse **Acciones** > **Iniciar**.

Estrategia de copia de seguridad incremental para siempre

IBM Spectrum Protect Plus proporciona una estrategia de copia de seguridad denominada *incremental para siempre*. En lugar de planificar trabajos de copia de seguridad completos , esta solución de copia de seguridad requiere solo una copia de seguridad inicial completa. Más adelante, se produce una secuencia continua de trabajos de copia de seguridad incremental.

El procesamiento de la copia de seguridad de imágenes e incremental tiene las ventajas siguientes:

- Reduce la cantidad de datos que pasan por la red
- Reduce el crecimiento de los datos porque todas las copias de seguridad incrementales solo contienen los bloques que han cambiado desde la copia de seguridad anterior
- Reduce la duración de los trabajos de copia de seguridad

El proceso incremental para siempre de IBM Spectrum Protect Plus incluye los pasos siguientes:

1. El primer trabajo de copia de seguridad crea una instantánea VSS de la aplicación Exchange. Como resultado, los archivos de base de datos están en un estado coherente de la aplicación. Los archivos de base de datos completos se copian en la ubicación de vSnap.
2. Todas las copias de seguridad posteriores crean una instantánea VSS de la aplicación Exchange. Los archivos de base de datos están en un estado coherente de la aplicación. Sin embargo, sólo los bloques de cambios de los archivos de base de datos se copian en la ubicación de vSnap.
3. Las copias de seguridad se reconstruye en cada punto en el tiempo en que se realiza una copia de seguridad, lo que hace posible recuperar la base de datos desde cualquier punto de copia de seguridad individual.

Restauración de bases de datos de Microsoft Exchange

Si los datos de una base de datos de Microsoft Exchange se pierden o se dañan, puede restaurarlos a partir de una copia de seguridad. Utilice el asistente "Restauración de instantáneas" para configurar una planificación de trabajos de restauración o una operación de restauración bajo demanda. Puede definir un trabajo que restaure los datos a la instancia original o a una instancia alternativa, con diferentes tipos de opciones de recuperación y configuraciones disponibles.

Antes de empezar

Asegúrese de que se cumplen los siguientes requisitos:

- Se ha definido al menos un trabajo de copia de seguridad de Microsoft Exchange y se ha ejecutado correctamente. Para obtener instrucciones sobre la definición de un trabajo de copia de seguridad, consulte “Definición de un trabajo de copia de seguridad de Acuerdo de nivel de servicio” en la página 169.
- Se han asignado roles y grupos de recursos de IBM Spectrum Protect Plus al usuario que define el trabajo de restauración. Para obtener más información sobre la asignación de roles, consulte Capítulo 13, “Gestión del acceso de usuarios”, en la página 303.
- Cuando se realiza una restauración desde un archivado de IBM Spectrum Protect, los archivos se migrarán a una agrupación de transferencia desde la cinta antes del inicio del trabajo. Dependiendo del tamaño de la restauración, este proceso puede tardar varias horas.

Importante: Para las operaciones de restauración granular, debe iniciar la sesión en el servidor de aplicaciones de Exchange y utilizar la GUI de MMC (Microsoft Management Console) para completar las tareas del navegador de restauración por lotes del buzón y restauración del buzón.

Procedimiento

Para restaurar los datos en una base de datos de Microsoft Exchange, lleve a cabo una de las acciones siguientes:

- Restaure una base de datos a la instancia y la ubicación originales.
- Restaure una base de datos a la instancia original con una ubicación de archivo diferente.
- Restaure una base de datos a una instancia alternativa.
- Restaure los datos del buzón utilizando la función de restauración granular.
- Restaure una base de datos en un grupo de disponibilidad de base de datos (DAG).

Restauración de una base de datos de Microsoft Exchange a la instancia original

Restaure una base de datos de Microsoft Exchange a su instancia original utilizando la modalidad de producción o la modalidad de prueba. Elija entre restaurar a la última copia de seguridad o a una versión de copia de seguridad de base de datos de Exchange anterior.

Antes de empezar

Asegúrese de que se cumplen los siguientes requisitos:

- Se ha definido al menos un trabajo de copia de seguridad de Microsoft Exchange y se ha ejecutado correctamente.

- Se han asignado roles y grupos de recursos de IBM Spectrum Protect Plus al usuario que define el trabajo de restauración. Para obtener más información sobre la asignación de roles, consulte Capítulo 13, “Gestión del acceso de usuarios”, en la página 303.

Acerca de esta tarea

Cuando restaura una base de datos a su ubicación original en modalidad de producción, no puede cambiar su nombre. Esta opción de restauración ejecuta una operación de restauración completa de producción, y los datos existentes se sobrescriben en el sitio de destino.

Procedimiento

Para definir un trabajo de restauración de Exchange, siga estos pasos:

1. En el panel de navegación, pulse **Gestionar protección** > **Aplicaciones** > **Exchange** > **Crear trabajo de restauración** para abrir el asistente "Restauración de instantáneas".

   Sugerencias:

   - También puede abrir el asistente "Restauración de instantáneas" pulsando **Trabajos y operaciones** > **Crear trabajo de restauración** > **Exchange**.
   - Para obtener un resumen en ejecución de las selecciones en el asistente "Restauración de instantáneas", mueva el cursor al icono de información en el panel de navegación del asistente.
   - Para omitir las páginas opcionales en el asistente, seleccione **Omitir pasos opcionales**.
2. En la página **Selección de origen**, complete los pasos siguientes:
   a) Pulse un origen de la lista para mostrar las bases de datos que están disponibles para las operaciones de restauración. También puede utilizar la función de búsqueda para buscar las instancias disponibles y alternar entre las instancias visualizadas mediante el filtro **Ver**.
   b) Haga clic en el icono de Signo más al lado de la base de datos que desea utilizar como origen de la operación de restauración. Puede seleccionar más de una base de datos en la lista.

      Los orígenes seleccionados se añaden a la lista de restauración situada junto a la lista de bases de datos. Para eliminar un elemento de la lista, haga clic en el icono de signo Menos al lado del elemento.
   c) Pulse **Siguiente** para continuar.
3. En la página **Instantánea de origen**, especifique la instancia de la base de datos que desee restaurar. Complete los siguientes campos y pulse **Siguiente** para continuar.

Opción	Descripción
Tipo de restauración	Seleccione el tipo de trabajo de restauración: **Bajo demanda: instantánea** Ejecuta un trabajo de restauración puntual desde una instantánea de base de datos. El trabajo de restauración se inicia inmediatamente después de la finalización del asistente. **Bajo demanda: punto en el tiempo** Ejecuta un trabajo de restauración puntual desde una copia de seguridad de un punto en el tiempo de una base de datos. El trabajo de restauración se inicia inmediatamente después de la finalización del asistente. **Recurrente** Crea un trabajo de restauración de punto en el tiempo repetitivo que se ejecuta en una planificación.
Tipo de ubicación de restauración	Seleccione un tipo de ubicación desde donde se restauran los datos:

Opción	Descripción
	Sitio El sitio en el que se hizo la copia de seguridad de las instantáneas. El sitio se define en el panel **Configuración del sistema** > **Sitio**. **Descarga de la nube** El servidor de nube en el que se han descargado las instantáneas. El servidor de nube se define en el panel **Configuración del sistema** > **Almacenamiento de copia de seguridad** > **Cloud**. **Descarga del repositorio** El servidor de repositorio donde se han descargado las instantáneas. El servidor de repositorio se define en el panel **Configuración del sistema** > **Almacenamiento de copia de seguridad** > **Servidor de repositorio**. **Archivado de nube** El servidor de nube en el que se han archivado las instantáneas. El servidor de nube se define en el panel **Configuración del sistema** > **Almacenamiento de copia de seguridad** > **Cloud**. **Archivado de repositorio** El servidor de repositorio en el que se han archivado las instantáneas. El servidor de repositorio se define en el panel **Configuración del sistema** > **Almacenamiento de copia de seguridad** > **Servidor de repositorio**.
Seleccionar una ubicación	Si está restaurando datos desde un sitio, seleccione una de las siguientes ubicaciones de restauración: **Demo** El sitio de demostración desde el que se restauran las instantáneas. **Primario** La ubicación del sitio primario desde la que se restauran las instantáneas. **Secundario** La ubicación del sitio secundario desde la que se restauran las instantáneas. Si está restaurando datos desde un servidor de nube o de repositorio, seleccione un servidor en el menú **Seleccionar una ubicación**.
Selector de fecha	Para las operaciones de restauración de instantánea bajo demanda, especifique un rango de fechas para mostrar las instantáneas disponibles dentro de ese rango de fechas.
Punto de restauración	Para las operaciones de restauración de instantánea bajo demanda, seleccione una instantánea de la lista de instantáneas disponibles en el rango de datos seleccionado.
Utilizar el servidor vSnap alternativo para el trabajo de restauración	Si está restaurando datos desde un recurso de nube o un servidor de repositorio, seleccione este recuadro para especificar un servidor de vSnap alternativo y, a continuación, seleccione un servidor en el menú **Seleccionar vSnap alternativo**. Cuando restaura datos desde un punto de restauración que se ha descargado o archivado en un servidor de repositorio o de recursos de nube, se utiliza un servidor vSnap como pasarela para completar la operación. De forma predeterminada, el servidor vSnap que se utiliza para completar la operación de restauración es el mismo servidor vSnap que se utiliza para completar las operaciones de copia de seguridad y de descarga. Para reducir la carga en el servidor vSnap, puede seleccionar un servidor vSnap alternativo para que sirva como pasarela.

4. En la página **Establecer destino**, seleccione **Restaurar a la instancia original** y pulse **Siguiente**.

5. En la página **Método de restauración**, elija una de las siguientes opciones:
   - **Probar**. En la modalidad de prueba, el agente crea una nueva base de datos utilizando los archivos de datos directamente desde el repositorio de vSnap. Este tipo de restauración se puede utilizar para realizar pruebas.
   - **Producción**. En la modalidad de producción, el agente restaura primero los archivos del volumen de vSnap al almacenamiento primario y luego crea la nueva base de datos utilizando los archivos restaurados.

   Solo para la restauración de prueba, en el campo **Nuevo nombre de base de datos**, especifique el nuevo nombre de la base de datos restaurada. El campo **Nuevo nombre de base de datos** también se visualiza cuando se elige la restauración de producción, pero es para restaurar a una nueva ubicación de base de datos en la instancia original. Para obtener instrucciones detalladas sobre esta tarea, consulte "Restauración de una base de datos de Exchange a una nueva ubicación en la instancia original" en la página 176.
6. Opcional: En la página **Opciones de trabajo**, configure opciones adicionales para el trabajo de restauración y pulse **Siguiente** para continuar.

   Opciones de recuperación
   Elija una de las siguientes opciones de recuperación:

   Sin recuperación
   Esta opción pasa por alto cualquier recuperación en avance después de la operación de restauración. La base de datos permanece en un estado `Avance pendiente` hasta que decida si desea ejecutar manualmente la recuperación en avance.

   Recuperar hasta el final de la copia de seguridad
   Restaure la base de datos seleccionada hasta el estado en el momento de creación de la copia de seguridad.

   Recuperar hasta el final de los registros disponibles
   Esta opción restaura la base de datos y aplica todos los registros disponibles (incluidos los registros más recientes que la copia de seguridad que pueden existir en el servidor de aplicaciones) para recuperar la base de datos hasta el último tiempo posible. Esta opción solo está disponible si ha seleccionado **Habilitar copia de seguridad de registro** en el trabajo de copia de seguridad.

   Recuperar hasta un momento específico
   Cuando las copias de seguridad de registro están habilitadas, esta opción restaura la base de datos y aplica registros del volumen de copia de seguridad de registro para recuperar la base de datos hasta un punto en el tiempo intermedio, especificado por el usuario. Elija la fecha y la hora seleccionando las opciones de **Por hora**.

   Opciones de aplicación
   Establezca las opciones de la aplicación:

   Número máximo de streams paralelos por base de datos
   Establezca el número máximo de streams de datos desde el almacenamiento de copias de seguridad por base de datos. Este valor se aplica a cada base de datos de la definición de trabajo. Todavía se pueden restaurar varias bases de datos en paralelo si el valor de la opción se establece en 1. Varios streams paralelos pueden mejorar la velocidad de restauración, pero el alto consumo de ancho de banda puede afectar al rendimiento general del sistema.

   Esta opción solo es aplicable cuando restaura una base de datos Exchange a su ubicación original utilizando su nombre de base de datos original.

   Opciones avanzadas
   Establezca las opciones de definición de trabajo avanzadas:

   Ejecutar la limpieza inmediatamente en caso de anomalía del trabajo
   Habilite esta opción para limpiar automáticamente los recursos asignados como parte de una restauración si falla la recuperación.

7. Opcional: En la página **Aplicar scripts**, seleccione el **Script anterior** o **Script posterior** que desea aplicar, o elija **Continuar trabajo/tarea en error de script**. Para obtener más información sobre cómo trabajar con scripts, consulte Configuración de scripts. Pulse **Siguiente** para continuar.
8. Realice una de las acciones siguientes en la página **Planificación** :
   - Si está ejecutando un trabajo bajo demanda, pulse **Siguiente**.
   - Si está configurando un trabajo recurrente, especifique un nombre para la planificación de trabajos y especifique la frecuencia y el momento en que se inicia el trabajo de restauración. Pulse **Siguiente**.
9. En la página **Revisar**, revise los valores del trabajo de restauración y pulse **Enviar** para crear el trabajo.

   Se crea el trabajo de restauración y puede comprobar su estado en **Trabajos y operaciones** > **Trabajos en ejecución**.

Restauración de una base de datos de Exchange a una nueva ubicación en la instancia original

Puede restaurar una base de datos de Microsoft Exchange a su instancia original, pero a una nueva ubicación en el servidor de aplicaciones. Elija entre restaurar a la última copia de seguridad o a una versión de copia de seguridad de base de datos de Exchange anterior.

Acerca de esta tarea

Cuando restaura una base de datos a la instancia original utilizando una operación de restauración de producción, puede restaurarla a una nueva ubicación de archivo en el servidor de aplicaciones con un nuevo nombre para la base de datos restaurada. En la modalidad de producción, el agente restaura primero los archivos del volumen de vSnap al almacenamiento primario y luego crea una nueva base de datos utilizando los archivos restaurados.

Procedimiento

Para definir un trabajo de restauración de Exchange, siga estos pasos:

1. En el panel de navegación, pulse **Gestionar protección** > **Aplicaciones** > **Exchange** > **Crear trabajo de restauración** para abrir el asistente "Restauración de instantáneas".

   Sugerencias:

   - También puede abrir el asistente "Restauración de instantáneas" pulsando **Trabajos y operaciones** > **Crear trabajo de restauración** > **Exchange**.
   - Para obtener un resumen en ejecución de las selecciones en el asistente "Restauración de instantáneas", mueva el cursor al icono de información en el panel de navegación del asistente.
   - Para omitir las páginas opcionales en el asistente, seleccione **Omitir pasos opcionales**.
2. En la página **Selección de origen**, complete los pasos siguientes:
   a) Pulse un origen de la lista para mostrar las bases de datos que están disponibles para las operaciones de restauración. También puede utilizar la función de búsqueda para buscar las instancias disponibles y alternar entre las instancias visualizadas mediante el filtro **Ver**.
   b) Haga clic en el icono de Signo más al lado de la base de datos que desea utilizar como origen de la operación de restauración. Puede seleccionar más de una base de datos en la lista.

      Los orígenes seleccionados se añaden a la lista de restauración situada junto a la lista de bases de datos. Para eliminar un elemento de la lista, haga clic en el icono de signo Menos al lado del elemento.
   c) Pulse **Siguiente** para continuar.
3. En la página **Instantánea de origen**, especifique la instancia de la base de datos que desee restaurar. Complete los siguientes campos y pulse **Siguiente** para continuar.

Opción	Descripción
Tipo de restauración	Seleccione el tipo de trabajo de restauración:

Opción	Descripción
	Bajo demanda: instantánea Ejecuta un trabajo de restauración puntual desde una instantánea de base de datos. El trabajo de restauración se inicia inmediatamente después de la finalización del asistente. **Bajo demanda: punto en el tiempo** Ejecuta un trabajo de restauración puntual desde una copia de seguridad de un punto en el tiempo de una base de datos. El trabajo de restauración se inicia inmediatamente después de la finalización del asistente. **Recurrente** Crea un trabajo de restauración de punto en el tiempo repetitivo que se ejecuta en una planificación.
Tipo de ubicación de restauración	Seleccione un tipo de ubicación desde donde se restauran los datos: **Sitio** El sitio en el que se hizo la copia de seguridad de las instantáneas. El sitio se define en el panel **Configuración del sistema** > **Sitio**. **Descarga de la nube** El servidor de nube en el que se han descargado las instantáneas. El servidor de nube se define en el panel **Configuración del sistema** > **Almacenamiento de copia de seguridad** > **Cloud**. **Descarga del repositorio** El servidor de repositorio donde se han descargado las instantáneas. El servidor de repositorio se define en el panel **Configuración del sistema** > **Almacenamiento de copia de seguridad** > **Servidor de repositorio**. **Archivado de nube** El servidor de nube en el que se han archivado las instantáneas. El servidor de nube se define en el panel **Configuración del sistema** > **Almacenamiento de copia de seguridad** > **Cloud**. **Archivado de repositorio** El servidor de repositorio en el que se han archivado las instantáneas. El servidor de repositorio se define en el panel **Configuración del sistema** > **Almacenamiento de copia de seguridad** > **Servidor de repositorio**.
Seleccionar una ubicación	Si está restaurando datos desde un sitio, seleccione una de las siguientes ubicaciones de restauración: **Demo** El sitio de demostración desde el que se restauran las instantáneas. **Primario** La ubicación del sitio primario desde la que se restauran las instantáneas. **Secundario** La ubicación del sitio secundario desde la que se restauran las instantáneas. Si está restaurando datos desde un servidor de nube o de repositorio, seleccione un servidor en el menú **Seleccionar una ubicación**.
Selector de fecha	Para las operaciones de restauración de instantánea bajo demanda, especifique un rango de fechas para mostrar las instantáneas disponibles dentro de ese rango de fechas.
Punto de restauración	Para las operaciones de restauración de instantánea bajo demanda, seleccione una instantánea de la lista de instantáneas disponibles en el rango de datos seleccionado.

Opción	Descripción
Utilizar el servidor vSnap alternativo para el trabajo de restauración	Si está restaurando datos desde un recurso de nube o un servidor de repositorio, seleccione este recuadro para especificar un servidor de vSnap alternativo y, a continuación, seleccione un servidor en el menú **Seleccionar vSnap alternativo**. Cuando restaura datos desde un punto de restauración que se ha descargado o archivado en un servidor de repositorio o de recursos de nube, se utiliza un servidor vSnap como pasarela para completar la operación. De forma predeterminada, el servidor vSnap que se utiliza para completar la operación de restauración es el mismo servidor vSnap que se utiliza para completar las operaciones de copia de seguridad y de descarga. Para reducir la carga en el servidor vSnap, puede seleccionar un servidor vSnap alternativo para que sirva como pasarela.

4. En la página **Establecer destino**, seleccione **Restaurar a la instancia original** y pulse **Siguiente**.
5. En la página **Método de restauración**, pulse la opción de restauración **Producción** .

   Consejo: Es obligatorio seleccionar la modalidad de producción para esta operación de restauración.

   a) En el campo **Nombre**, expanda el nombre de la base de datos para ver la información de vía de acceso de la base de datos existente en el servidor de aplicaciones.

   b) En el campo **Nuevo nombre de base de datos**, especifique el nuevo nombre de la base de datos restaurada.

   c) En el campo **Vía de acceso de destino**, añada la nueva ubicación del archivo de base de datos de Exchange, incluido el nombre .edb, y la ubicación de registros.
   Por ejemplo, para una base de datos denominada Database_A. edb, especifique C:\ExchangeDatabase\Database_A\Database_A. edb, y para la ubicación de los registros (**Vía de acceso de origen** E01), especifique D: \ExchangeDatabase\Logs\Database_A\
6. Opcional: En la página **Opciones de trabajo**, configure opciones adicionales para el trabajo de restauración y pulse **Siguiente** para continuar.

   Opciones de recuperación
   Elija una de las siguientes opciones de recuperación:

   Sin recuperación
   Esta opción pasa por alto cualquier recuperación en avance después de la operación de restauración. La base de datos permanece en un estado `Avance pendiente` hasta que decida si desea ejecutar manualmente la recuperación en avance.

   Recuperar hasta el final de la copia de seguridad
   Restaure la base de datos seleccionada hasta el estado en el momento de creación de la copia de seguridad.

   Recuperar hasta el final de los registros disponibles
   Esta opción restaura la base de datos y aplica todos los registros disponibles (incluidos los registros más recientes que la copia de seguridad que pueden existir en el servidor de aplicaciones) para recuperar la base de datos hasta el último tiempo posible. Esta opción solo está disponible si ha seleccionado **Habilitar copia de seguridad de registro** en el trabajo de copia de seguridad.

   Recuperar hasta un momento específico
   Cuando las copias de seguridad de registro están habilitadas, esta opción restaura la base de datos y aplica registros del volumen de copia de seguridad de registro para recuperar la base de datos hasta un punto en el tiempo intermedio, especificado por el usuario. Elija la fecha y la hora seleccionando las opciones de **Por hora**.

   Opciones de aplicación
   Establezca las opciones de la aplicación:

Número máximo de streams paralelos por base de datos
Establezca el número máximo de streams de datos desde el almacenamiento de copias de seguridad por base de datos. Este valor se aplica a cada base de datos de la definición de trabajo. Todavía se pueden restaurar varias bases de datos en paralelo si el valor de la opción se establece en 1. Varios streams paralelos pueden mejorar la velocidad de restauración, pero el alto consumo de ancho de banda puede afectar al rendimiento general del sistema.

Esta opción solo es aplicable cuando restaura una base de datos Exchange a su ubicación original utilizando su nombre de base de datos original.

Opciones avanzadas
Establezca las opciones de definición de trabajo avanzadas:

Ejecutar la limpieza inmediatamente en caso de anomalía del trabajo
Habilite esta opción para limpiar automáticamente los recursos asignados como parte de una restauración si falla la recuperación.

7. Opcional: En la página **Aplicar scripts**, seleccione el **Script anterior** o **Script posterior** que desea aplicar, o elija **Continuar trabajo/tarea en error de script**. Para obtener más información sobre cómo trabajar con scripts, consulte Configuración de scripts. Pulse **Siguiente** para continuar.
8. Realice una de las acciones siguientes en la página **Planificación** :
   - Si está ejecutando un trabajo bajo demanda, pulse **Siguiente**.
   - Si está configurando un trabajo recurrente, especifique un nombre para la planificación de trabajos y especifique la frecuencia y el momento en que se inicia el trabajo de restauración. Pulse **Siguiente**.
9. En la página **Revisar**, revise los valores del trabajo de restauración y pulse **Enviar** para crear el trabajo.
   Se crea el trabajo de restauración y puede comprobar su estado en **Trabajos y operaciones** > **Trabajos en ejecución**.

Restauración de una base de datos de Microsoft Exchange a una instancia alternativa
Puede seleccionar una copia de seguridad de base de datos de Microsoft Exchange y restaurarla an una instancia de Exchange Server en un host alternativo. Puede restaurar la base de datos en modalidad de producción o en modalidad de prueba a la instancia alternativa.

Antes de empezar
Asegúrese de que se cumplen los siguientes requisitos:

- Hay suficiente espacio disponible de disco y volúmenes dedicados asignados para la copia de los archivos.
- La estructura del sistema de archivos en el servidor de origen es la misma que la estructura del sistema de archivos en el servidor de destino. Esta estructura de sistema de archivos incluye espacios de tabla, registros en línea y el directorio de bases de datos local.

Procedimiento

1. En el panel de navegación, pulse **Gestionar protección** > **Aplicaciones** > **Exchange** > **Crear trabajo de restauración** para abrir el asistente "Restauración de instantáneas".

   Sugerencias:

   - También puede abrir el asistente "Restauración de instantáneas" pulsando **Trabajos y operaciones** > **Crear trabajo de restauración** > **Exchange**.
   - Para obtener un resumen en ejecución de las selecciones en el asistente "Restauración de instantáneas", mueva el cursor al icono de información en el panel de navegación del asistente.
   - Para omitir las páginas opcionales en el asistente, seleccione **Omitir pasos opcionales**.
2. En la página **Selección de origen**, complete los pasos siguientes:

a) Pulse un origen de la lista para mostrar las bases de datos que están disponibles para las operaciones de restauración. También puede utilizar la función de búsqueda para buscar las instancias disponibles y alternar entre las instancias visualizadas mediante el filtro **Ver**.

b) Haga clic en el icono de Signo más  al lado de la base de datos que desea utilizar como origen de la operación de restauración. Puede seleccionar más de una base de datos en la lista.

Los orígenes seleccionados se añaden a la lista de restauración situada junto a la lista de bases de datos. Para eliminar un elemento de la lista, haga clic en el icono de signo Menos  al lado del elemento.

c) Pulse **Siguiente** para continuar.

3. En la página **Instantánea de origen**, especifique la instancia de la base de datos que desee restaurar. Complete los siguientes campos y pulse **Siguiente** para continuar.

Opción	Descripción
Tipo de restauración	Seleccione el tipo de trabajo de restauración: **Bajo demanda: instantánea** Ejecuta un trabajo de restauración puntual desde una instantánea de base de datos. El trabajo de restauración se inicia inmediatamente después de la finalización del asistente. **Bajo demanda: punto en el tiempo** Ejecuta un trabajo de restauración puntual desde una copia de seguridad de un punto en el tiempo de una base de datos. El trabajo de restauración se inicia inmediatamente después de la finalización del asistente. **Recurrente** Crea un trabajo de restauración de punto en el tiempo repetitivo que se ejecuta en una planificación.
Tipo de ubicación de restauración	Seleccione un tipo de ubicación desde donde se restauran los datos: **Sitio** El sitio en el que se hizo la copia de seguridad de las instantáneas. El sitio se define en el panel **Configuración del sistema** > **Sitio**. **Descarga de la nube** El servidor de nube en el que se han descargado las instantáneas. El servidor de nube se define en el panel **Configuración del sistema** > **Almacenamiento de copia de seguridad** > **Cloud**. **Descarga del repositorio** El servidor de repositorio donde se han descargado las instantáneas. El servidor de repositorio se define en el panel **Configuración del sistema** > **Almacenamiento de copia de seguridad** > **Servidor de repositorio**. **Archivado de nube** El servidor de nube en el que se han archivado las instantáneas. El servidor de nube se define en el panel **Configuración del sistema** > **Almacenamiento de copia de seguridad** > **Cloud**. **Archivado de repositorio** El servidor de repositorio en el que se han archivado las instantáneas. El servidor de repositorio se define en el panel **Configuración del sistema** > **Almacenamiento de copia de seguridad** > **Servidor de repositorio**.
Seleccionar una ubicación	Si está restaurando datos desde un sitio, seleccione una de las siguientes ubicaciones de restauración: **Demo** El sitio de demostración desde el que se restauran las instantáneas.

Opción	Descripción
	Primario La ubicación del sitio primario desde la que se restauran las instantáneas. **Secundario** La ubicación del sitio secundario desde la que se restauran las instantáneas. Si está restaurando datos desde un servidor de nube o de repositorio, seleccione un servidor en el menú **Seleccionar una ubicación**.
Selector de fecha	Para las operaciones de restauración de instantánea bajo demanda, especifique un rango de fechas para mostrar las instantáneas disponibles dentro de ese rango de fechas.
Punto de restauración	Para las operaciones de restauración de instantánea bajo demanda, seleccione una instantánea de la lista de instantáneas disponibles en el rango de datos seleccionado.
Utilizar el servidor vSnap alternativo para el trabajo de restauración	Si está restaurando datos desde un recurso de nube o un servidor de repositorio, seleccione este recuadro para especificar un servidor de vSnap alternativo y, a continuación, seleccione un servidor en el menú **Seleccionar vSnap alternativo**. Cuando restaura datos desde un punto de restauración que se ha descargado o archivado en un servidor de repositorio o de recursos de nube, se utiliza un servidor vSnap como pasarela para completar la operación. De forma predeterminada, el servidor vSnap que se utiliza para completar la operación de restauración es el mismo servidor vSnap que se utiliza para completar las operaciones de copia de seguridad y de descarga. Para reducir la carga en el servidor vSnap, puede seleccionar un servidor vSnap alternativo para que sirva como pasarela.

4. En la página **Establecer destino**, elija **Restaurar a la instancia alternativa**, seleccione la instancia de destino a la que desea restaurar la base de datos y, a continuación, haga clic en **Siguiente**.
5. En la página **Método de restauración**, elija una de las siguientes opciones:
   - **Probar**. En la modalidad de prueba, el agente crea una nueva base de datos utilizando los archivos de datos directamente desde el repositorio de vSnap. Este tipo de restauración se puede utilizar para realizar pruebas.
   - **Producción**. En la modalidad de producción, el agente restaura primero los archivos del volumen de vSnap al almacenamiento primario y luego crea la nueva base de datos utilizando los archivos restaurados.

   a) En el campo **Nuevo nombre de base de datos**, especifique un nuevo nombre de base de datos.

   b) (Solo restauración de producción) Expanda el nombre de la base de datos para ver la información de la vía de acceso. En el campo **Vía de acceso de destino**, añada la ubicación del archivo de base de datos de Exchange en el host alternativo, incluido el nombre .edb, y la ubicación de los registros.

   Por ejemplo, para una base de datos denominada Database_A. edb, especifique C:\ExchangeDatabase\Database_A\Database_A. edb, y para la ubicación de los registros , especifique c:\ExchangeDatabase\Logs\Database_A\
6. Opcional: En la página **Opciones de trabajo**, configure opciones adicionales para el trabajo de restauración y pulse **Siguiente** para continuar.

   Opciones de recuperación
   Elija una de las siguientes opciones de recuperación:

   Sin recuperación
   Esta opción pasa por alto cualquier recuperación en avance después de la operación de restauración. La base de datos permanece en un estado `Avance pendiente` hasta que decida si desea ejecutar manualmente la recuperación en avance.

Recuperar hasta el final de la copia de seguridad
Restaure la base de datos seleccionada hasta el estado en el momento de creación de la copia de seguridad.

Recuperar hasta el final de los registros disponibles
Esta opción restaura la base de datos y aplica todos los registros disponibles (incluidos los registros más recientes que la copia de seguridad que pueden existir en el servidor de aplicaciones) para recuperar la base de datos hasta el último tiempo posible. Esta opción solo está disponible si ha seleccionado **Habilitar copia de seguridad de registro** en el trabajo de copia de seguridad.

Recuperar hasta un momento específico
Cuando las copias de seguridad de registro están habilitadas, esta opción restaura la base de datos y aplica registros del volumen de copia de seguridad de registro para recuperar la base de datos hasta un punto en el tiempo intermedio, especificado por el usuario. Elija la fecha y la hora seleccionando las opciones de **Por hora**.

Opciones de aplicación
Establezca las opciones de la aplicación:

Número máximo de streams paralelos por base de datos
Establezca el número máximo de streams de datos desde el almacenamiento de copias de seguridad por base de datos. Este valor se aplica a cada base de datos de la definición de trabajo. Todavía se pueden restaurar varias bases de datos en paralelo si el valor de la opción se establece en 1. Varios streams paralelos pueden mejorar la velocidad de restauración, pero el alto consumo de ancho de banda puede afectar al rendimiento general del sistema.

Esta opción solo es aplicable cuando restaura una base de datos Exchange a su ubicación original utilizando su nombre de base de datos original.

Opciones avanzadas
Establezca las opciones de definición de trabajo avanzadas:

Ejecutar la limpieza inmediatamente en caso de anomalía del trabajo
Habilite esta opción para limpiar automáticamente los recursos asignados como parte de una restauración si falla la recuperación.

7. Opcional: En la página **Aplicar scripts**, seleccione el **Script anterior** o **Script posterior** que desea aplicar, o elija **Continuar trabajo/tarea en error de script**. Para obtener más información sobre cómo trabajar con scripts, consulte Configuración de scripts. Pulse **Siguiente** para continuar.
8. Realice una de las acciones siguientes en la página **Planificación** :
   - Si está ejecutando un trabajo bajo demanda, pulse **Siguiente**.
   - Si está configurando un trabajo recurrente, especifique un nombre para la planificación de trabajos y especifique la frecuencia y el momento en que se inicia el trabajo de restauración. Pulse **Siguiente**.
9. En la página **Revisar**, revise los valores del trabajo de restauración y pulse **Enviar** para crear el trabajo.
   Se crea el trabajo de restauración y puede comprobar su estado en **Trabajos y operaciones** > **Trabajos en ejecución**.

Restauración de elementos de buzón individuales mediante una operación de restauración granular
Puede restaurar elementos de buzón individuales de Microsoft Exchange utilizando una operación de restauración granular y la GUI MMC (Microsoft Management Console) de IBM Spectrum Protect Plus.

Antes de empezar
Debe disponer de permisos RBAC (control de acceso basado en roles) para completar las operaciones de restauración de buzones individuales. Si los permisos RBAC no estuvieran asignados, podría encontrarse errores de configuración en la GUI MCC de IBM Spectrum Protect Plus para cada rol que falte.

Consejo:

Si se encuentran errores de configuración basados en roles en la GUI MCC de IBM Spectrum Protect Plus, puede establecer manualmente los permisos necesarios para resolver los errores (consulte “Privilegios ”

en la página 165) o bien puede ejecutar el asistente de configuración de IBM Spectrum Protect Plus para configurar automáticamente los permisos (véase el paso "14" en la página 185).

Acerca de esta tarea

Para iniciar una operación de restauración granular, complete los pasos de preparación de la GUI de IBM Spectrum Protect Plus y, a continuación, inicie la sesión en el servidor de aplicaciones de Exchange. A continuación, utilice la GUI de MMC de IBM Spectrum Protect Plus para restaurar los datos de buzón de usuario de la base de datos de recuperación que se crea mediante la operación de restauración granular. Se puede utilizar una operación de restauración granular para realizar las tareas siguientes:

- Puede restaurar elementos de buzón seleccionados en el buzón original, otro buzón en línea en el mismo servidor o en un archivo `.pst` de Unicode.
- Puede restaurar una base de datos de buzón de carpeta pública, un buzón de carpeta pública, o solo una parte del buzón, por ejemplo, una carpeta pública específica.
- Puede restaurar un buzón de archivado o una parte del buzón, por ejemplo, una carpeta específica.
- Puede restaurar mensajes de buzón de archivado a un buzón que se encuentra en Exchange Server, en un buzón de archivado o en un archivo `.pst` de Exchange Server.

Procedimiento

1. En el panel de navegación, pulse **Gestionar protección** > **Aplicaciones** > **Exchange** > **Crear trabajo de restauración** para abrir el asistente "Restauración de instantáneas".

   Sugerencias:

   - También puede abrir el asistente "Restauración de instantáneas" pulsando **Trabajos y operaciones** > **Crear trabajo de restauración** > **Exchange**.
   - Para obtener un resumen en ejecución de las selecciones en el asistente "Restauración de instantáneas", mueva el cursor al icono de información en el panel de navegación del asistente.
   - Para omitir las páginas opcionales en el asistente, seleccione **Omitir pasos opcionales**.
2. En la página **Selección de origen**, complete los pasos siguientes:
   a) Pulse un origen de la lista para mostrar las bases de datos que están disponibles para las operaciones de restauración. También puede utilizar la función de búsqueda para buscar las instancias disponibles y alternar entre las instancias visualizadas mediante el filtro **Ver**.
   b) Haga clic en el icono de Signo más al lado de la base de datos que desea utilizar como origen de la operación de restauración.

      Consejo: Debe seleccionar solo una base de datos para una operación de restauración granular. Si selecciona varias bases de datos, la opción de restauración granular no estará disponible en la página **Método de restauración**.

      El origen seleccionado se añade a la lista de restauración junto a la lista de base de datos. Para eliminar un elemento de la lista, haga clic en el icono de signo Menos al lado del elemento.
   c) Pulse **Siguiente** para continuar.
3. En la página **Instantánea de origen**, especifique la instancia de la base de datos que desee restaurar. Complete los siguientes campos y pulse **Siguiente** para continuar.

Opción	Descripción
Tipo de restauración	Seleccione el tipo de trabajo de restauración: **Bajo demanda: instantánea** Ejecuta un trabajo de restauración puntual desde una instantánea de base de datos. El trabajo de restauración se inicia inmediatamente después de la finalización del asistente.

Opción	Descripción
	Bajo demanda: punto en el tiempo Ejecuta un trabajo de restauración puntual desde una copia de seguridad de un punto en el tiempo de una base de datos. El trabajo de restauración se inicia inmediatamente después de la finalización del asistente. **Recurrente** Crea un trabajo de restauración de punto en el tiempo repetitivo que se ejecuta en una planificación.
Tipo de ubicación de restauración	Seleccione un tipo de ubicación desde donde se restauran los datos: **Sitio** El sitio en el que se hizo la copia de seguridad de las instantáneas. El sitio se define en el panel **Configuración del sistema** > **Sitio**. **Descarga de la nube** El servidor de nube en el que se han descargado las instantáneas. El servidor de nube se define en el panel **Configuración del sistema** > **Almacenamiento de copia de seguridad** > **Cloud**. **Descarga del repositorio** El servidor de repositorio donde se han descargado las instantáneas. El servidor de repositorio se define en el panel **Configuración del sistema** > **Almacenamiento de copia de seguridad** > **Servidor de repositorio**. **Archivado de nube** El servidor de nube en el que se han archivado las instantáneas. El servidor de nube se define en el panel **Configuración del sistema** > **Almacenamiento de copia de seguridad** > **Cloud**. **Archivado de repositorio** El servidor de repositorio en el que se han archivado las instantáneas. El servidor de repositorio se define en el panel **Configuración del sistema** > **Almacenamiento de copia de seguridad** > **Servidor de repositorio**.
Seleccionar una ubicación	Si está restaurando datos desde un sitio, seleccione una de las siguientes ubicaciones de restauración: **Demo** El sitio de demostración desde el que se restauran las instantáneas. **Primario** La ubicación del sitio primario desde la que se restauran las instantáneas. **Secundario** La ubicación del sitio secundario desde la que se restauran las instantáneas. Si está restaurando datos desde un servidor de nube o de repositorio, seleccione un servidor en el menú **Seleccionar una ubicación**.
Selector de fecha	Para las operaciones de restauración de instantánea bajo demanda, especifique un rango de fechas para mostrar las instantáneas disponibles dentro de ese rango de fechas.
Punto de restauración	Para las operaciones de restauración de instantánea bajo demanda, seleccione una instantánea de la lista de instantáneas disponibles en el rango de datos seleccionado.
Utilizar el servidor vSnap alternativo para	Si está restaurando datos desde un recurso de nube o un servidor de repositorio, seleccione este recuadro para especificar un servidor de vSnap alternativo y, a continuación, seleccione un servidor en el menú **Seleccionar vSnap alternativo**.

Opción	Descripción
el trabajo de restauración	Cuando restaura datos desde un punto de restauración que se ha descargado o archivado en un servidor de repositorio o de recursos de nube, se utiliza un servidor vSnap como pasarela para completar la operación. De forma predeterminada, el servidor vSnap que se utiliza para completar la operación de restauración es el mismo servidor vSnap que se utiliza para completar las operaciones de copia de seguridad y de descarga. Para reducir la carga en el servidor vSnap, puede seleccionar un servidor vSnap alternativo para que sirva como pasarela.

4. En la página **Establecer destino**, seleccione **Restaurar a la instancia original** y pulse **Siguiente**.
5. En la página **Método de restauración**, pulse **Restauración granular**.

   El nombre de la base de datos de recuperación se visualiza en el campo **Nuevo nombre de base de datos**. El nombre está formado por el nombre de la base de datos existente con el sufijo _RDB.
6. Opcional: En la página **Opciones de trabajo**, **Recuperar hasta el final de la copia de seguridad** y **Ejecutar la limpieza inmediatamente en caso de anomalía del trabajo** están seleccionadas de forma predeterminada. Pulse **Siguiente** para continuar.
7. Opcional: En la página **Aplicar scripts**, seleccione el **Script anterior** o **Script posterior** que desea aplicar, o elija **Continuar trabajo/tarea en error de script**. Para obtener más información sobre cómo trabajar con scripts, consulte Configuración de scripts. Pulse **Siguiente** para continuar.
8. Realice una de las acciones siguientes en la página **Planificación** :
   - Si está ejecutando un trabajo bajo demanda, pulse **Siguiente**.
   - Si está configurando un trabajo recurrente, especifique un nombre para la planificación de trabajos y especifique la frecuencia y el momento en que se inicia el trabajo de restauración. Pulse **Siguiente**.
9. En la página **Revisar**, revise los valores del trabajo de restauración y pulse **Enviar** para crear el trabajo.

   Se crea el trabajo de restauración y puede comprobar su estado en **Trabajos y operaciones** > **Trabajos en ejecución**.
10. En el panel de navegación, haga clic en **Trabajos y operaciones** > **Recursos activos** para ver la base de datos de recuperación y los detalles del punto de montaje.

    Consejo: Pulse el icono para visualizar un mensaje de información que describa los pasos siguientes para completar la tarea de restauración granular.
11. Conéctese a la instancia de servidor de aplicaciones de Exchange utilizando la conexión a escritorio remoto (RDC) o el sistema de red virtual (VNC) si se conecta de forma remota, o bien iniciando la sesión localmente en la máquina de Exchange Server.

    La operación de restauración granular instala e inicia automáticamente la GUI MMC de IBM Spectrum Protect Plus en el servidor de aplicaciones. Si la GUI de MMC no se puede iniciar, iníciela manualmente utilizando la vía de acceso que se proporciona en el mensaje de información de **Recursos activos**.
12. En la GUI MMC de IBM Spectrum Protect Plus, pulse el nodo **Proteger y recuperar datos** y seleccione **Exchange Server**.
13. En la pestaña **Recuperar** de la instancia de Exchange Server, pulse **Ver** > **Navegador de restauración de buzón** para ver el buzón de la base de datos de recuperación.
14. Opcional: Ejecute el asistente de configuración de IBM Spectrum Protect Plus:
    a) En el panel de navegación, pulse **Panel de instrumentos** > **Gestionar** > **Configuración** > **Asistentes** > **Configuración de IBM Spectrum Protect Plus**.
    b) En el panel **Acciones**, pulse **Iniciar**.

       El asistente de configuración ejecuta la comprobación de los requisitos.

c) Cuando las comprobaciones de requisitos se han ejecutado, pulse el enlace **Advertencias** situado junto a **Comprobación de roles de usuario**.

d) En el recuadro de diálogo de mensaje, para añadir los roles que faltan, pulse **Sí**.

e) En el asistente de configuración, pulse **Siguiente** y, a continuación, pulse **Finalizar**.

15. En el árbol **Navegador de restauración de buzón > Origen**, pulse el buzón que contiene los elementos que desea restaurar, lo cual permite examinar las carpetas y los mensajes individuales.

    Elija entre las acciones siguientes para seleccionar la carpeta o el mensaje que desea restaurar.

Tabla 19. Vista previa y filtrado de elementos de buzón

Tarea	**Acción**
Vista previa de elementos de buzón	a. Seleccione un elemento de buzón, como por ejemplo **Bandeja de entrada**, para visualizar su contenido en el panel de vista previa. b. Pulse un elemento individual en el panel de vista previa, como por ejemplo un mensaje de correo electrónico, para ver el texto del mensaje y los detalles. c. Si un elemento contiene un archivo adjunto, pulse el icono de archivo adjunto para obtener una vista previa de su contenido.
Filtrar elementos de buzón	Utilice las opciones de filtro para reducir la lista de carpetas y mensajes para restaurar: a. Pulse **Mostrar opciones de filtro** y **Añadir fila**. b. Pulse la tecla de flecha abajo en el campo **Nombre de columna** y seleccione un elemento para el filtro. Puede filtrar por el nombre de carpeta, el texto de asunto y otras opciones. **Restricción:** Puede filtrar carpetas de buzón públicas únicamente por la columna **Nombre de carpeta**. Cuando selecciona **Todo el contenido**, los elementos del buzón se filtran por nombre del archivo adjunto, remitente, asunto y cuerpo del mensaje. c. En el campo **Operador**, seleccione un operador: Contiene. d. En el campo **Valor**, especifique un valor de filtro. e. Para especificar criterios de filtro adicionales, pulse **Añadir fila**. f. Pulse **Aplicar filtro** para filtrar los mensajes y las carpetas.

16. Cuando haya seleccionado el elemento de buzón que desea restaurar, en el panel **Acciones**, pulse la tarea de restauración que desea ejecutar. Elija una de las opciones siguientes:

    - **Restaurar carpeta a buzón original**
    - **Restaurar mensajes a buzón original**
    - **Guardar contenido de mensaje de correo**

Consejo: Si pulsa **Guardar contenido de mensaje de correo**, se visualiza una ventana Guardar archivo de Windows. Especifique la ubicación y el nombre del mensaje y pulse **Guardar**.

Cuando selecciona la opción de restauración, se abre la ventana **Progreso de la restauración**, se muestra el progreso de la operación de restauración, y se restaura el elemento de buzón.

17. Para restaurar un elemento de buzón a otro buzón o archivo `.pst`, lleve a cabo los pasos siguientes.

    Nota: Puede restaurar un buzón completo a otro buzón o archivo `.pst`.

    Elija entre las acciones de la tabla siguiente:

Tabla 20. Restauración de un elemento de buzón de correo a otro buzón o archivo `.pst`

Tarea	Acción
Restaurar un elemento de buzón (o un buzón) a un buzón diferente	a. En el panel **Acciones**, pulse **Abrir buzón de Exchange**. b. Escriba el alias del buzón para identificarlo como el destino de la restauración. c. Arrastre el elemento de buzón de origen (o buzón) al buzón de destino en el panel de resultados. **Restricción:** No puede arrastrar elementos de correo o subcarpetas desde la carpeta `Elementos recuperables` hasta un buzón de destino.
Restaurar un elemento de buzón (o buzón de correo) a un archivo de carpetas personales de Outlook (`.pst`)	a. En el panel **Acciones**, pulse **Abrir archivo PST no Unicode**. b. Cuando se abra la ventana **Abrir archivo**, seleccione un archivo `.pst` existente o cree un archivo `.pst`. c. Arrastre el elemento de buzón de origen (o buzón de correo) al archivo `.pst` de destino en el panel de resultados. **Restricción:** Puede utilizar la vista **Navegador de restauración de buzón** solo con archivos `.pst` que no sean Unicode.

Tabla 20. Restauración de un elemento de buzón de correo a otro buzón o archivo `.pst` (continuación)

Tarea	Acción
Restaurar una carpeta pública	Seleccione esta acción para restaurar una carpeta pública a un buzón de carpeta pública en línea existente. Puede filtrar el buzón y restaurar una determinada carpeta pública a una carpeta pública en línea existente. En el campo **Carpeta a restaurar**, escriba el nombre de la carpeta pública que desea restaurar. • Para restaurar una subcarpeta de una carpeta padre, especifique la vía de acceso a la carpeta completa en este formato: *nombre_carpeta_padre/nombre_subcarpeta*. • Para restaurar todas las subcarpetas en una carpeta padre utilice *nombre_carpeta_padre/**. • Si la vía de acceso a la carpeta completa incluye espacios, ponga la vía de acceso a la carpeta entre comillas dobles y no añada un carácter de barra inclinada invertida (\). También puede restaurar toda o parte de una carpeta pública a un buzón de carpeta pública diferente del buzón original. En el campo **Buzón de carpeta pública de destino** especifique el buzón de carpeta pública de destino en el que desea efectuar la restauración.

18. En el panel **Acciones**, pulse **Cerrar buzón de Exchange** o **Cerrar archivo PST** para cerrar el buzón de destino o el archivo `.pst`.

    Consejo: Puede habilitar Microsoft Management Console para recopilar información de diagnóstico para ayudarle en la determinación de problemas relacionados con las operaciones de restauración. El proceso recopila archivos de configuración, archivos de rastreo y diagnósticos globales de la GUI de MMC. Para obtener más información, consulte la siguiente nota técnica: Habilitación de la información de diagnóstico en la GUI de MMC de IBM Spectrum Protect Plus(http://www.ibm.com/support/docview.wss?uid=ibm10882270).
19. Cuando haya finalizado la operación de restauración de los elementos individuales, vuelva a IBM Spectrum Protect Plus. En el panel **Trabajos y operación** > **Recursos activos**, haga clic en **Acciones** > **Cancelar restauración granular** para finalizar el proceso de restauración granular.

Restauración de buzones mediante una operación de restauración granular

Puede restaurar los buzones de Microsoft Exchange utilizando una operación de restauración granular y la GUI MMC (Microsoft Management Console) de IBM Spectrum Protect Plus.

Antes de empezar

Debe disponer de permisos RBAC (control de acceso basado en roles) para completar las operaciones de restauración de buzones individuales. Si los permisos RBAC no estuvieran asignados, podría encontrarse errores de configuración en la GUI MCC de IBM Spectrum Protect Plus para cada rol que falte.

Consejo:

Si se encuentran errores de configuración basados en roles en la GUI MCC de IBM Spectrum Protect Plus, puede establecer manualmente los permisos necesarios para resolver los errores (consulte “Privilegios ” en la página 165) o bien puede ejecutar el asistente de configuración de IBM Spectrum Protect Plus para configurar automáticamente los permisos (véase el paso “14” en la página 191).

Acerca de esta tarea

Para iniciar una operación de restauración granular, complete los pasos de preparación de la GUI de IBM Spectrum Protect Plus y, a continuación, inicie la sesión en el servidor de aplicaciones de Exchange. A continuación, utilice la GUI MMC de IBM Spectrum Protect Plus para restaurar los datos de buzón de usuario de la base de datos de recuperación creada mediante la operación de restauración granular. Se puede utilizar una operación de restauración granular para realizar las tareas siguientes:

- Puede restaurar un buzón entero o elementos del buzón seleccionados al buzón original, otro buzón en línea en el mismo servidor, o a un archivo `.pst` de Unicode.
- Puede restaurar una base de datos de buzón de carpeta pública, un buzón de carpeta pública, o solo una parte del buzón, por ejemplo, una carpeta pública específica.
- Puede restaurar un buzón de archivado o una parte del buzón, por ejemplo, una carpeta específica.
- Puede restaurar mensajes de buzón de archivado a un buzón que se encuentra en Exchange Server, en un buzón de archivado o en un archivo `.pst` de Exchange Server.

Procedimiento

1. En el panel de navegación, pulse **Gestionar protección** > **Aplicaciones** > **Exchange** > **Crear trabajo de restauración** para abrir el asistente "Restauración de instantáneas".

   Sugerencias:

   - También puede abrir el asistente "Restauración de instantáneas" pulsando **Trabajos y operaciones** > **Crear trabajo de restauración** > **Exchange**.
   - Para obtener un resumen en ejecución de las selecciones en el asistente "Restauración de instantáneas", mueva el cursor al icono de información en el panel de navegación del asistente.
   - Para omitir las páginas opcionales en el asistente, seleccione **Omitir pasos opcionales**.
2. En la página **Selección de origen**, complete los pasos siguientes:
   a) Pulse un origen de la lista para mostrar las bases de datos que están disponibles para las operaciones de restauración. También puede utilizar la función de búsqueda para buscar las instancias disponibles y alternar entre las instancias visualizadas mediante el filtro **Ver**.
   b) Haga clic en el icono de Signo más al lado de la base de datos que desea utilizar como origen de la operación de restauración.

      Consejo: Debe seleccionar solo una base de datos para una operación de restauración granular. Si selecciona varias bases de datos, la opción de restauración granular no estará disponible en la página **Método de restauración**.

      El origen seleccionado se añade a la lista de restauración junto a la lista de base de datos. Para eliminar un elemento de la lista, haga clic en el icono de signo Menos al lado del elemento.
   c) Pulse **Siguiente** para continuar.
3. En la página **Instantánea de origen**, especifique la instancia de la base de datos que desee restaurar. Complete los siguientes campos y pulse **Siguiente** para continuar.

Opción	Descripción
Tipo de restauración	Seleccione el tipo de trabajo de restauración:

Opción	Descripción
	Bajo demanda: instantánea Ejecuta un trabajo de restauración puntual desde una instantánea de base de datos. El trabajo de restauración se inicia inmediatamente después de la finalización del asistente. **Bajo demanda: punto en el tiempo** Ejecuta un trabajo de restauración puntual desde una copia de seguridad de un punto en el tiempo de una base de datos. El trabajo de restauración se inicia inmediatamente después de la finalización del asistente. **Recurrente** Crea un trabajo de restauración de punto en el tiempo repetitivo que se ejecuta en una planificación.
Tipo de ubicación de restauración	Seleccione un tipo de ubicación desde donde se restauran los datos: **Sitio** El sitio en el que se hizo la copia de seguridad de las instantáneas. El sitio se define en el panel **Configuración del sistema** > **Sitio**. **Descarga de la nube** El servidor de nube en el que se han descargado las instantáneas. El servidor de nube se define en el panel **Configuración del sistema** > **Almacenamiento de copia de seguridad** > **Cloud**. **Descarga del repositorio** El servidor de repositorio donde se han descargado las instantáneas. El servidor de repositorio se define en el panel **Configuración del sistema** > **Almacenamiento de copia de seguridad** > **Servidor de repositorio**. **Archivado de nube** El servidor de nube en el que se han archivado las instantáneas. El servidor de nube se define en el panel **Configuración del sistema** > **Almacenamiento de copia de seguridad** > **Cloud**. **Archivado de repositorio** El servidor de repositorio en el que se han archivado las instantáneas. El servidor de repositorio se define en el panel **Configuración del sistema** > **Almacenamiento de copia de seguridad** > **Servidor de repositorio**.
Seleccionar una ubicación	Si está restaurando datos desde un sitio, seleccione una de las siguientes ubicaciones de restauración: **Demo** El sitio de demostración desde el que se restauran las instantáneas. **Primario** La ubicación del sitio primario desde la que se restauran las instantáneas. **Secundario** La ubicación del sitio secundario desde la que se restauran las instantáneas. Si está restaurando datos desde un servidor de nube o de repositorio, seleccione un servidor en el menú **Seleccionar una ubicación**.
Selector de fecha	Para las operaciones de restauración de instantánea bajo demanda, especifique un rango de fechas para mostrar las instantáneas disponibles dentro de ese rango de fechas.
Punto de restauración	Para las operaciones de restauración de instantánea bajo demanda, seleccione una instantánea de la lista de instantáneas disponibles en el rango de datos seleccionado.

Opción	Descripción
Utilizar el servidor vSnap alternativo para el trabajo de restauración	Si está restaurando datos desde un recurso de nube o un servidor de repositorio, seleccione este recuadro para especificar un servidor de vSnap alternativo y, a continuación, seleccione un servidor en el menú **Seleccionar vSnap alternativo**. Cuando restaura datos desde un punto de restauración que se ha descargado o archivado en un servidor de repositorio o de recursos de nube, se utiliza un servidor vSnap como pasarela para completar la operación. De forma predeterminada, el servidor vSnap que se utiliza para completar la operación de restauración es el mismo servidor vSnap que se utiliza para completar las operaciones de copia de seguridad y de descarga. Para reducir la carga en el servidor vSnap, puede seleccionar un servidor vSnap alternativo para que sirva como pasarela.

4. En la página **Establecer destino**, seleccione **Restaurar a la instancia original** y pulse **Siguiente**.
5. En la página **Método de restauración**, pulse **Restauración granular**.

   El nombre de la base de datos de recuperación se visualiza en el campo **Nuevo nombre de base de datos**. El nombre está formado por el nombre de la base de datos existente con el sufijo _RDB.
6. Opcional: En la página **Opciones de trabajo**, **Recuperar hasta el final de la copia de seguridad** y **Ejecutar la limpieza inmediatamente en caso de anomalía del trabajo** están seleccionadas de forma predeterminada. Pulse **Siguiente** para continuar.
7. Opcional: En la página **Aplicar scripts**, seleccione el **Script anterior** o **Script posterior** que desea aplicar, o elija **Continuar trabajo/tarea en error de script**. Para obtener más información sobre cómo trabajar con scripts, consulte Configuración de scripts. Pulse **Siguiente** para continuar.
8. Realice una de las acciones siguientes en la página **Planificación** :
   - Si está ejecutando un trabajo bajo demanda, pulse **Siguiente**.
   - Si está configurando un trabajo recurrente, especifique un nombre para la planificación de trabajos y especifique la frecuencia y el momento en que se inicia el trabajo de restauración. Pulse **Siguiente**.
9. En la página **Revisar**, revise los valores del trabajo de restauración y pulse **Enviar** para crear el trabajo.

   Se crea el trabajo de restauración y puede comprobar su estado en **Trabajos y operaciones** > **Trabajos en ejecución**.
10. En el panel de navegación, haga clic en **Trabajos y operaciones** > **Recursos activos** para ver la base de datos de recuperación y los detalles del punto de montaje.

    Consejo: Pulse el icono para visualizar un mensaje de información que describa los pasos siguientes para completar la tarea de restauración granular.
11. Conéctese a la instancia de servidor de aplicaciones de Exchange utilizando la conexión a escritorio remoto (RDC) o el sistema de red virtual (VNC) si se conecta de forma remota, o bien iniciando la sesión localmente en la máquina de Exchange Server.

    La operación de restauración granular instala e inicia automáticamente la GUI MMC de IBM Spectrum Protect Plus en el servidor de aplicaciones. Si la GUI de MMC no se puede iniciar, iníciela manualmente utilizando la vía de acceso que se proporciona en el mensaje de información de **Recursos activos**.
12. En la GUI MMC de IBM Spectrum Protect Plus, pulse el nodo **Proteger y recuperar datos** y seleccione **Exchange Server**.
13. En la pestaña **Recuperar** de la instancia de Exchange Server, seleccione **Ver** > **Restauración de buzón**.

    Se muestra una lista de buzones de usuario de todas las bases de datos incluidas en la copia de seguridad.
14. Opcional: Ejecute el asistente de configuración de IBM Spectrum Protect Plus:

a) En el panel de navegación, pulse **Panel de instrumentos** > **Gestionar** > **Configuración** > **Asistentes** > **Configuración de IBM Spectrum Protect Plus**.

b) En el panel **Acciones**, pulse **Iniciar**.

El asistente de configuración ejecuta la comprobación de los requisitos.

c) Cuando las comprobaciones de requisitos se han ejecutado, pulse el enlace **Advertencias** situado junto a **Comprobación de roles de usuario**.

d) En el recuadro de diálogo de mensaje, para añadir los roles que faltan, pulse **Sí**.

e) En el asistente de configuración, pulse **Siguiente** y, a continuación, pulse **Finalizar**.

15. Seleccione uno o más buzones de la base de datos de recuperación que desea restaurar. Los buzones se listan por Nombre de buzón, Alias, Servidor, Base de datos y Tipo de buzón.

Puede restaurar únicamente los buzones que se encuentran en la base de datos de recuperación.

Consejo: Los buzones de otras bases de datos se muestran en esta vista únicamente para fines informativos. Si el buzón que desea restaurar no está en la base de datos de recuperación, utilice esta vista para determinar la base de datos de Exchange a la que se ha asignado el buzón de usuario. A continuación, puede ejecutar de nuevo la tarea de restauración granular para dicha base de datos.

16. Para completar la operación de restauración, en el panel **Acciones**, pulse una de las opciones de restauración siguientes.

Tabla 21. Opciones de restauración

Opción	**Acción**
Restaurar correo a la ubicación original	Restaure los elementos de correo a su ubicación en el momento de la operación de copia de seguridad.
Restaurar correo a una ubicación alternativa	Restaure los elementos de correo a un buzón distinto. • En la ventana **Opciones de buzón alternativo**, especifique el nombre de **Alias de buzón**. **Consejo:** Si los elementos de buzón o las tareas están marcados con un distintivo en la carpeta `Elementos recuperables` de un buzón, los elementos se restauran con el atributo del distintivo en la vista **Elementos y tareas con distintivo** del buzón de destino.
Restaurar correo a un archivo PST no Unicode **Restricción:** • Esta opción solo está disponible para Exchange Server 2013. • Cada carpeta puede contener un máximo de 16.383 elementos de correo.	Restaure los elementos de correo a un archivo de carpetas personales que no sea Unicode (`.pst`). Al restaurar los elementos de correo a un archivo `.pst` con un buzón seleccionado, se le solicitará un nombre de archivo. Al restaurar los elementos de correo a un archivo `.pst` con más de un buzón seleccionado, se le solicitará una ubicación de directorio. Cada buzón se restaura a un archivo `.pst` distinto que refleja el nombre del buzón en el directorio especificado. Si el archivo `.pst` existe, se utiliza. De lo contrario, el archivo se creará.

Tabla 21. Opciones de restauración (continuación)

Opción	Acción
Restaurar correo a archivo PST Unicode	Restaure los elementos de correo a un archivo `.pst` de Unicode. Al restaurar los elementos de correo a un archivo `.pst` con un buzón seleccionado, se le solicitará un nombre de archivo. Al restaurar los elementos de correo a un archivo `.pst` con más de un buzón seleccionado, se le solicitará una ubicación de directorio. **Consejo:** Puede especificar un nombre de vía de acceso estándar (por ejemplo, `c:\PST\mailbox.pst`) o una vía de acceso UNC (por ejemplo, `\\server\c$\PST\mailbox.pst`). Cuando se especifica una vía de acceso estándar, la vía de acceso se convierte en una vía de acceso UNC. Si UNC es una vía de acceso UNC no predeterminada, especifique directamente la vía de acceso UNC. Cada buzón se restaura a un archivo `.pst` distinto que refleja el nombre del buzón en el directorio especificado. Si el archivo `.pst` existe, se utiliza. De lo contrario, el archivo se creará.
Restaurar buzón de carpeta pública	Restaure un buzón de carpeta pública a un buzón de carpeta pública en línea. En el campo **Carpeta a restaurar**, especifique el nombre de la carpeta pública que desea restaurar: • Para restaurar una subcarpeta de una carpeta padre, especifique la vía de acceso a la carpeta completa en este formato: *nombre_carpeta_padre*/*nombre_subcarpeta*. • Para restaurar todas las subcarpetas en una carpeta padre utilice *nombre_carpeta_padre*/*. • Si la vía de acceso a la carpeta completa incluye espacios, ponga la vía de acceso a la carpeta entre comillas dobles y no añada un carácter de barra inclinada invertida (\). También puede restaurar todo el buzón de carpeta pública o parte de él a un buzón de carpeta pública distinto al original. En el campo **Buzón de carpeta pública de destino**, especifique el buzón de la carpeta pública de destino.

Tabla 21. Opciones de restauración (continuación)

Opción	Acción
Restaurar correo a buzón de archivado	Esta acción se aplica a un buzón principal o a un buzón de archivado. Seleccione esta acción para restaurar la totalidad o parte de cualquiera de los dos tipos de buzón al buzón de archivado original o a un buzón de archivado alternativo. Puede filtrar el buzón de archivado y restaurar una carpeta de buzón específica. En el campo **Carpeta a restaurar** especifique el nombre de la carpeta del buzón de archivado que desea restaurar. • Para restaurar una subcarpeta de una carpeta padre, especifique la vía de acceso a la carpeta completa en este formato: *nombre_carpeta_padre*/*nombre_subcarpeta*. • Para restaurar todas las subcarpetas en una carpeta padre utilice *nombre_carpeta_padre*/*. • Si la vía de acceso a la carpeta completa incluye espacios, ponga la vía de acceso a la carpeta entre comillas dobles y no añada un carácter de barra inclinada invertida (\). En el campo **Buzón de archivado de destino**, especifique el destino del buzón de archivado.
Excluir elementos de correo recuperables al restaurar el buzón	Aplique esta acción si está restaurando una carpeta pública, en línea o un buzón de archivado a un buzón original, un buzón alternativo o un archivo `.pst` de Unicode. Especifique **Sí** para excluir los elementos de correo de la carpeta `Elementos recuperables` de las operaciones de restauración de buzón. **No** es el valor predeterminado.

Consejo: Puede habilitar Microsoft Management Console para recopilar información de diagnóstico para ayudarle en la determinación de problemas relacionados con las operaciones de restauración. El proceso recopila archivos de configuración, archivos de rastreo y diagnósticos globales de la GUI de MMC. Para obtener más información, consulte la siguiente nota técnica: Habilitación de la información de diagnóstico en la GUI de MMC de IBM Spectrum Protect Plus(http://www.ibm.com/support/docview.wss?uid=ibm10882270).

17. Cuando haya finalizado la operación de restauración de buzón, vuelva a IBM Spectrum Protect Plus. En el panel **Trabajos y operación** > **Recursos activos**, haga clic en **Acciones** > **Cancelar restauración granular** para finalizar el proceso de restauración granular.

Restauración de copias de seguridad del grupo de disponibilidad

Con IBM Spectrum Protect Plus, puede restaurar una copia de seguridad del Grupo de disponibilidad de base de datos (DAG) de Exchange Server a la instancia original o a una instancia alternativa.

Acerca de esta tarea

En un entorno DAG, debe restaurar una base de datos a una copia de base de datos activa. Si ha seleccionado una copia de base de datos pasiva como el destino preferido de las operaciones de copia de seguridad, IBM Spectrum Protect Plus intenta restaurar de forma predeterminada la base de datos a esta copia pasiva. La operación de restauración no se ejecuta correctamente. En este caso, puede elegir

restaurar la base de datos a una instancia alternativa y, a continuación, seleccionar la copia de base de datos activa.

Procedimiento

Para definir un trabajo de restauración de Exchange, siga estos pasos:

1. En el panel de navegación, pulse **Gestionar protección** > **Aplicaciones** > **Exchange** > **Crear trabajo de restauración** para abrir el asistente "Restauración de instantáneas".

   Sugerencias:

   - También puede abrir el asistente "Restauración de instantáneas" pulsando **Trabajos y operaciones** > **Crear trabajo de restauración** > **Exchange**.
   - Para obtener un resumen en ejecución de las selecciones en el asistente "Restauración de instantáneas", mueva el cursor al icono de información en el panel de navegación del asistente.
   - Para omitir las páginas opcionales en el asistente, seleccione **Omitir pasos opcionales**.

2. En la página **Selección de origen**, siga estos pasos:
   a) Haga clic en el menú **Ver** y seleccione **Grupos de disponibilidad de base de datos**.
   b) En la lista **Grupos de disponibilidad**, pulse una instancia de Exchange para ver la lista de puntos de restauración de dicha instancia y seleccione las versiones de copia de seguridad que desea restaurar. También puede utilizar la función de búsqueda para buscar las instancias disponibles y alternar entre las instancias visualizadas mediante el filtro **Ver**.
   c) Haga clic en el icono Añadir a la lista de restauración al lado de la base de datos que desea utilizar como origen de la operación de restauración. Puede seleccionar más de una base de datos en la lista.

      Los orígenes seleccionados se añaden a la lista de restauración situada junto a la lista de bases de datos. Para eliminar un elemento del origen de lista, pulse el icono situado junto al elemento.
   d) Pulse **Siguiente** para continuar.
3. En la página **Instantánea de origen**, especifique la instancia de la base de datos que desee restaurar. Complete los siguientes campos y pulse **Siguiente** para continuar.

Opción	Descripción
Tipo de restauración	Seleccione el tipo de trabajo de restauración: **Bajo demanda: instantánea** Ejecuta un trabajo de restauración puntual desde una instantánea de base de datos. El trabajo de restauración se inicia inmediatamente después de la finalización del asistente. **Bajo demanda: punto en el tiempo** Ejecuta un trabajo de restauración puntual desde una copia de seguridad de un punto en el tiempo de una base de datos. El trabajo de restauración se inicia inmediatamente después de la finalización del asistente. **Recurrente** Crea un trabajo de restauración de punto en el tiempo repetitivo que se ejecuta en una planificación.
Tipo de ubicación de restauración	Seleccione un tipo de ubicación desde donde se restauran los datos: **Sitio** El sitio en el que se hizo la copia de seguridad de las instantáneas. El sitio se define en el panel **Configuración del sistema** > **Sitio**.

Opción	Descripción
	Descarga de la nube El servidor de nube en el que se han descargado las instantáneas. El servidor de nube se define en el panel **Configuración del sistema** > **Almacenamiento de copia de seguridad** > **Cloud**. **Descarga del repositorio** El servidor de repositorio donde se han descargado las instantáneas. El servidor de repositorio se define en el panel **Configuración del sistema** > **Almacenamiento de copia de seguridad** > **Servidor de repositorio**. **Archivado de nube** El servidor de nube en el que se han archivado las instantáneas. El servidor de nube se define en el panel **Configuración del sistema** > **Almacenamiento de copia de seguridad** > **Cloud**. **Archivado de repositorio** El servidor de repositorio en el que se han archivado las instantáneas. El servidor de repositorio se define en el panel **Configuración del sistema** > **Almacenamiento de copia de seguridad** > **Servidor de repositorio**.
Seleccionar una ubicación	Si está restaurando datos desde un sitio, seleccione una de las siguientes ubicaciones de restauración: **Demo** El sitio de demostración desde el que se restauran las instantáneas. **Primario** La ubicación del sitio primario desde la que se restauran las instantáneas. **Secundario** La ubicación del sitio secundario desde la que se restauran las instantáneas. Si está restaurando datos desde un servidor de nube o de repositorio, seleccione un servidor en el menú **Seleccionar una ubicación**.
Selector de fecha	Para las operaciones de restauración de instantánea bajo demanda, especifique un rango de fechas para mostrar las instantáneas disponibles dentro de ese rango de fechas.
Punto de restauración	Para las operaciones de restauración de instantánea bajo demanda, seleccione una instantánea de la lista de instantáneas disponibles en el rango de datos seleccionado.
Utilizar el servidor vSnap alternativo para el trabajo de restauración	Si está restaurando datos desde un recurso de nube o un servidor de repositorio, seleccione este recuadro para especificar un servidor de vSnap alternativo y, a continuación, seleccione un servidor en el menú **Seleccionar vSnap alternativo**. Cuando restaura datos desde un punto de restauración que se ha descargado o archivado en un servidor de repositorio o de recursos de nube, se utiliza un servidor vSnap como pasarela para completar la operación. De forma predeterminada, el servidor vSnap que se utiliza para completar la operación de restauración es el mismo servidor vSnap que se utiliza para completar las operaciones de copia de seguridad y de descarga. Para reducir la carga en el servidor vSnap, puede seleccionar un servidor vSnap alternativo para que sirva como pasarela.

4. En la página **Establecer destino**, especifique dónde desea restaurar la base de datos y pulse **Siguiente**.

   Restaurar a la instancia original
   Seleccione esta opción para restaurar la base de datos en el servidor original.

Restaurar a la instancia alternativa
Seleccione esta opción para restaurar la base de datos en un destino local distinto del servidor original y, a continuación, seleccione la ubicación alternativa en la lista de servidores disponibles.

Atención: Cuando selecciona el destino, debe seleccionar un nodo activo como destino; de lo contrario, la operación de restauración falla.

5. En la página **Método de restauración**, elija una de las siguientes opciones:
   - **Probar**. Seleccione esta opción para restaurar directamente los datos desde el repositorio de vSnap. Este tipo de restauración se puede utilizar para realizar pruebas.
   - **Producción**. Seleccione esta opción para restaurar la base de datos completa con una operación de restauración de datos de copia completa. Esta operación de restauración es para el uso permanente de la base de datos restaurada.

   Pulse **Siguiente** para continuar.
6. Opcional: En la página **Opciones de trabajo**, configure opciones adicionales para el trabajo de restauración y pulse **Siguiente** para continuar.

   Opciones de recuperación
   Elija una de las siguientes opciones de recuperación:

   Sin recuperación
   Esta opción pasa por alto cualquier recuperación en avance después de la operación de restauración. La base de datos permanece en un estado `Avance pendiente` hasta que decida si desea ejecutar manualmente la recuperación en avance.

   Recuperar hasta el final de la copia de seguridad
   Restaure la base de datos seleccionada hasta el estado en el momento de creación de la copia de seguridad.

   Recuperar hasta el final de los registros disponibles
   Esta opción restaura la base de datos y aplica todos los registros disponibles (incluidos los registros más recientes que la copia de seguridad que pueden existir en el servidor de aplicaciones) para recuperar la base de datos hasta el último tiempo posible. Esta opción solo está disponible si ha seleccionado **Habilitar copia de seguridad de registro** en el trabajo de copia de seguridad.

   Recuperar hasta un momento específico
   Cuando las copias de seguridad de registro están habilitadas, esta opción restaura la base de datos y aplica registros del volumen de copia de seguridad de registro para recuperar la base de datos hasta un punto en el tiempo intermedio, especificado por el usuario. Elija la fecha y la hora seleccionando las opciones de **Por hora**.

   Opciones de aplicación
   Establezca las opciones de la aplicación:

   Número máximo de streams paralelos por base de datos
   Establezca el número máximo de streams de datos desde el almacenamiento de copias de seguridad por base de datos. Este valor se aplica a cada base de datos de la definición de trabajo. Todavía se pueden restaurar varias bases de datos en paralelo si el valor de la opción se establece en 1. Varios streams paralelos pueden mejorar la velocidad de restauración, pero el alto consumo de ancho de banda puede afectar al rendimiento general del sistema.

   Esta opción solo es aplicable cuando restaura una base de datos Exchange a su ubicación original utilizando su nombre de base de datos original.

   Opciones avanzadas
   Establezca las opciones de definición de trabajo avanzadas:

   Ejecutar la limpieza inmediatamente en caso de anomalía del trabajo
   Habilite esta opción para limpiar automáticamente los recursos asignados como parte de una restauración si falla la recuperación.

7. Opcional: En la página **Aplicar scripts**, seleccione el **Script anterior** o **Script posterior** que desea aplicar, o elija **Continuar trabajo/tarea en error de script**. Para obtener más información sobre cómo trabajar con scripts, consulte Configuración de scripts. Pulse **Siguiente** para continuar.
8. Realice una de las acciones siguientes en la página **Planificación** :
   - Si está ejecutando un trabajo bajo demanda, pulse **Siguiente**.
   - Si está configurando un trabajo recurrente, especifique un nombre para la planificación de trabajos y especifique la frecuencia y el momento en que se inicia el trabajo de restauración. Pulse **Siguiente**.
9. En la página **Revisar**, revise los valores del trabajo de restauración y pulse **Enviar** para crear el trabajo.

   Se crea el trabajo de restauración y puede comprobar su estado en **Trabajos y operaciones** > **Trabajos en ejecución**.

Acceso a archivos de base de datos de Exchange con la modalidad de acceso instantáneo

Puede acceder a los archivos de base de datos de Microsoft Exchange utilizando el tipo de restauración de acceso instantáneo y montar los archivos de base de datos desde el volumen vSnap en un servidor de aplicaciones.

Acerca de esta tarea

En modalidad de acceso instantáneo, no se realiza ninguna acción adicional después de que IBM Spectrum Protect Plus monte la unidad compartida. Utilice los datos para la recuperación personalizada de datos de los archivos en el volumen de vSnap.

Procedimiento

1. En el panel de navegación, pulse **Gestionar protección** > **Aplicaciones** > **Exchange** > **Crear trabajo de restauración** para abrir el asistente "Restauración de instantáneas".

   Sugerencias:

   - También puede abrir el asistente "Restauración de instantáneas" pulsando **Trabajos y operaciones** > **Crear trabajo de restauración** > **Exchange**.
   - Para obtener un resumen en ejecución de las selecciones en el asistente "Restauración de instantáneas", mueva el cursor al icono de información en el panel de navegación del asistente.
   - Para omitir las páginas opcionales en el asistente, seleccione **Omitir pasos opcionales**.
2. En la página **Selección de origen**, complete los pasos siguientes:
   a) Pulse un origen de la lista para mostrar las bases de datos que están disponibles para las operaciones de restauración. También puede utilizar la función de búsqueda para buscar las instancias disponibles y alternar entre las instancias visualizadas mediante el filtro **Ver**.

   b) Haga clic en el icono de Signo más al lado de la base de datos que desea utilizar como origen de la operación de restauración. Puede seleccionar más de una base de datos en la lista.

   Los orígenes seleccionados se añaden a la lista de restauración situada junto a la lista de bases de datos. Para eliminar un elemento de la lista, haga clic en el icono de signo Menos al lado del elemento.

   c) Pulse **Siguiente** para continuar.
3. En la página **Instantánea de origen**, especifique la instancia de la base de datos que desee restaurar. Complete los siguientes campos y pulse **Siguiente** para continuar.

Opción	Descripción
Tipo de restauración	Seleccione el tipo de trabajo de restauración:

Opción	Descripción
	Bajo demanda: instantánea Ejecuta un trabajo de restauración puntual desde una instantánea de base de datos. El trabajo de restauración se inicia inmediatamente después de la finalización del asistente. **Bajo demanda: punto en el tiempo** Ejecuta un trabajo de restauración puntual desde una copia de seguridad de un punto en el tiempo de una base de datos. El trabajo de restauración se inicia inmediatamente después de la finalización del asistente. **Recurrente** Crea un trabajo de restauración de punto en el tiempo repetitivo que se ejecuta en una planificación.
Tipo de ubicación de restauración	Seleccione un tipo de ubicación desde donde se restauran los datos: **Sitio** El sitio en el que se hizo la copia de seguridad de las instantáneas. El sitio se define en el panel **Configuración del sistema** > **Sitio**. **Descarga de la nube** El servidor de nube en el que se han descargado las instantáneas. El servidor de nube se define en el panel **Configuración del sistema** > **Almacenamiento de copia de seguridad** > **Cloud**. **Descarga del repositorio** El servidor de repositorio donde se han descargado las instantáneas. El servidor de repositorio se define en el panel **Configuración del sistema** > **Almacenamiento de copia de seguridad** > **Servidor de repositorio**. **Archivado de nube** El servidor de nube en el que se han archivado las instantáneas. El servidor de nube se define en el panel **Configuración del sistema** > **Almacenamiento de copia de seguridad** > **Cloud**. **Archivado de repositorio** El servidor de repositorio en el que se han archivado las instantáneas. El servidor de repositorio se define en el panel **Configuración del sistema** > **Almacenamiento de copia de seguridad** > **Servidor de repositorio**.
Seleccionar una ubicación	Si está restaurando datos desde un sitio, seleccione una de las siguientes ubicaciones de restauración: **Demo** El sitio de demostración desde el que se restauran las instantáneas. **Primario** La ubicación del sitio primario desde la que se restauran las instantáneas. **Secundario** La ubicación del sitio secundario desde la que se restauran las instantáneas. Si está restaurando datos desde un servidor de nube o de repositorio, seleccione un servidor en el menú **Seleccionar una ubicación**.
Selector de fecha	Para las operaciones de restauración de instantánea bajo demanda, especifique un rango de fechas para mostrar las instantáneas disponibles dentro de ese rango de fechas.
Punto de restauración	Para las operaciones de restauración de instantánea bajo demanda, seleccione una instantánea de la lista de instantáneas disponibles en el rango de datos seleccionado.

Opción	Descripción
Utilizar el servidor vSnap alternativo para el trabajo de restauración	Si está restaurando datos desde un recurso de nube o un servidor de repositorio, seleccione este recuadro para especificar un servidor de vSnap alternativo y, a continuación, seleccione un servidor en el menú **Seleccionar vSnap alternativo**. Cuando restaura datos desde un punto de restauración que se ha descargado o archivado en un servidor de repositorio o de recursos de nube, se utiliza un servidor vSnap como pasarela para completar la operación. De forma predeterminada, el servidor vSnap que se utiliza para completar la operación de restauración es el mismo servidor vSnap que se utiliza para completar las operaciones de copia de seguridad y de descarga. Para reducir la carga en el servidor vSnap, puede seleccionar un servidor vSnap alternativo para que sirva como pasarela.

4. En la página **Establecer destino**, especifique dónde desea montar los archivos de base de datos y haga clic en **Siguiente**.

Opción	Descripción
Restaurar a ubicación original	Seleccione esta opción para montar los archivos de base de datos en el servidor original.
Restaurar a ubicación alternativa	Seleccione esta opción para montar los archivos de base de datos en un destino local que sea diferente del servidor original y, a continuación, seleccione la ubicación alternativa de la lista de servidores disponibles.

5. En la página **Método de restauración**, seleccione **Acceso instantáneo** y, a continuación, pulse **Siguiente**.
6. Opcional: En la página **Opciones de trabajo**, configure las opciones adicionales, si es necesario, y pulse **Siguiente** para continuar.
7. Opcional: En la página **Aplicar scripts**, seleccione el **Script anterior** o **Script posterior** que desea aplicar, o elija **Continuar trabajo/tarea en error de script**. Para obtener más información sobre cómo trabajar con scripts, consulte Configuración de scripts. Pulse **Siguiente** para continuar.
8. Realice una de las acciones siguientes en la página **Planificación** :
   - Si está ejecutando un trabajo bajo demanda, pulse **Siguiente**.
   - Si está configurando un trabajo recurrente, especifique un nombre para la planificación de trabajos y especifique la frecuencia y el momento en que se inicia el trabajo de restauración. Pulse **Siguiente**.
9. En la página **Revisar**, revise los valores del trabajo de restauración y pulse **Enviar** para crear el trabajo.

   Se crea el trabajo de restauración y puede comprobar su estado en **Trabajos y operaciones** > **Trabajos en ejecución**.
10. Ahora puede acceder a los archivos de base de datos de Exchange en el punto de montaje del servidor de aplicaciones y llevar a cabo cualquier acción relacionada con Exchange o personalizada que desee realizar.

    Nota: Los archivos de base de datos de Exchange en el punto de montaje son de lectura/escritura. No obstante, su actualización no modifica la copia de seguridad original.
11. Cuando finalice la operación de restauración de acceso instantáneo, vaya al panel **Recursos activos**, y pulse **Acciones** > **Cancelar restauración** para eliminar la base de datos montada y finalizar el proceso de restauración.

MongoDB

Tras añadir correctamente las instancias de MongoDB a IBM Spectrum Protect Plus, puede empezar a proteger los datos en bases de datos de MongoDB. Cree políticas de acuerdo de nivel de servicio (SLA) para realizar copias de seguridad de los datos de MongoDB y mantenerlos.

Asegúrese de que el entorno de MongoDB cumple los requisitos del sistema. Para obtener más información, consulte “Requisitos de MongoDB” en la página 37.

Requisitos previos para MongoDB

Se deben cumplir todos los requisitos del sistema y los requisitos previos para IBM Spectrum Protect Plusservidor de aplicaciones MongoDB antes de empezar a proteger los datos de MongoDB con IBM Spectrum Protect Plus.

Para requisitos del sistema MongoDB consulte MongoDB system requirements.

Para cumplir los requisitos previos de MongoDB, complete las comprobaciones y acciones siguientes.

1. Asegúrese de que ha cumplido los requisitos previos de espacio, tal como se describe en Requisitos de espacio para protección de MongoDB.
2. Establezca el límite de tamaño de archivo para el usuario de instancia de MongoDB con el mandato **ulimit** -f en ilimitado. De forma alternativa, establezca el valor en un valor suficientemente alto para permitir la copia de los archivos de base de datos más grandes en los trabajos de copia de seguridad y restauración. Si cambia el valor de **ulimit**, reinicie la instancia de MongoDB para finalizar la configuración.
3. Si está ejecutando MongoDB en un entorno de AIX o Linux, asegúrese de que la versión de sudo instalada esté en el nivel soportado.

   Para obtener más información sobre el nivel de versión, consulte “Requisitos de MongoDB” en la página 37. Para obtener información sobre el establecimiento de privilegios de sudo, consulte “Establecimiento de privilegios sudo” en la página 203.
4. Si las bases de datos de MongoDB están protegidas por la autenticación, debe configurar el control de acceso basado en roles. Para obtener más información, consulte “Roles para MongoDB” en la página 202.
5. Cada instancia de MongoDB que se va a proteger debe estar registrada en IBM Spectrum Protect Plus. Después de registrar las instancias, IBM Spectrum Protect Plus ejecuta un inventario para detectar los recursos de MongoDB. Asegúrese de que todas las instancias que desea proteger se detecten y listen correctamente.
6. Asegúrese de que el servicio SSH se está ejecutando en el puerto 22 en el servidor y que los cortafuegos están configurados para permitir que IBM Spectrum Protect Plus se conecte al servidor con SSH. El subsistema SFTP para SSH debe estar habilitado.
7. Asegúrese de que no configura los puntos de montaje anidados.

Restricciones

Se aplican las restricciones siguientes al servidor de aplicaciones de MongoDB:

- Las configuraciones de clúster con fragmentos de MongoDB se detectan cuando se ejecuta un inventario, pero estos recursos no son admisibles para operaciones de copia de seguridad o restauración.
- Los caracteres Unicode en los nombres de vía de acceso de archivo de MongoDB no pueden ser manejados por IBM Spectrum Protect Plus. Todos los nombres deben estar en ASCII.

Virtualización

Proteja el entorno de MongoDB con IBM Spectrum Protect Plus cuando se ejecuta en uno de los sistemas operativos invitados siguientes:

- Red Hat Enterprise Linux
- Máquina virtual basada en Kernel (KVM) de SUSE Linux Enterprise Server

Roles para MongoDB

Debe definir roles de control de acceso basado en roles (RBAC) para los usuarios del agente de MongoDB si la autenticación está habilitada en la base de datos de MongoDB. Cuando los roles están configurados, los usuarios pueden proteger y supervisar los recursos de MongoDB con IBM Spectrum Protect Plus de acuerdo con los roles definidos por los usuarios.

Control de acceso basado en roles para MongoDB

Para cada usuario de MongoDB, especifique los roles de acceso utilizando un mandato similar al ejemplo siguiente:

```
use admin
db.grantRolesToUser("<username>",
[ { role: "hostManager", db: "admin" },
{ role: "clusterManager", db: "admin" } ] )
```

Están disponibles los roles siguientes:

hostManager
Este rol proporciona acceso al mandato **fsyncLock**. Este acceso es necesario para copias de seguridad coherentes de la aplicación de bases de datos de MongoDB en las que el registro por diario no está habilitado. Este rol también proporciona acceso al mandato de cierre, que se utiliza durante una operación de restauración para cerrar la instancia del servidor de MongoDBa la que va dirigida la restauración.

clusterMonitor
Este rol proporciona acceso a mandatos para la supervisión y lectura del estado de la base de datos de MongoDB. Los mandatos siguientes están disponibles para usuarios con este rol:

- **getCmdLineOpts**
- **serverVersion**
- **replSetGetConfig**
- **replSetGetStatus**
- **isMaster**
- **listShards**

clusterManager
Este rol solo es necesario para ejecutar operaciones de restauración de prueba de conjuntos de réplicas. Los usuarios que ejecutan el mandato **replSetReconfig** pueden crear la instancia restaurada de un conjunto de réplicas de un único nodo. replica set. Este rol habilita el acceso de lectura y escritura durante las operaciones de restauración de prueba de conjuntos de réplicas. Sin este acceso, el nodo en el conjunto de réplicas permanecería en el estado REMOVED sin acceso de lectura y escritura. Además, este rol proporciona acceso a mandatos para leer el estado de la base de datos de MongoDB. Están disponibles los mandatos siguientes para este rol:

- **replSetReconfig**
- **getCmdLineOpts**
- **serverVersion**
- **replSetGetConfig**
- **replSetGetStatus**
- **isMaster**

- **listShards**

Requisitos previos de espacio para la protección de MongoDB
Antes de empezar a hacer una copia de seguridad de los datos de MongoDB, asegúrese de que tiene suficiente espacio libre en los hosts de destino y de origen y en el repositorio de vSnap. Es necesario espacio adicional para almacenar las copias de seguridad del gestor de volúmenes lógicos temporales (LVM) de volúmenes lógicos en los que se encuentran los datos de MongoDB. Estas copias de seguridad temporales, que se conocen como instantáneas de LVM, se crean automáticamente mediante el agente de MongoDB.

Instantáneas de LVM

Las instantáneas de LVM son copias de un punto en el tiempo específico de los volúmenes lógicos de LVM. Después de que finalice la operación de copia de archivo, el agente de IBM Spectrum Protect Plus MongoDB elimina las instantáneas de LVM anteriores en una operación de limpieza.

Para cada volumen lógico de instantánea de LVM, debe asignar al menos un 10 por ciento de espacio libre en el grupo de volúmenes. Si hay suficiente espacio libre en el grupo de volúmenes, el agente de IBM Spectrum Protect Plus MongoDB reserva hasta el 25 por ciento del tamaño de volumen lógico de origen para el volumen lógico de la instantánea.

LVM2 de Linux
Cuando se ejecuta una operación de copia de seguridad de MongoDB, MongoDB solicita una instantánea. Esta instantánea se crea en un sistema LVM (Gestión de volúmenes lógicos) para cada volumen lógico con datos o registros para la base de datos seleccionada. En sistemas Linux, los volúmenes lógicos están gestionados por LVM2.

Una instantánea de LVM2 basada en software se toma como un nuevo volumen lógico en el mismo grupo de volúmenes. Los volúmenes de instantánea se montan temporalmente en la misma máquina que ejecuta la instancia de MongoDB de modo que se puedan transferir al repositorio de vSnap.

En Linux , el gestor de volúmenes LVM2 almacena la instantánea de un volumen lógico dentro del mismo grupo de volúmenes. Debe haber suficiente espacio disponible para almacenar el volumen lógico. El volumen lógico crece en tamaño a medida que los datos cambian en el volumen de origen durante el tiempo de vida de la instantánea.

Establecimiento de privilegios sudo
Para utilizar IBM Spectrum Protect Plus para proteger los datos, debe instalar la versión necesaria del programa sudo.

Acerca de esta tarea

Configure un usuario agente de IBM Spectrum Protect Plus dedicado con los privilegios de superusuario necesarios para sudo. Esta configuración permite que los usuarios agentes ejecuten mandatos sin una contraseña.

Procedimiento

1. Cree un usuario agente emitiendo el mandato siguiente:

   `useradd -m` *`agente`*

   donde *agente* especifica el nombre del usuario agente de IBM Spectrum Protect Plus.
2. Establezca una contraseña para el nuevo usuario emitiendo el mandato siguiente:

   `passwd` *`agente_mongodb`*
3. Para habilitar privilegios de superusuario para el usuario agente, establezca el valor `!requiretty`. Al final del archivo de configuración sudo, añada las líneas siguientes:

   ```
   Defaults:agente !requiretty
   agente ALL=(ALL) NOPASSWD:ALL
   ```

Como alternativa, si el archivo de sudoers está configurado para importar configuraciones de otro directorio, por ejemplo `/etc/sudoers.d`, puede añadir las líneas en el archivo adecuado en dicho directorio. .

Adición de un servidor de aplicaciones de MongoDB

Para empezar a proteger los recursos de MongoDB, debe añadir el servidor que aloja las instancias de MongoDB y establecer las credenciales de las instancias. Repita el procedimiento para añadir todos los servidores que alojan recursos de MongoDB.

Acerca de esta tarea

Para añadir un servidor de aplicaciones de MongoDB a IBM Spectrum Protect Plus, debe tener la dirección host de la máquina.

Procedimiento

1. En el panel de navegación, expanda **Gestionar protección** > **Aplicaciones** > **MongoDB**.
2. En la ventana **MongoDB**, pulse **Gestionar servidores de aplicaciones** y, a continuación, pulse **Añadir servidor de aplicaciones** para añadir la máquina host.

3. En el formulario **Propiedades de aplicación**, especifique la dirección de host.
4. Decida si desea registrar el host con un usuario o una clave SSH.

   Si selecciona **Usuario**, puede elegir entre especificar un nuevo usuario y una nueva contraseña, o un usuario existente. Si selecciona **Clave SSH**, seleccione la clave SSH en el menú.

   Restricción: Cualquier usuario que se haya especificado debe disponer de privilegios sudo establecidos.

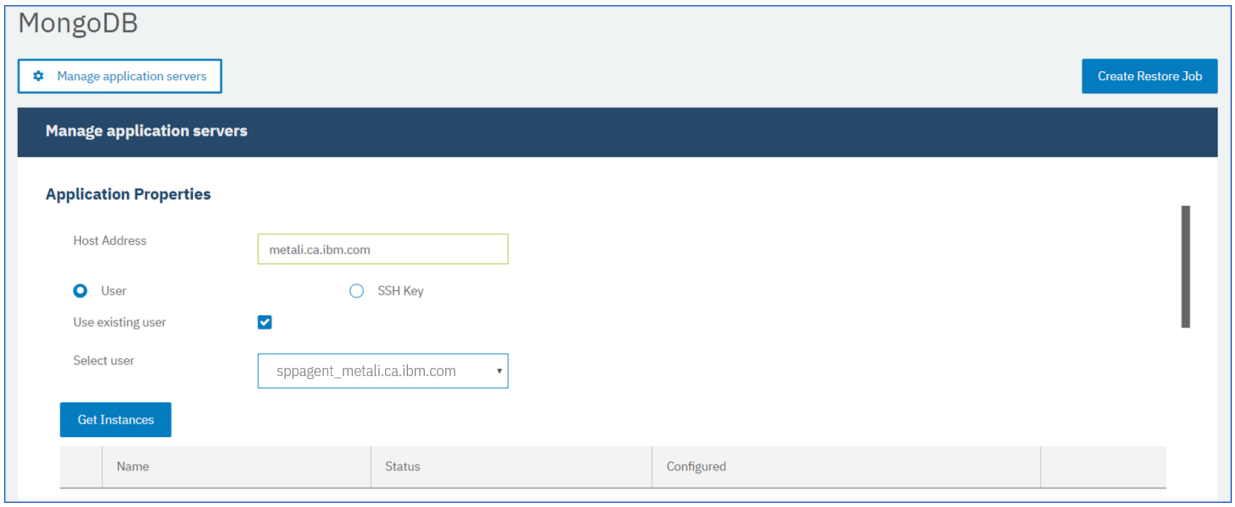


Figura 25. Adición de un agente MongoDB

5. Pulse **Obtener instancias** para detectar y listar las instancias de MongoDB que están disponibles para el servidor de host que está añadiendo.

   Cada instancia de MongoDB aparece en la lista con su dirección de host de conexión, el estado y una indicación de si está configurada.

   Atención: Si registra más de un servidor de aplicaciones para un conjunto de réplicas, el nombre de instancia que se visualiza puede cambiar después de cada operación de inventario, copia de seguridad o restauración. El nombre de host del servidor de aplicaciones añadido más reciente que pertenece al conjunto de réplicas se utiliza como parte del nombre de instancia.

Se ejecuta una operación de inventario como parte de las operaciones de copia de seguridad y restauración.

6. Si utiliza el control de acceso, configure una instancia estableciendo las credenciales. Pulse **Establecer credencial** y establezca el ID de usuario y la contraseña. Como alternativa, puede seleccionar utilizar un perfil de usuario existente.

   Para obtener más información sobre el control de acceso, consulte Capítulo 13, “Gestión del acceso de usuarios”, en la página 303.

   Cuando establezca las credenciales, debe asignar roles de usuario de MongoDB para las operaciones de copia de seguridad y restauración con acceso a los servidores de MongoDB protegidos por roles utilizando el mecanismo Salted Challenge Response Authentication Mechanism (SCRAM) o bien la autenticación de desafío y respuesta. El usuario de MongoDB que se ha asignado para el servidor de MongoDB protegido por roles requiere uno de los siguientes niveles de acceso para proteger los recursos:

   - *Gestor de host*: gestiona la base de datos como el administrador. Este rol es necesario para tomar y gestionar instantáneas.
   - *Administrador de clústeres*: recupera información de configuración y ejecuta las operaciones de restauración en modalidad de prueba de conjuntos de réplicas de MongoDB. Este rol es necesario para volver a configurar las operaciones de restauración en modalidad de prueba de conjuntos de réplicas de MongoDB para las consultas de datos.
   - *Supervisor de clúster*: supervisa la protección de recursos de MongoDB y recupera la información de configuración.
7. Opcional: Establezca la opción **Número máximo de bases de datos simultáneas** especificando un número en el campo.
8. Guarde el formulario, repita los pasos para añadir otros servidores de aplicaciones de MongoDB a IBM Spectrum Protect Plus.

Qué hacer a continuación

Después de añadir servidores de aplicaciones de MongoDB a IBM Spectrum Protect Plus, se ejecuta automáticamente un inventario en cada servidor de aplicaciones para detectar las bases de datos relevantes en esas instancias.

Para verificar si se han añadido las bases de datos, revise el registro de trabajo. Vaya a **Trabajos y operaciones**. Pulse la pestaña **Trabajos en ejecución** y busque la entrada de registro Inventario de servidor de aplicaciones más reciente.

Los trabajos completados se muestran en la pestaña **Historial de trabajos**. Puede utilizar la lista **Ordenar por** para ordenar los trabajos en función de la hora de inicio, el tipo, el estado, el nombre del trabajo o la duración. Utilice el campo **Buscar por nombre** para buscar trabajos por nombre. Puede utilizar asteriscos como caracteres comodín en el nombre.

Deben detectarse bases de datos para asegurarse de que se pueden proteger. Para obtener instrucciones sobre la ejecución de un inventario manual, consulte Detección de recursos MongoDB.

Detección de recursos de MongoDB

Después de añadir los servidores de aplicaciones MongoDB a IBM Spectrum Protect Plus, se ejecuta un inventario de forma automática para detectar todas las instancias y bases de datos de MongoDB. Puede ejecutar un inventario manual en cualquier servidor de aplicaciones para detectar, listar y almacenar todas las bases de datos de MongoDB para el host seleccionado.

Antes de empezar

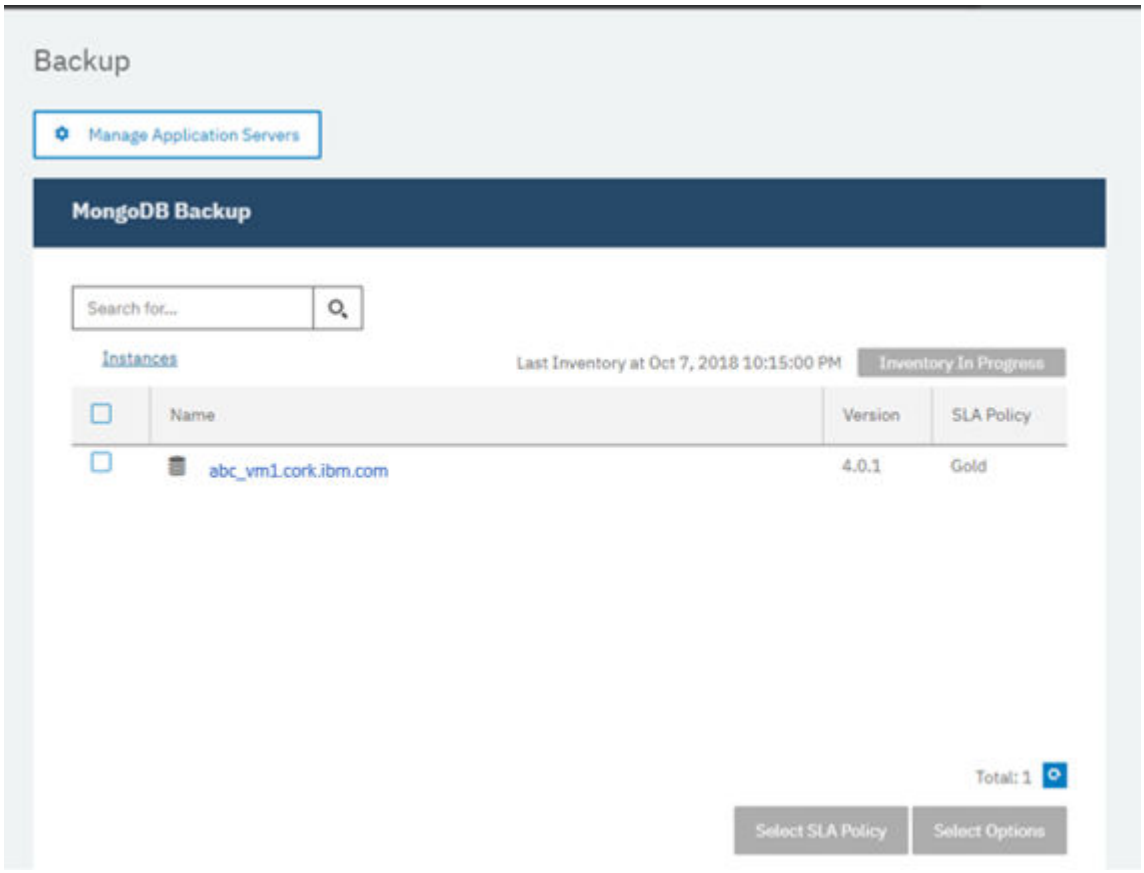
Asegúrese de que ha añadido los servidores de aplicaciones de MongoDB a IBM Spectrum Protect Plus. Para obtener instrucciones, consulte Adición de un servidor de aplicaciones de MongoDB.

Procedimiento

1. En el panel de navegación, expanda **Gestionar protección** > **Aplicaciones** > **MongoDB**.

   Consejo: Para añadir más instancias de MongoDB al panel **Instancias**, siga las instrucciones que se indican en Adición de un servidor de aplicaciones de MongoDB.

2. Pulse **Ejecutar inventario**.



   Cuando se ejecuta el inventario, el botón cambia a **Inventario en curso**. Puede ejecutar un inventario en cualquier servidor de aplicaciones disponible, pero solo puede ejecutar un proceso de inventario a la vez.

   Para supervisar el trabajo de inventario, vaya a **Trabajos y operaciones**. Pulse la pestaña **Trabajos en ejecución** y busque la entrada de registro Inventario de servidor de aplicaciones más reciente.

   Los trabajos completados se muestran en la pestaña **Historial de trabajos**. Puede utilizar la lista **Ordenar por** para ordenar los trabajos en función de la hora de inicio, el tipo, el estado, el nombre del trabajo o la duración. Utilice el campo **Buscar por nombre** para buscar trabajos por nombre. Puede utilizar asteriscos como caracteres comodín en el nombre.

3. Pulse una instancia para abrir una vista que muestre las bases de datos que se detectan para dicha instancia. Si falta alguna de las bases de datos en la lista **Instancias**, compruebe el servidor de aplicaciones de MongoDB y vuelva a ejecutar el inventario. En algunos casos, determinadas bases de datos se marcan como no admisibles para la copia de seguridad; pase el cursor por encima de la base de datos para desvelar la razón.

   Consejo: Para volver a la lista de instancias, pulse el enlace **Instancias** en el panel **Copia de seguridad de MongoDB**.

   Atención: Si registra más de un servidor de aplicaciones para un conjunto de réplicas, el nombre de instancia que se visualiza puede cambiar después de cada operación de inventario, copia de seguridad o restauración. El nombre de host del servidor de aplicaciones inventariado más recientemente que pertenece al conjunto de réplicas se utiliza como parte del nombre de

instancia. Se ejecuta una operación de inventario como parte de las operaciones de copia de seguridad y restauración.

Qué hacer a continuación

Para empezar a proteger las bases de datos de MongoDB que están catalogadas en la instancia seleccionada, aplique una política de acuerdo de nivel de servicio (SLA) a la instancia. Para obtener instrucciones sobre cómo establecer una política de SLA, consulte Definición de una política de SLA.

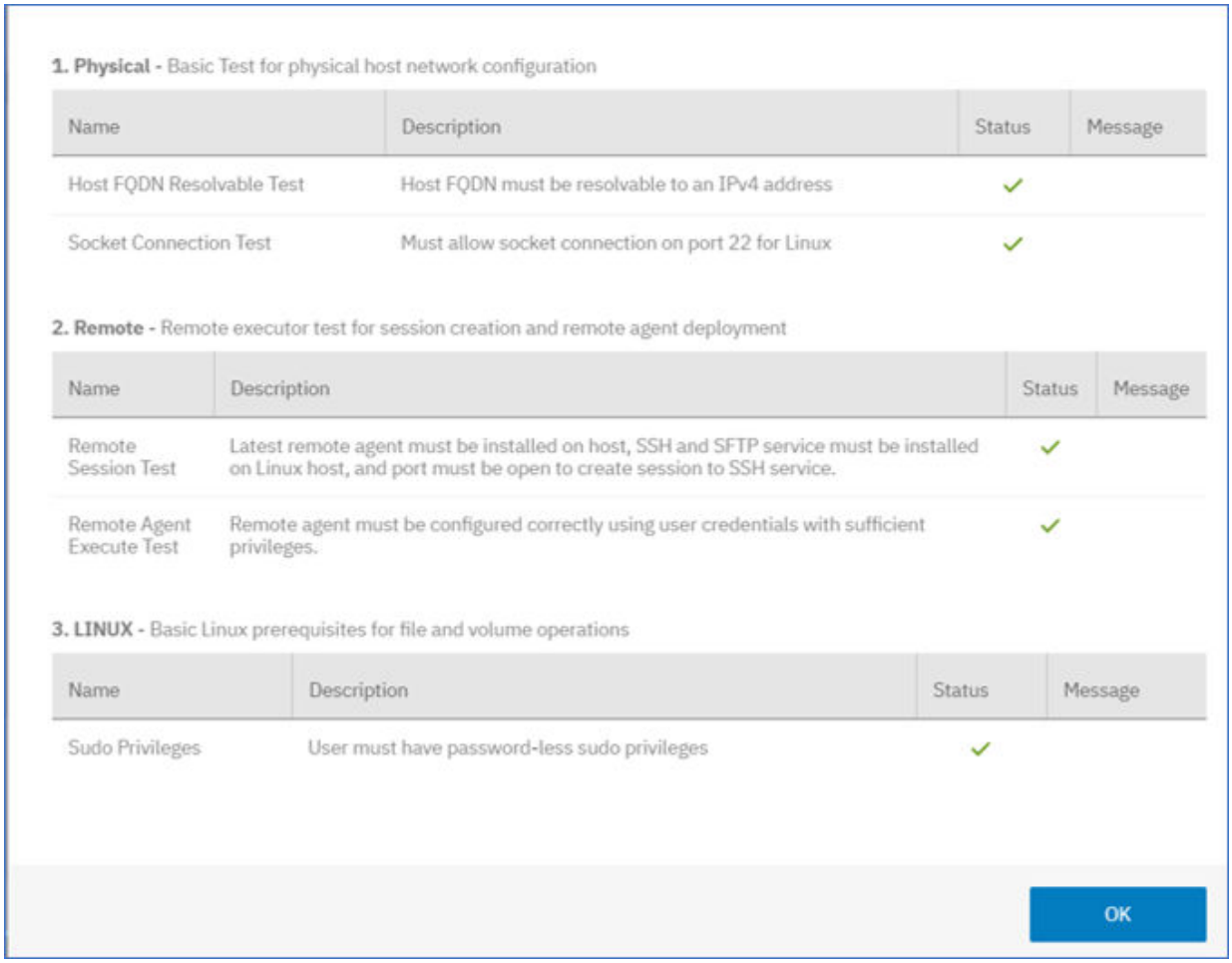
Prueba de conexión de MongoDB

Después de añadir un servidor de aplicaciones de MongoDB, puede probar la conexión. La prueba verifica la comunicación entre IBM Spectrum Protect Plus y el servidor de MongoDB. También comprueba si el área de permisos de sudo correcta está disponible para el usuario que ejecuta la prueba.

Procedimiento

1. En el panel de navegación, pulse **Gestionar protección** > **Aplicaciones** > **MongoDB**.
2. En la ventana **MongoDB**, pulse **Gestionar servidores de aplicaciones** y seleccione la dirección de host que desea probar.

   Se muestra una lista de los servidores de aplicaciones de MongoDB que están disponibles.
3. Pulse **Acciones** y seleccione **Probar** para iniciar las pruebas de verificación de las conexiones y los valores del sistema físicos y remotos.



   El informe muestra una lista que incluye las pruebas de configuración de red de host física y las pruebas de instalación del servidor remoto en el host.
4. Pulse **Aceptar** para cerrar el informe de prueba. Si se notifican problemas, soluciónelos y vuelva a ejecutar la prueba para verificar los arreglos.

Copia de seguridad de datos de MongoDB

Defina trabajos de copia de seguridad de MongoDB regulares con opciones para ejecutar y crear copias de seguridad para proteger los datos. Para realizar regularmente una copia de seguridad de los datos, defina un trabajo de copia de seguridad que incluya una política de acuerdo de nivel de servicio (SLA).

Antes de empezar

Durante la operación de copia de seguridad inicial, IBM Spectrum Protect Plus crea un nuevo volumen de vSnap y una unidad compartida de NFS. Durante las copias de seguridad incrementales, se reutiliza el volumen creado previamente. El agente IBM Spectrum Protect Plus de MongoDB monta el recurso compartido en el servidor de MongoDB en el que se ha completado la copia de seguridad.

Revise los requisitos previos siguientes antes de crear una definición de trabajo de copia de seguridad:

- Añada los servidores de aplicaciones de los que desea realizar una copia de seguridad. Para obtener información sobre el procedimiento, consulte Adición de un servidor de aplicaciones de MongoDB.
- Configure una política de SLA. Para obtener información sobre el procedimiento, consulte Definición de un trabajo de copia de seguridad de Acuerdo de nivel de servicio .
- Para que un usuario pueda configurar operaciones de copia de seguridad y restauración de IBM Spectrum Protect Plus, deben asignarse roles y grupos de recursos al usuario. Otorgue a los usuarios acceso a recursos, y operaciones de copia de seguridad y restauración, en el panel **Cuentas**. Para obtener más información, consulte Capítulo 13, “Gestión del acceso de usuarios”, en la página 303 y “Roles para MongoDB” en la página 202.

Restricción: No ejecute trabajos de inventario al mismo tiempo que se planifican trabajos de copia de seguridad.

Procedimiento

1. En el panel de navegación, expanda **Gestionar protección** > **Aplicaciones** > **MongoDB**.
2. Marque el recuadro de selección de la instancia de la que desea realizar una copia de seguridad.

   Bajo cada instancia de MongoDB, los datos de los que se va a realizar una copia de seguridad aparecen listados como **ALL**. Cada instancia del panel Instancias aparece listada por el nombre de instancia, la versión y la política de SLA aplicada.
3. Pulse **Seleccionar opciones** para especificar el número de corrientes paralelas para la operación de copia de seguridad y, a continuación, pulse **Guardar**. Si selecciona un número adecuado de streams paralelos, puede minimizar el tiempo necesario para el trabajo de copia de seguridad.

   Las opciones guardadas se utilizan para todos los trabajos de copia de seguridad de esta instancia tal como se ha seleccionado.
4. Para ejecutar el trabajo de copia de seguridad con estas opciones, pulse el nombre de la instancia, seleccione la representación de la base de datos **ALL** y pulse **Ejecutar**.

   El trabajo de copia comienza y puede ver los detalles en **Trabajos y operaciones** > **Trabajos en ejecución**.

   Consejo: El botón **Ejecutar** solo está habilitado si se aplica una política de SLA a la representación **ALL** de las bases de datos.
5. Seleccione de nuevo la instancia y pulse **Seleccionar una política de SLA** para elegir una política de SLA.
6. Guarde la selección de SLA.

   Para definir un nuevo SLA para editar una política existente con las tasas de retención y frecuencia personalizadas, seleccione **Gestionar protección** > **Descripción general de política**. En el panel **Políticas de SLA**, pulse **Añadir política de SLA** y defina las preferencias de política.

Qué hacer a continuación

Una vez guardada la política de SLA, puede ejecutar la política en cualquier momento pulsando **Acciones** junto al nombre de la política y seleccionando **Iniciar**. El estado del registro cambia para mostrar que el trabajo de copia de seguridad está en el estado En `ejecución`.

Para cancelar un trabajo que se está ejecutando, pulse **Acciones** junto al nombre de la política y seleccione **Cancelar**. Un mensaje le preguntará si desea conservar los datos de los que ya se ha realizado una copia de seguridad. Responda **Sí** si desea conservar los datos de copia de seguridad o bien **No** si desea descartar la copia de seguridad.

Definición de un trabajo de acuerdo de nivel de servicio regular

Una vez listadas las instancias de MongoDB, seleccione y aplique una política de SLA para empezar a proteger los datos.

Procedimiento

1. En el panel de navegación, expanda **Gestionar protección** > **Aplicaciones** > **MongoDB**.
2. Seleccione la instancia de MongoDB para realizar una copia de seguridad de todos los datos de dicha instancia.

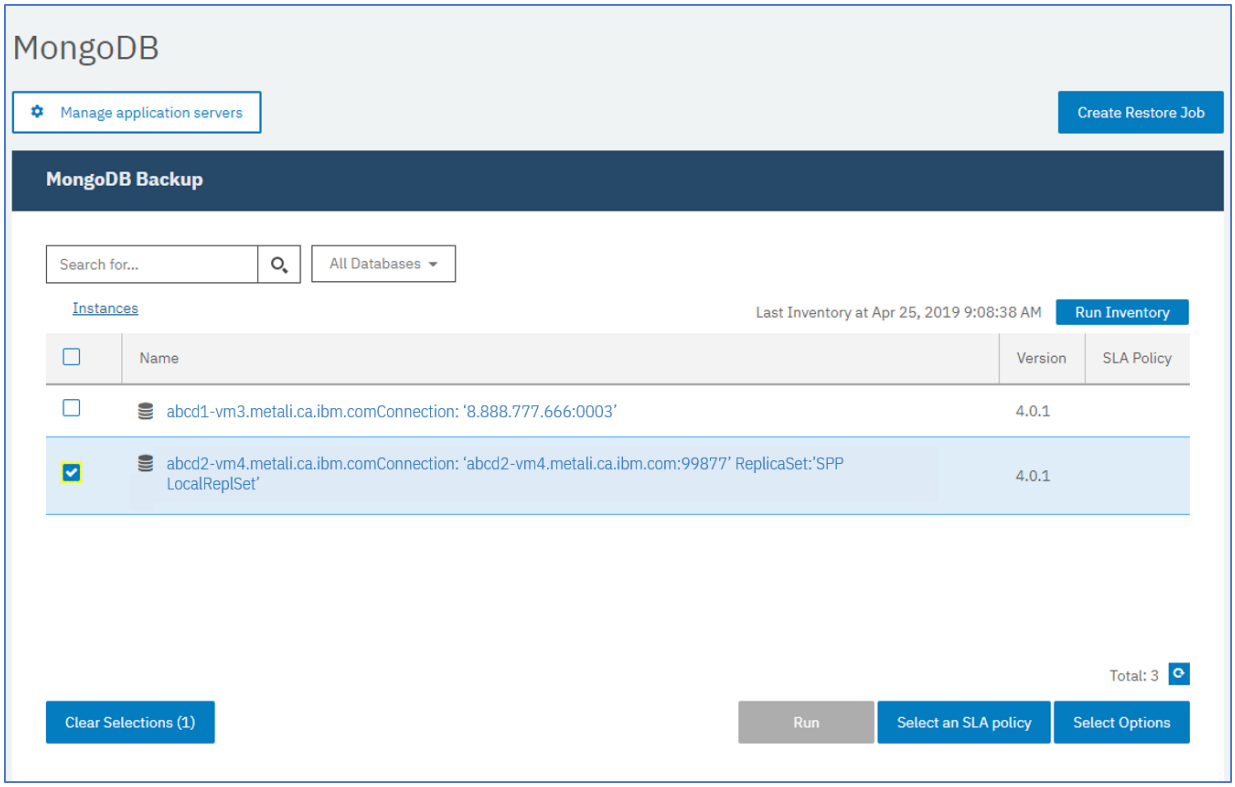


Figura 26. Panel Copia de seguridad de MongoDB que muestra las instancias

3. Pulse **Seleccionar una política de SLA** y elija una política de SLA. Guarde su selección.

   Las opciones predefinidas son Oro, Plata y Bronce, cada una con frecuencias diferentes y velocidades de retención diferentes. También puede crear una política de SLA personalizada desplazándose hasta **Descripción general de política** > **Añadir política de SLA**.
4. Opcional: Para permitir que varios streams de copia de seguridad reduzcan el tiempo que se utiliza para realizar copias de seguridad de bases de datos grandes, pulse **Seleccionar opciones** y especifique un número de streams paralelos. Guarde los cambios.

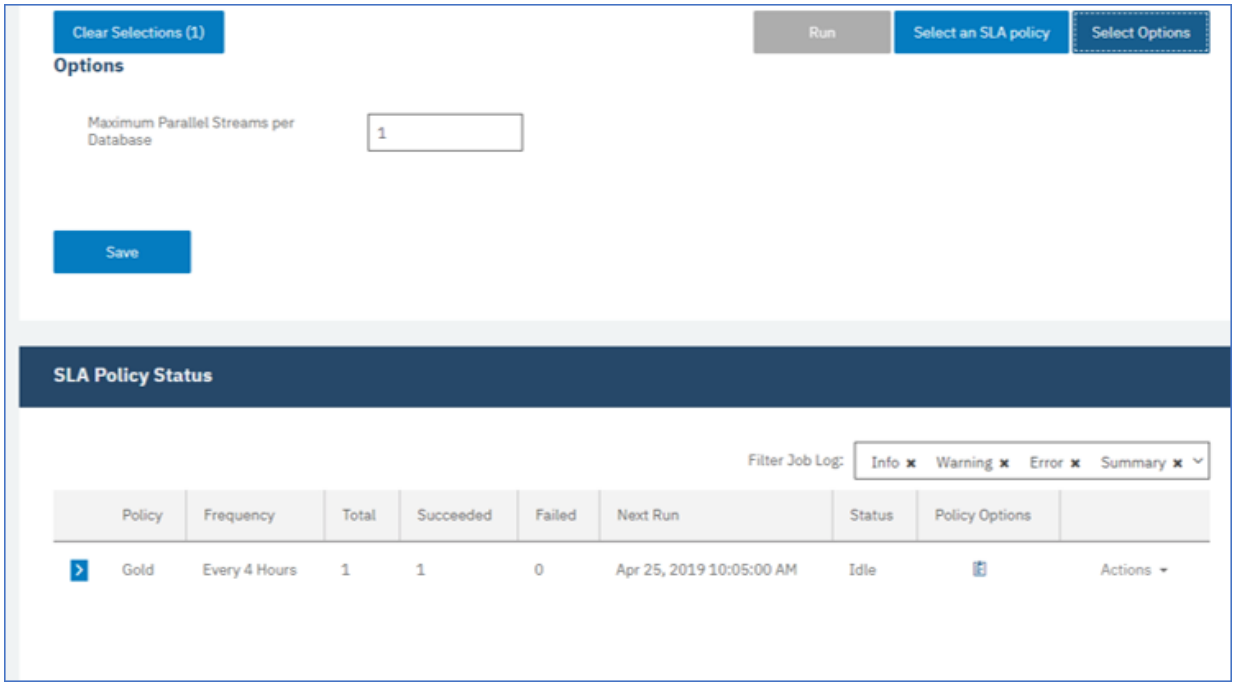


Figura 27. Opciones de copia de seguridad y estado de la política de SLA

5. Configure la política de SLA pulsando el icono de la columna **Opciones de política** de la tabla **Estado de política de SLA**.

   Para obtener más información sobre las opciones de configuración de SLA, consulte "Configuración de opciones de configuración de SLA para la copia de seguridad" en la página 210.
6. Para ejecutar la política fuera del trabajo planificado, seleccione la instancia. Pulse el botón **Acciones** y seleccione **Iniciar**. El estado cambia a **En ejecución** para el SLA elegido y puede seguir el progreso del trabajo en el registro mostrado.

Qué hacer a continuación

Una vez guardada la política de SLA, puede ejecutar la política en cualquier momento pulsando **Acciones** junto al nombre de la política y seleccionando **Iniciar**. El estado del registro cambia para mostrar que el trabajo de copia de seguridad está en el estado En `ejecución`.

Para cancelar un trabajo que se está ejecutando, pulse **Acciones** junto al nombre de la política y seleccione **Cancelar**. Un mensaje le preguntará si desea conservar los datos de los que ya se ha realizado una copia de seguridad. Responda **Sí** si desea conservar los datos de copia de seguridad o bien **No** si desea descartar la copia de seguridad.

Configuración de opciones de configuración de SLA para la copia de seguridad

Después de configurar una política de acuerdo de nivel de servicio (SLA) para el trabajo de copia de seguridad, puede optar por configurar opciones adicionales para ese trabajo. Las opciones de SLA adicionales incluyen la ejecución de scripts y la ejecución forzosa de una copia de seguridad base completa.

Procedimiento

1. En la columna **Opciones de política** de la tabla **Estado de la política de SLA** para el trabajo que está configurando, pulse el icono del portapapeles para especificar las opciones de configuración adicionales.

   Si el trabajo ya está configurado, pulse en el icono para editar la configuración.

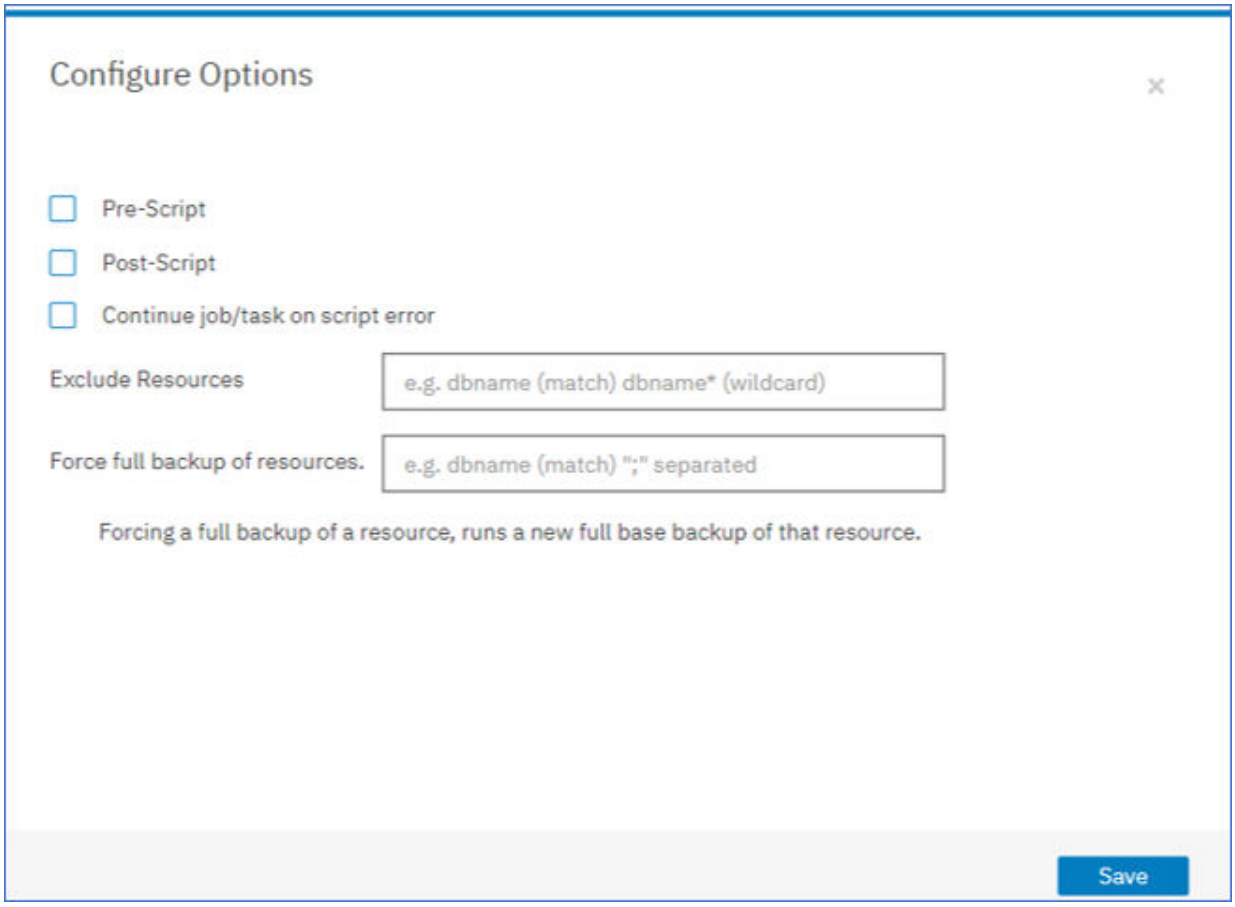


Figura 28. Especificación de opciones de configuración de SLA adicionales

2. Pulse **Script anterior** y defina la configuración de script anterior, eligiendo una de las opciones siguientes:
   - Pulse **Utilizar servidor de scripts** y seleccione un script cargado en el menú.
   - No pulse **Utilizar servidor de scripts**. Seleccione un servidor de aplicaciones en la lista para ejecutar el script en dicha ubicación.
3. Pulse **Script posterior** y defina la configuración de PostScript eligiendo una de las opciones siguientes:
   - Pulse **Utilizar servidor de scripts** y seleccione un script cargado en el menú.
   - No pulse **Utilizar servidor de scripts**. Seleccione un servidor de aplicaciones en la lista para ejecutar el script en dicha ubicación.

   Los scripts y los servidores de scripts se configuran en la página **Configuración del sistema** > **Script**. Para obtener más información sobre cómo trabajar con scripts, consulte **Configuración de scripts**.
4. Para continuar ejecutando el trabajo cuando falle el script asociado con el trabajo, seleccione **Continuar trabajo/tarea en error de script**.

   Si se selecciona esta opción, se reintentará la operación de copia de seguridad o restauración tras un fallo inicial, y el estado del script se notificará como COMPLETADO cuando un script complete el proceso con un código de retorno distinto de cero. Si no se selecciona esta opción, no se reintentará la operación de copia de seguridad o restauración y el estado de la tarea de script se notificará como FALLIDO.
5. Sáltese las opciones de **Excluir recursos** para SLA de MongoDB, dado que no puede especificar recursos para excluir. Se realizará una copia de seguridad de las instancias en lugar de las bases de datos individuales
6. Para crear una copia de seguridad completa y nueva de una instancia de MongoDB, seleccione **Forzar copia de seguridad completa de los recursos**.

Se crea una nueva copia de seguridad completa de ese recurso para sustituir la copia de seguridad existente de dicho recurso por una única aparición. Después de esto, se realizará una copia de seguridad del recurso de forma incremental como antes.

Restauración de datos de MongoDB

Para restaurar datos, defina un trabajo que restaure datos a la última copia de seguridad o seleccione una copia de seguridad anterior. Decida si desea restaurar los datos a la instancia original o a una instancia alternativa en una máquina distinta, creando una copia clonada. Defina y guarde el trabajo de restauración para que se ejecute como una operación ad hoc, o para que se ejecute regularmente como un trabajo planificado.

Antes de empezar

Antes de crear un trabajo de restauración para MongoDB, asegúrese de que se cumplen los requisitos siguientes:

- Se ha configurado como mínimo un trabajo de copia de seguridad de MongoDB y se está ejecutando correctamente. Para obtener instrucciones sobre la configuración de un trabajo de copia de seguridad, consulte "Copia de seguridad de datos de MongoDB" en la página 208.
- Se han asignado roles y grupos de recursos de IBM Spectrum Protect Plus al usuario que configura el trabajo de restauración. Para obtener instrucciones sobre la asignación de roles, consulte Capítulo 13, "Gestión del acceso de usuarios", en la página 303 y "Roles para MongoDB" en la página 202.
- Se ha asignado suficiente espacio de disco en el servidor de destino para la operación de restauración.
- Se han asignado volúmenes dedicados para la copia de archivos.
- Están disponibles la misma estructura de directorios y el mismo diseño en los servidores de origen y destino.
- Cuando se realiza una restauración desde un archivado de IBM Spectrum Protect, los archivos se migrarán a una agrupación de transferencia desde la cinta antes del inicio del trabajo. Dependiendo del tamaño de la restauración, este proceso puede tardar varias horas.

Para las operaciones de restauración a instancias alternativas, MongoDB debe estar en el mismo nivel de versión en las máquinas de destino y de host.

Para obtener más información sobre los requisitos de espacio, consulte Requisitos previos de espacio para la protección de MongoDB. Para obtener más información sobre los requisitos previos y la configuración, consulte Requisitos previos para MongoDB.

Procedimiento

Para definir un trabajo de restauración de MongoDB, complete los pasos siguientes:

1. En el panel de navegación, pulse **Gestionar protección** > **Aplicaciones** > **MongoDB** > **Crear trabajo de restauración** para abrir el asistente Restauración de instantánea.

   Sugerencias:

   - También puede iniciar el asistente de restauración de instantáneas pulsando **Trabajos y operaciones** > **Crear trabajo de restauración** > **MongoDB**.
   - Para ver un resumen en ejecución de las selecciones en el asistente de restauración de instantáneas, mueva el cursor al icono  .
   - Si desea omitir las páginas opcionales en el asistente, seleccione **Omitir pasos opcionales**.
2. En la página **Selección de origen**, complete los pasos siguientes:
   a) Pulse un origen de la lista para mostrar las bases de datos que están disponibles para las operaciones de restauración. También puede utilizar la función de búsqueda para buscar las instancias disponibles y alternar entre las instancias visualizadas mediante el filtro **Ver**.

b) Haga clic en el icono Añadir a la lista de restauración  al lado de la base de datos que desea utilizar como origen de la operación de restauración. Puede seleccionar más de una base de datos en la lista.

Los orígenes seleccionados se añaden a la lista de restauración situada junto a la lista de bases de datos. Para eliminar un elemento del origen de la lista, pulse el icono Eliminar de la lista de restauración  junto al elemento.

c) Pulse **Siguiente** para continuar.

3. En la página **Instantánea de origen**, especifique la instancia de la base de datos que desee restaurar. Complete los siguientes campos y pulse **Siguiente** para continuar.

Opción	Descripción
Tipo de restauración	Seleccione el tipo de trabajo de restauración que se va a ejecutar. **Bajo demanda: instantánea** Realiza una operación de restauración puntual a partir de una copia de seguridad de instantánea. **Bajo demanda: punto en el tiempo** Realiza una operación de restauración puntual a partir de una copia de seguridad específica de un punto en el tiempo. **Recurrente** Ejecuta las operaciones de restauración planificadas de los datos desde los últimos puntos de restauración.
Tipo de ubicación de restauración	Seleccione el tipo de ubicación desde el que se realiza la restauración: **Sitio** Restaura los datos de un sitio que está asociado con el servidor de almacenamiento de copia de seguridad. **Descarga de la nube** Restaura los datos que se almacenan en el almacenamiento en la nube. **Descarga del repositorio** Restaura los datos que se almacenan en el servidor de repositorio. **Archivado de nube** Restaura los datos que se archivan en el almacenamiento en la nube. **Archivado de repositorio** Restaura los datos que se archivan en el servidor de repositorio.
Seleccionar una ubicación	Si está restaurando datos desde un sitio, seleccione una de las siguientes ubicaciones de restauración: **Demo** Restaura los datos desde el servidor vSnap de demostración que se ha configurado con fines de prueba. **Primario** Restaura los datos desde el servidor vSnap que es el destino de copia de seguridad primario. **Secundario** Restaura los datos desde el servidor vSnap que es el destino de copia de seguridad secundario. Si restaura datos desde un servidor de nube o de repositorio, no es necesario realizar una selección, ya que la ubicación ya está seleccionada.
Selector de fecha	Para las operaciones de restauración bajo demanda, especifique el rango de fechas para el que desea mostrar las instantáneas que están disponibles.

Opción	Descripción
Punto de restauración	Para las operaciones de restauración bajo demanda, seleccione una instantánea en la lista de instantáneas disponibles en el rango de fechas seleccionado.
Utilizar el servidor vSnap alternativo para el trabajo de restauración	Seleccione este recuadro para especificar un servidor vSnap alternativo cuando restaure un punto de restauración específico desde un recurso de nube o un servidor de repositorio y, a continuación, seleccione un servidor en el menú **Seleccionar vSnap alternativo**. Cuando restaura datos desde un punto de restauración que se ha descargado a un recurso de nube o servidor de repositorio, se utiliza un servidor vSnap como pasarela para completar la operación. De forma predeterminada, el servidor vSnap que se utiliza para completar la operación de restauración es el mismo servidor vSnap que se utiliza para completar las operaciones de copia de seguridad y de descarga. Para reducir la carga en el servidor vSnap, puede seleccionar un servidor vSnap alternativo para que sirva como pasarela para la operación de restauración.

4. En la página **Establecer destino**, seleccione **Restaurar a la instancia original** para restaurar en el servidor original o **Restaurar a la instancia alternativa** para restaurar en una ubicación distinta que puede seleccionar en las ubicaciones listadas.

   Para obtener más información sobre la restauración de datos a la instancia original, consulte Restauración a la instancia original. Para obtener más información sobre la restauración de los datos a una instancia alternativa, consulte Restauración a una instancia alternativa.

5. En la página **Método de restauración**, elija el tipo de operación de restauración y pulse **Siguiente** para continuar.

   - **Prueba**: en esta modalidad, el agente crea una base de datos utilizando los archivos de datos directamente desde el repositorio de vSnap. Esta opción solo está disponible cuando se restauran los datos a una instancia alternativa. Los miembros de los conjuntos de réplicas no se reconfigurarán después de que se inicie el servidor de MongoDB. El servidor se inicia como un conjunto de réplicas de un único nodo.
   - **Producción**: en esta modalidad, el servidor de aplicaciones de MongoDB copia primero los archivos del repositorio de vSnap en el host de destino. A continuación, los datos copiados se utilizan para iniciar la base de datos. Las instancias de MongoDB que son miembros de un conjunto de réplicas no se inician durante una operación de restauración de producción. Esta acción evita que los datos se sobrescriban al conectarse al conjunto de réplicas.
   - **Acceso instantáneo**: en esta modalidad, no se emprende ninguna acción adicional después de que IBM Spectrum Protect Plus monte el recurso compartido. Utilice los datos para la recuperación personalizada de los archivos en el repositorio de vSnap.

   Para la modalidad de prueba o la modalidad de producción, puede especificar opcionalmente un nuevo nombre para la base de datos restaurada.

   Para la modalidad de producción, también puede especificar una nueva carpeta para la base de datos restaurada expandiendo la base de datos e introduciendo un nuevo nombre de carpeta.

6. Opcional: En la página **Opciones de trabajo**, configure opciones adicionales para el trabajo de restauración y pulse **Siguiente** para continuar.

   En la sección **Opciones de recuperación**, la opción **Recuperar hasta el final de la copia de seguridad** para MongoDB está seleccionada de forma predeterminada. Esta opción recupera los datos seleccionados en el estado en el que se encontraban en el momento en que se creó la copia de seguridad. La operación de recuperación utiliza los archivos de registro que se incluyen en la copia de seguridad de MongoDB.

   Opciones de aplicación

   Establezca las opciones de la aplicación:

Sobrescribir base de datos existente
Habilite esta opción para permitir que el trabajo de restauración sobrescriba la base de datos seleccionada. Si esta opción no está seleccionada, el trabajo de restauración falla cuando se encuentran los datos con el mismo nombre durante el proceso de restauración.

Atención: Asegúrese de que ningún otro dato comparte el mismo directorio de bases de datos local que los datos originales o los datos se sobrescribirán.

Número máximo de streams paralelos por base de datos
Establezca el número máximo de secuencias de datos en paralelo desde el almacenamiento de copia de seguridad por base de datos. Este valor se aplica a cada base de datos de la definición de trabajo. Todavía se pueden restaurar varias bases de datos en paralelo si el valor de la opción se establece en 1. Varios streams paralelos pueden agilizar las operaciones de restauración, pero el alto consumo de ancho de banda puede afectar al rendimiento general del sistema.

Esta opción solo es aplicable cuando restaura una base de datos MongoDB a su ubicación original utilizando su nombre de base de datos original.

Opciones avanzadas
Establezca las opciones de definición de trabajo avanzadas:

Ejecutar la limpieza inmediatamente en caso de anomalía del trabajo
Esta opción se selecciona de forma predeterminada para limpiar automáticamente los recursos asignados como parte de una operación de restauración si la recuperación no se realiza correctamente.

Permitir la sobrescritura de sesión
Seleccione esta opción para sustituir las bases de datos existentes con el mismo nombre durante una operación de restauración. Durante una operación de restauración de disco instantánea, la base de datos existente se cierra y se sobrescriben y, a continuación, se reinicia la base de datos recuperada. Si esta opción no está seleccionada y se encuentra una base de datos con el mismo nombre, la operación de restauración falla con un error.

Continúe con las restauraciones de otras bases de datos seleccionadas incluso si una falla
Si una base de datos de la instancia no se restaura correctamente, la operación de restauración continúa para los demás datos que se están restaurando. Cuando esta opción no está seleccionada, el trabajo de restauración se detiene cuando falla la recuperación de un recurso.

Prefijo de punto de montaje
Para las operaciones de restauración de **Acceso instantáneo**, especifique un prefijo de punto de montaje para la vía de acceso en la que se va a dirigir el montaje.

7. Opcional: En la página **Aplicar scripts**, especifique los scripts que pueden ejecutarse antes o después de que se ejecute un trabajo. Los scripts Batch y PowerShell están soportados en los sistemas operativos Windows mientras que los scripts de shell están soportados en los sistemas operativos Linux.

Script anterior
Seleccione este recuadro de selección para elegir un script cargado y una aplicación o un servidor de scripts en el que se ejecutará el script anterior. Para seleccionar un servidor de aplicaciones, desmarque el recuadro de selección **Utilizar servidor de scripts**. Para configurar scripts y servidores de scripts, pulse **Configuración del sistema** > **Script**.

Script posterior
Seleccione esta opción para elegir un script cargado y una aplicación o un servidor de scripts en el que se ejecutará el script posterior. Para seleccionar un servidor de aplicaciones, desmarque el recuadro de selección **Utilizar servidor de scripts**. Para configurar scripts y servidores de scripts, pulse la página **Configuración del sistema** > **Script**.

Continuar trabajo/tarea en error de script
Seleccione esta opción para continuar ejecutando el trabajo si falla el script asociado con el trabajo. Cuando esta opción está habilitada, en el caso de que un script termine de procesarse con un código de retorno distinto de cero, el trabajo de copia de seguridad o restauración

continúa ejecutándose y el estado de la tarea del script anterior se notifica como COMPLETED. Si un script posterior termina de procesarse con un código de retorno distinto de cero, el estado de la tarea del script posterior se notifica como COMPLETED. Cuando esta opción no está seleccionada, el trabajo de copia de seguridad o restauración no se ejecuta, y el estado de la tarea Script previo o Script posterior se notifica como FAILED.

Pulse **Siguiente** para continuar.

8. En la página **Planificación**, pulse **Siguiente** para iniciar los trabajos bajo demanda después de completar el asistente de restauración de instantáneas. Para los trabajos recurrentes, especifique un nombre para la planificación de trabajos y especifique la frecuencia y el momento en que se debe iniciar el trabajo de restauración.
9. En la página **Revisar** , revise los valores del trabajo de restauración.

   Atención: Revise las opciones seleccionadas antes de continuar en **Enviar**, ya que los datos se sobrescribirán cuando se seleccione la opción de aplicación **Sobrescribir datos existentes**. Puede cancelar un trabajo de restauración cuando está en curso, pero si se selecciona la opción **Sobrescribir datos existentes**, los datos se sobrescriben aunque cancele el trabajo.

10. Para continuar con el trabajo, pulse **Enviar**. Para cancelar el trabajo, vaya a **Trabajos y operaciones** y haga clic en la pestaña **Planificación** . Busque el trabajo de restauración que desea cancelar. Pulse **Acciones** y seleccione **Cancelar**.

Resultados

Unos momentos después de seleccionar **Restaurar**, el trabajo **onDemandRestore** se añade al panel **Trabajos y operaciones** > **Trabajos en ejecución**. Haga clic en el registro para mostrar los detalles paso a paso de la operación. También puede descargar el archivo de registro comprimido pulsando **Descargar.zip**. Para cualquier otro trabajo, haga clic en las pestañas **Trabajos en ejecución** o **Historial de trabajos** y pulse el trabajo para ver sus detalles.

La dirección IP y el puerto para el servidor restaurado se encuentran en el archivo de registro para la operación de restauración. Vaya a **Trabajos y operaciones** > **Trabajos en ejecución** para buscar los registros para la operación de restauración.

Para obtener información sobre la restauración de datos a la instancia original, consulte Restauración a la instancia original. Para obtener información sobre la restauración de los datos en una instancia alternativa, consulte Restauración a una instancia alternativa.

Restauración de datos de MongoDB a la instancia original

Puede restaurar una instancia de MongoDB en el host original y elegir entre la restauración en la última copia de seguridad o una versión de copia de seguridad de la base de datos de MongoDB anterior. Cuando restaure datos a su instancia original, no podrá cambiarle el nombre. Esta opción de restauración ejecuta una restauración de producción completa de los datos y los datos existentes se sobrescriben en el sitio de destino si la opción de aplicación **Sobrescribir bases de datos existentes** está seleccionada.

Antes de empezar

Antes de crear un trabajo de restauración para MongoDB, asegúrese de que se cumplen los requisitos siguientes:

- Se ha configurado como mínimo un trabajo de copia de seguridad de MongoDB y se está ejecutando correctamente. Para obtener instrucciones sobre la configuración de un trabajo de copia de seguridad, consulte “Copia de seguridad de datos de MongoDB” en la página 208.
- Se han asignado roles y grupos de recursos de IBM Spectrum Protect Plus al usuario que configura el trabajo de restauración. Para obtener instrucciones sobre la asignación de roles, consulte Capítulo 13, “Gestión del acceso de usuarios”, en la página 303 y “Roles para MongoDB” en la página 202.
- Se ha asignado suficiente espacio de disco en el servidor de destino para la operación de restauración.
- Se han asignado volúmenes dedicados para la copia de archivos.

- Están disponibles la misma estructura de directorios y el mismo diseño en los servidores de origen y destino.
- Cuando se realiza una restauración desde un archivado de IBM Spectrum Protect, los archivos se migrarán a una agrupación de transferencia desde la cinta antes del inicio del trabajo. Dependiendo del tamaño de la restauración, este proceso puede tardar varias horas.

Para obtener más información sobre los requisitos de espacio, consulte Requisitos previos de espacio para la protección de MongoDB. Para obtener más información sobre los requisitos previos y la configuración, consulte Requisitos previos para MongoDB.

Procedimiento

1. En el panel de navegación, pulse **Gestionar protección** > **Aplicaciones** > **MongoDB** > **Crear trabajo de restauración** para abrir el asistente Restauración de instantánea.

   Sugerencias:

   - También puede iniciar el asistente de restauración de instantáneas pulsando **Trabajos y operaciones** > **Crear trabajo de restauración** > **MongoDB**.
   - Para ver un resumen en ejecución de las selecciones en el asistente de restauración de instantáneas, mueva el cursor al icono .
   - Si desea omitir las páginas opcionales en el asistente, seleccione **Omitir pasos opcionales**.
2. En la página **Selección de origen**, complete los pasos siguientes:
   a) Pulse un origen de la lista para mostrar las bases de datos que están disponibles para las operaciones de restauración. También puede utilizar la función de búsqueda para buscar las instancias disponibles y alternar entre las instancias visualizadas mediante el filtro **Ver**.
   b) Haga clic en el icono Añadir a la lista de restauración al lado de la base de datos que desea utilizar como origen de la operación de restauración. Puede seleccionar más de una base de datos en la lista.

      Los orígenes seleccionados se añaden a la lista de restauración situada junto a la lista de bases de datos. Para eliminar un elemento del origen de la lista, pulse el icono Eliminar de la lista de restauración junto al elemento.
   c) Pulse **Siguiente** para continuar.
3. En la página **Instantánea de origen**, especifique la instancia de la base de datos que desee restaurar. Complete los siguientes campos y pulse **Siguiente** para continuar.

Opción	Descripción
Tipo de restauración	Seleccione el tipo de trabajo de restauración que se va a ejecutar. **Bajo demanda: instantánea** Realiza una operación de restauración puntual a partir de una copia de seguridad de instantánea. **Bajo demanda: punto en el tiempo** Realiza una operación de restauración puntual a partir de una copia de seguridad específica de un punto en el tiempo. **Recurrente** Ejecuta las operaciones de restauración planificadas de los datos desde los últimos puntos de restauración.
Tipo de ubicación de restauración	Seleccione el tipo de ubicación desde el que se realiza la restauración: **Sitio** Restaura los datos de un sitio que está asociado con el servidor de almacenamiento de copia de seguridad.

Opción	Descripción
	Descarga de la nube Restaura los datos que se almacenan en el almacenamiento en la nube. **Descarga del repositorio** Restaura los datos que se almacenan en el servidor de repositorio. **Archivado de nube** Restaura los datos que se archivan en el almacenamiento en la nube. **Archivado de repositorio** Restaura los datos que se archivan en el servidor de repositorio.
Seleccionar una ubicación	Si está restaurando datos desde un sitio, seleccione una de las siguientes ubicaciones de restauración: **Demo** Restaura los datos desde el servidor vSnap de demostración que se ha configurado con fines de prueba. **Primario** Restaura los datos desde el servidor vSnap que es el destino de copia de seguridad primario. **Secundario** Restaura los datos desde el servidor vSnap que es el destino de copia de seguridad secundario. Si restaura datos desde un servidor de nube o de repositorio, no es necesario realizar una selección, ya que la ubicación ya está seleccionada.
Selector de fecha	Para las operaciones de restauración bajo demanda, especifique el rango de fechas para el que desea mostrar las instantáneas que están disponibles.
Punto de restauración	Para las operaciones de restauración bajo demanda, seleccione una instantánea en la lista de instantáneas disponibles en el rango de fechas seleccionado.
Utilizar el servidor vSnap alternativo para el trabajo de restauración	Seleccione este recuadro para especificar un servidor vSnap alternativo cuando restaure un punto de restauración específico desde un recurso de nube o un servidor de repositorio y, a continuación, seleccione un servidor en el menú **Seleccionar vSnap alternativo**. Cuando restaura datos desde un punto de restauración que se ha descargado a un recurso de nube o servidor de repositorio, se utiliza un servidor vSnap como pasarela para completar la operación. De forma predeterminada, el servidor vSnap que se utiliza para completar la operación de restauración es el mismo servidor vSnap que se utiliza para completar las operaciones de copia de seguridad y de descarga. Para reducir la carga en el servidor vSnap, puede seleccionar un servidor vSnap alternativo para que sirva como pasarela para la operación de restauración.

4. En la página "Establecer destino", seleccione **Restaurar a la instancia original** y pulse **Siguiente**.
5. En la página **Método de restauración**, elija el tipo de operación de restauración y pulse **Siguiente** para continuar.
   - **Producción**

     Para recuperar una instancia completa en la instancia original, el método preferido consiste en elegir esta opción con la opción de sobrescritura de aplicación. Las instancias de MongoDB que son miembros de un conjunto de réplicas no se inician durante una operación de restauración de producción. Esta acción evita que los datos se sobrescriban al conectarse al conjunto de réplicas.
   - **Probar**

     Elija esta opción para restaurar los datos en el mismo servidor, pero utilizando un puerto distinto.

- **Acceso instantáneo**

  Elija esta opción para montar la copia de seguridad en el servidor de aplicaciones sin restaurar o sobrescribir los datos.

  Pulse **Siguiente** para continuar.

Para la modalidad de prueba o la modalidad de producción, puede especificar opcionalmente un nuevo nombre para la base de datos restaurada.

Para la modalidad de producción, también puede especificar una nueva carpeta para la base de datos restaurada expandiendo la base de datos e introduciendo un nuevo nombre de carpeta.

6. Opcional: En la página **Opciones de trabajo**, configure opciones adicionales para el trabajo de restauración y pulse **Siguiente** para continuar.

   En la sección **Opciones de recuperación**, la opción **Recuperar hasta el final de la copia de seguridad** para MongoDB está seleccionada de forma predeterminada. Esta opción recupera los datos seleccionados en el estado en el que se encontraban en el momento en que se creó la copia de seguridad. La operación de recuperación utiliza los archivos de registro que se incluyen en la copia de seguridad de MongoDB.

   Opciones de aplicación

   Establezca las opciones de la aplicación:

   Sobrescribir base de datos existente

   Habilite esta opción para permitir que el trabajo de restauración sobrescriba la base de datos seleccionada. Si esta opción no está seleccionada, el trabajo de restauración falla cuando se encuentran los datos con el mismo nombre durante el proceso de restauración.

   Atención: Asegúrese de que ningún otro dato comparte el mismo directorio de bases de datos local que los datos originales o los datos se sobrescribirán.

   Número máximo de streams paralelos por base de datos

   Establezca el número máximo de secuencias de datos en paralelo desde el almacenamiento de copia de seguridad por base de datos. Este valor se aplica a cada base de datos de la definición de trabajo. Todavía se pueden restaurar varias bases de datos en paralelo si el valor de la opción se establece en 1. Varios streams paralelos pueden agilizar las operaciones de restauración, pero el alto consumo de ancho de banda puede afectar al rendimiento general del sistema.

   Esta opción solo es aplicable cuando restaura una base de datos MongoDB a su ubicación original utilizando su nombre de base de datos original.

   Opciones avanzadas

   Establezca las opciones de definición de trabajo avanzadas:

   Ejecutar la limpieza inmediatamente en caso de anomalía del trabajo

   Esta opción se selecciona de forma predeterminada para limpiar automáticamente los recursos asignados como parte de una operación de restauración si la recuperación no se realiza correctamente.

   Permitir la sobrescritura de sesión

   Seleccione esta opción para sustituir las bases de datos existentes con el mismo nombre durante una operación de restauración. Durante una operación de restauración de disco instantánea, la base de datos existente se cierra y se sobrescriben y, a continuación, se reinicia la base de datos recuperada. Si esta opción no está seleccionada y se encuentra una base de datos con el mismo nombre, la operación de restauración falla con un error.

   Continúe con las restauraciones de otras bases de datos seleccionadas incluso si una falla

   Si una base de datos de la instancia no se restaura correctamente, la operación de restauración continúa para los demás datos que se están restaurando. Cuando esta opción no está seleccionada, el trabajo de restauración se detiene cuando falla la recuperación de un recurso.

Prefijo de punto de montaje
Para las operaciones de restauración de **Acceso instantáneo**, especifique un prefijo de punto de montaje para la vía de acceso en la que se va a dirigir el montaje.

7. Opcional: En la página **Aplicar scripts**, especifique los scripts que pueden ejecutarse antes o después de que se ejecute un trabajo. Los scripts Batch y PowerShell están soportados en los sistemas operativos Windows mientras que los scripts de shell están soportados en los sistemas operativos Linux.

   Script anterior
   Seleccione este recuadro de selección para elegir un script cargado y una aplicación o un servidor de scripts en el que se ejecutará el script anterior. Para seleccionar un servidor de aplicaciones, desmarque el recuadro de selección **Utilizar servidor de scripts**. Para configurar scripts y servidores de scripts, pulse **Configuración del sistema** > **Script**.

   Script posterior
   Seleccione esta opción para elegir un script cargado y una aplicación o un servidor de scripts en el que se ejecutará el script posterior. Para seleccionar un servidor de aplicaciones, desmarque el recuadro de selección **Utilizar servidor de scripts**. Para configurar scripts y servidores de scripts, pulse la página **Configuración del sistema** > **Script**.

   Continuar trabajo/tarea en error de script
   Seleccione esta opción para continuar ejecutando el trabajo si falla el script asociado con el trabajo. Cuando esta opción está habilitada, en el caso de que un script termine de procesarse con un código de retorno distinto de cero, el trabajo de copia de seguridad o restauración continúa ejecutándose y el estado de la tarea del script anterior se notifica como `COMPLETED`. Si un script posterior termina de procesarse con un código de retorno distinto de cero, el estado de la tarea del script posterior se notifica como `COMPLETED`. Cuando esta opción no está seleccionada, el trabajo de copia de seguridad o restauración no se ejecuta, y el estado de la tarea Script previo o Script posterior se notifica como `FAILED`.

   Pulse **Siguiente** para continuar.
8. En la página **Planificación**, pulse **Siguiente** para iniciar los trabajos bajo demanda después de completar el asistente de restauración de instantáneas. Para los trabajos recurrentes, especifique un nombre para la planificación de trabajos y especifique la frecuencia y el momento en que se debe iniciar el trabajo de restauración.
9. En la página **Revisar** , revise los valores del trabajo de restauración.

   Atención: Revise las opciones seleccionadas antes de continuar en **Enviar**, ya que los datos se sobrescribirán cuando se seleccione la opción de aplicación **Sobrescribir datos existentes**. Puede cancelar un trabajo de restauración cuando está en curso, pero si se selecciona la opción **Sobrescribir datos existentes**, los datos se sobrescriben aunque cancele el trabajo.

10. Para continuar con el trabajo, pulse **Enviar**. Para cancelar el trabajo, vaya a **Trabajos y operaciones** y haga clic en la pestaña **Planificación** . Busque el trabajo de restauración que desea cancelar. Pulse **Acciones** y seleccione **Cancelar**.

Restauración de datos de MongoDB a una instancia alternativa

Puede seleccionar una copia de seguridad de base de datos de MongoDB y restaurarla a un host alternativo. También puede elegir restaurar una base de datos en un repositorio de vSnap diferente, o bien puede cambiar el nombre de la base de datos. Este proceso crea una copia exacta de la instancia en un host distinto.

Antes de empezar

Antes de crear un trabajo de restauración para MongoDB, asegúrese de que se cumplen los requisitos siguientes:

- Se ha configurado como mínimo un trabajo de copia de seguridad de MongoDB y se está ejecutando correctamente. Para obtener instrucciones sobre la configuración de un trabajo de copia de seguridad, consulte "Copia de seguridad de datos de MongoDB" en la página 208.
- Se han asignado roles y grupos de recursos de IBM Spectrum Protect Plus al usuario que configura el trabajo de restauración. Para obtener instrucciones sobre la asignación de roles, consulte Capítulo 13, "Gestión del acceso de usuarios", en la página 303 y "Roles para MongoDB" en la página 202.
- Se ha asignado suficiente espacio de disco en el servidor de destino para la operación de restauración.
- Se han asignado volúmenes dedicados para la copia de archivos.
- Están disponibles la misma estructura de directorios y el mismo diseño en los servidores de origen y destino.
- Cuando se realiza una restauración desde un archivado de IBM Spectrum Protect, los archivos se migrarán a una agrupación de transferencia desde la cinta antes del inicio del trabajo. Dependiendo del tamaño de la restauración, este proceso puede tardar varias horas.

Para las operaciones de restauración a instancias alternativas, MongoDB debe estar en el mismo nivel de versión en las máquinas de destino y de host.

Para obtener más información sobre los requisitos de espacio, consulte Requisitos previos de espacio para la protección de MongoDB. Para obtener más información sobre los requisitos previos y la configuración, consulte Requisitos previos para MongoDB.

Procedimiento

1. En el panel de navegación, pulse **Gestionar protección** > **Aplicaciones** > **MongoDB** > **Crear trabajo de restauración** para abrir el asistente Restauración de instantánea.

   Sugerencias:

   - También puede iniciar el asistente de restauración de instantáneas pulsando **Trabajos y operaciones** > **Crear trabajo de restauración** > **MongoDB**.
   - Para ver un resumen en ejecución de las selecciones en el asistente de restauración de instantáneas, mueva el cursor al icono .
   - Si desea omitir las páginas opcionales en el asistente, seleccione **Omitir pasos opcionales**.
2. En la página **Selección de origen**, complete los pasos siguientes:
   a) Pulse un origen de la lista para mostrar las bases de datos que están disponibles para las operaciones de restauración. También puede utilizar la función de búsqueda para buscar las instancias disponibles y alternar entre las instancias visualizadas mediante el filtro **Ver**.
   b) Haga clic en el icono Añadir a la lista de restauración al lado de la base de datos que desea utilizar como origen de la operación de restauración. Puede seleccionar más de una base de datos en la lista.

      Los orígenes seleccionados se añaden a la lista de restauración situada junto a la lista de bases de datos. Para eliminar un elemento del origen de la lista, pulse el icono Eliminar de la lista de restauración junto al elemento.
   c) Pulse **Siguiente** para continuar.
3. En la página **Instantánea de origen**, especifique la instancia de la base de datos que desee restaurar. Complete los siguientes campos y pulse **Siguiente** para continuar.

Opción	Descripción
Tipo de restauración	Seleccione el tipo de trabajo de restauración que se va a ejecutar. **Bajo demanda: instantánea** Realiza una operación de restauración puntual a partir de una copia de seguridad de instantánea.

Opción	Descripción
	Bajo demanda: punto en el tiempo Realiza una operación de restauración puntual a partir de una copia de seguridad específica de un punto en el tiempo. **Recurrente** Ejecuta las operaciones de restauración planificadas de los datos desde los últimos puntos de restauración.
Tipo de ubicación de restauración	Seleccione el tipo de ubicación desde el que se realiza la restauración: **Sitio** Restaura los datos de un sitio que está asociado con el servidor de almacenamiento de copia de seguridad. **Descarga de la nube** Restaura los datos que se almacenan en el almacenamiento en la nube. **Descarga del repositorio** Restaura los datos que se almacenan en el servidor de repositorio. **Archivado de nube** Restaura los datos que se archivan en el almacenamiento en la nube. **Archivado de repositorio** Restaura los datos que se archivan en el servidor de repositorio.
Seleccionar una ubicación	Si está restaurando datos desde un sitio, seleccione una de las siguientes ubicaciones de restauración: **Demo** Restaura los datos desde el servidor vSnap de demostración que se ha configurado con fines de prueba. **Primario** Restaura los datos desde el servidor vSnap que es el destino de copia de seguridad primario. **Secundario** Restaura los datos desde el servidor vSnap que es el destino de copia de seguridad secundario. Si restaura datos desde un servidor de nube o de repositorio, no es necesario realizar una selección, ya que la ubicación ya está seleccionada.
Selector de fecha	Para las operaciones de restauración bajo demanda, especifique el rango de fechas para el que desea mostrar las instantáneas que están disponibles.
Punto de restauración	Para las operaciones de restauración bajo demanda, seleccione una instantánea en la lista de instantáneas disponibles en el rango de fechas seleccionado.
Utilizar el servidor vSnap alternativo para el trabajo de restauración	Seleccione este recuadro para especificar un servidor vSnap alternativo cuando restaure un punto de restauración específico desde un recurso de nube o un servidor de repositorio y, a continuación, seleccione un servidor en el menú **Seleccionar vSnap alternativo**. Cuando restaura datos desde un punto de restauración que se ha descargado a un recurso de nube o servidor de repositorio, se utiliza un servidor vSnap como pasarela para completar la operación. De forma predeterminada, el servidor vSnap que se utiliza para completar la operación de restauración es el mismo servidor vSnap que se utiliza para completar las operaciones de copia de seguridad y de descarga. Para reducir la carga en el servidor vSnap, puede seleccionar un servidor vSnap alternativo para que sirva como pasarela para la operación de restauración.

4. En la página **Establecer destino**, elija **Restaurar a la instancia alternativa** seleccione la instancia de destino en la que desea restaurar los datos.

   La instancia original no se puede seleccionar, porque no puede sobrescribir los datos originales cuando selecciona **Restaurar a la instancia alternativa**. Tampoco puede seleccionar instancias en niveles de versión diferentes o instancias en el mismo host que la instancia original.

   Pulse **Siguiente** para continuar.
5. En la página **Método de restauración**, elija el tipo de operación de restauración y pulse **Siguiente** para continuar.

   - **Prueba**: en esta modalidad, el agente crea una base de datos utilizando los archivos de datos directamente desde el repositorio de vSnap. Esta opción solo está disponible cuando se restauran los datos a una instancia alternativa. Los miembros de los conjuntos de réplicas no se reconfigurarán después de que se inicie el servidor de MongoDB. El servidor se inicia como un conjunto de réplicas de un único nodo.
   - **Producción**: en esta modalidad, el servidor de aplicaciones de MongoDB copia primero los archivos del repositorio de vSnap en el host de destino. A continuación, los datos copiados se utilizan para iniciar la base de datos. Las instancias de MongoDB que son miembros de un conjunto de réplicas no se inician durante una operación de restauración de producción. Esta acción evita que los datos se sobrescriban al conectarse al conjunto de réplicas.
   - **Acceso instantáneo**: en esta modalidad, no se emprende ninguna acción adicional después de que IBM Spectrum Protect Plus monte el recurso compartido. Utilice los datos para la recuperación personalizada de los archivos en el repositorio de vSnap.

   Para la modalidad de prueba o la modalidad de producción, puede especificar opcionalmente un nuevo nombre para la base de datos restaurada.

   Para la modalidad de producción, también puede especificar una nueva carpeta para la base de datos restaurada expandiendo la base de datos e introduciendo un nuevo nombre de carpeta.
6. Opcional: En la página **Opciones de trabajo**, configure opciones adicionales para el trabajo de restauración y pulse **Siguiente** para continuar.

   En la sección **Opciones de recuperación**, la opción **Recuperar hasta el final de la copia de seguridad** para MongoDB está seleccionada de forma predeterminada. Esta opción recupera los datos seleccionados en el estado en el que se encontraban en el momento en que se creó la copia de seguridad. La operación de recuperación utiliza los archivos de registro que se incluyen en la copia de seguridad de MongoDB.

   Opciones de aplicación

   Establezca las opciones de la aplicación:

   Sobrescribir base de datos existente

   Habilite esta opción para permitir que el trabajo de restauración sobrescriba la base de datos seleccionada. Si esta opción no está seleccionada, el trabajo de restauración falla cuando se encuentran los datos con el mismo nombre durante el proceso de restauración.

   Atención: Asegúrese de que ningún otro dato comparte el mismo directorio de bases de datos local que los datos originales o los datos se sobrescribirán.

   Número máximo de streams paralelos por base de datos

   Establezca el número máximo de secuencias de datos en paralelo desde el almacenamiento de copia de seguridad por base de datos. Este valor se aplica a cada base de datos de la definición de trabajo. Todavía se pueden restaurar varias bases de datos en paralelo si el valor de la opción se establece en 1. Varios streams paralelos pueden agilizar las operaciones de restauración, pero el alto consumo de ancho de banda puede afectar al rendimiento general del sistema.

   Esta opción solo es aplicable cuando restaura una base de datos MongoDB a su ubicación original utilizando su nombre de base de datos original.

   Opciones avanzadas

   Establezca las opciones de definición de trabajo avanzadas:

Ejecutar la limpieza inmediatamente en caso de anomalía del trabajo
Esta opción se selecciona de forma predeterminada para limpiar automáticamente los recursos asignados como parte de una operación de restauración si la recuperación no se realiza correctamente.

Permitir la sobrescritura de sesión
Seleccione esta opción para sustituir las bases de datos existentes con el mismo nombre durante una operación de restauración. Durante una operación de restauración de disco instantánea, la base de datos existente se cierra y se sobrescriben y, a continuación, se reinicia la base de datos recuperada. Si esta opción no está seleccionada y se encuentra una base de datos con el mismo nombre, la operación de restauración falla con un error.

Continúe con las restauraciones de otras bases de datos seleccionadas incluso si una falla
Si una base de datos de la instancia no se restaura correctamente, la operación de restauración continúa para los demás datos que se están restaurando. Cuando esta opción no está seleccionada, el trabajo de restauración se detiene cuando falla la recuperación de un recurso.

Prefijo de punto de montaje
Para las operaciones de restauración de **Acceso instantáneo**, especifique un prefijo de punto de montaje para la vía de acceso en la que se va a dirigir el montaje.

7. Opcional: En la página **Aplicar scripts**, especifique los scripts que pueden ejecutarse antes o después de que se ejecute un trabajo. Los scripts Batch y PowerShell están soportados en los sistemas operativos Windows mientras que los scripts de shell están soportados en los sistemas operativos Linux.

   Script anterior
   Seleccione este recuadro de selección para elegir un script cargado y una aplicación o un servidor de scripts en el que se ejecutará el script anterior. Para seleccionar un servidor de aplicaciones, desmarque el recuadro de selección **Utilizar servidor de scripts**. Para configurar scripts y servidores de scripts, pulse **Configuración del sistema** > **Script**.

   Script posterior
   Seleccione esta opción para elegir un script cargado y una aplicación o un servidor de scripts en el que se ejecutará el script posterior. Para seleccionar un servidor de aplicaciones, desmarque el recuadro de selección **Utilizar servidor de scripts**. Para configurar scripts y servidores de scripts, pulse la página **Configuración del sistema** > **Script**.

   Continuar trabajo/tarea en error de script
   Seleccione esta opción para continuar ejecutando el trabajo si falla el script asociado con el trabajo. Cuando esta opción está habilitada, en el caso de que un script termine de procesarse con un código de retorno distinto de cero, el trabajo de copia de seguridad o restauración continúa ejecutándose y el estado de la tarea del script anterior se notifica como `COMPLETED`. Si un script posterior termina de procesarse con un código de retorno distinto de cero, el estado de la tarea del script posterior se notifica como `COMPLETED`. Cuando esta opción no está seleccionada, el trabajo de copia de seguridad o restauración no se ejecuta, y el estado de la tarea Script previo o Script posterior se notifica como `FAILED`.

   Pulse **Siguiente** para continuar.
8. En la página **Planificación**, pulse **Siguiente** para iniciar los trabajos bajo demanda después de completar el asistente de restauración de instantáneas. Para los trabajos recurrentes, especifique un nombre para la planificación de trabajos y especifique la frecuencia y el momento en que se debe iniciar el trabajo de restauración.
9. En la página **Revisar** , revise los valores del trabajo de restauración.

   Atención: Revise las opciones seleccionadas antes de continuar en **Enviar**, ya que los datos se sobrescribirán cuando se seleccione la opción de aplicación **Sobrescribir datos existentes**. Puede cancelar un trabajo de restauración cuando está en curso, pero si se selecciona la opción **Sobrescribir datos existentes**, los datos se sobrescriben aunque cancele el trabajo.

10. Para continuar con el trabajo, pulse **Enviar**. Para cancelar el trabajo, vaya a **Trabajos y operaciones** y haga clic en la pestaña **Planificación** . Busque el trabajo de restauración que desea cancelar. Pulse **Acciones** y seleccione **Cancelar**.

Uso de la operación de restauración granular para MongoDB

Puede restaurar colecciones o bases de datos de MongoDB específicas utilizando una operación de restauración granular. Para una operación de restauración granular, primero ejecute un trabajo de restauración de prueba y, a continuación, ejecute los mandatos de MongoDB adecuados.

Antes de empezar

Si la autenticación está habilitada, debe proporcionar credenciales para los usuarios de modo que puedan corregir los permisos de la instancia en la operación de restauración de prueba.

Acerca de esta tarea

La operación de restauración granular para MongoDB se basa en un trabajo de restauración de modalidad de prueba. Cuando ejecuta el trabajo de restauración de prueba en IBM Spectrum Protect Plus, y los mandatos **mongodump** y **mongorestore** en el servidor de MongoDB, puede acceder a bases de datos o colecciones individuales desde el origen de recuperación.

Utilice este procedimiento para completar una de las tareas siguientes:

- Restaure cualquier número de bases de datos utilizando los mandatos **mongodump** y **mongorestore** para las bases de datos que necesite.
- Restaure cualquier número de colecciones utilizando los mandatos **mongodump** y **mongorestore** para las colecciones que necesite.

Procedimiento

1. En el panel de navegación, pulse **Gestionar protección** > **Aplicaciones** > **MongoDB**.
2. Pulse **Crear trabajo de restauración** para abrir el asistente de restauración. MongoDB se selecciona automáticamente.
3. En la página **Selección de origen**, complete los pasos siguientes:
   a) Pulse un origen de la lista para mostrar las bases de datos que están disponibles para las operaciones de restauración. También puede utilizar la función de búsqueda para buscar las instancias disponibles y alternar entre las instancias visualizadas mediante el filtro **Ver**.
   b) Haga clic en el icono Añadir a la lista de restauración al lado de la base de datos que desea utilizar como origen de la operación de restauración. Puede seleccionar más de una base de datos en la lista.

      Los orígenes seleccionados se añaden a la lista de restauración situada junto a la lista de bases de datos. Para eliminar un elemento del origen de la lista, pulse el icono Eliminar de la lista de restauración junto al elemento.
   c) Pulse **Siguiente** para continuar.
4. En la página **Establecer destino**, seleccione **Restaurar a instancia alternativa**y seleccione la instancia de destino en la que desea restaurar los datos.

   No puede seleccionar la instancia original que no se puede seleccionar porque no puede sobrescribir los datos originales cuando selecciona **Restaurar a instancia alternativa**. No se pueden seleccionar instancias en distintos niveles de versiones. Tampoco se pueden seleccionar otras instancias en el mismo host que la instancia original.

   Pulse **Siguiente** para continuar.
5. En la página **Método de restauración**, seleccione **Probar**y pulse **Siguiente** para continuar con el proceso de restauración de prueba.
6. Continúe a través de las páginas del asistente de restauración y seleccione las opciones necesarias.
7. En la página **Revisar** , revise los valores del trabajo de restauración.

Atención: Revise las opciones seleccionadas antes de continuar en **Enviar**, ya que los datos se sobrescribirán cuando se seleccione la opción de aplicación **Sobrescribir datos existentes**. Puede cancelar un trabajo de restauración cuando está en curso, pero si se selecciona la opción **Sobrescribir datos existentes**, los datos se sobrescriben aunque cancele el trabajo.

8. Inicie la sesión en el servidor de MongoDB al que se dirige el trabajo de restauración de prueba.
9. Ejecute el mandato del sistema MongoDB `ps -ef | grep mongod` para encontrar la ubicación de instancia de MongoDB de recuperación temporal.
10. Ejecute el mandato `mongodump` de MongoDB para crear un archivo de volcado de cualquier base de datos o colección específica.

    Utilice el mandato adecuado. El primer mandato es para una base de datos y el segundo mandato es para una colección:

    ```
    mongodump
    --host <nombre_host> --port <puerto> --db <nombrebd> <carpeta_volcado>
    ```

    O,

    ```
    mongodump --host <nombre_host> --port <puerto> --collection <nombre_colección>
    <carpeta_volcado>
    ```

11. Ejecute el mandato **`mongorestore`** para restaurar el archivo de volcado en cualquier instancia de MongoDB. Elija la instancia de MongoDB original para la que se ha creado la copia de seguridad, o cualquier instancia alternativa.

    Utilice el mandato adecuado. El primer mandato es para una base de datos y el segundo mandato es para una colección:

    ```
    mongorestore --host <nombre_host> --port <puerto> --db <nombrebd> <carpeta_volcado>
    \<nombrebd>
    ```

    O bien

    ```
    mongorestore --host <nombre_host> --port <puerto> --collection <nombre_colección>
    <carpeta_volcado>\<nombrebd>
    ```

12. Cuando finalice la operación de restauración de la base de datos o de la colección, vaya a **Trabajos y operaciones** > **Recursos activos**.
13. Pulse **Acciones** > **Cancelar restauración** para finalizar el procedimiento de restauración granular.

Copia de seguridad y restauración de datos de SQL Server

Para proteger el contenido en un servidor de SQL Server, registre primero la instancia de SQL Server para que IBM Spectrum Protect Plus lo reconozca. A continuación, cree trabajos para las operaciones de copia de seguridad y restauración

Requisitos del sistema

Asegúrese de que el entorno de SQL Server cumple los requisitos del sistema en "Requisitos de Microsoft SQL Server" en la página 43.

Registro y autenticación

Registre cada servidor de SQL Server en IBM Spectrum Protect Plus por nombre o dirección IP. Al registrar un nodo de SQL Server Cluster (AlwaysOn), registre cada nodo por nombre o dirección IP. Tenga en cuenta que las direcciones IP deben ser de orientación pública y estar a la escucha en el puerto 5985. El nombre de dominio completo y el nombre DNS de nodo de la máquina virtual deben poder resolverse y direccionarse desde el dispositivo de IBM Spectrum Protect Plus.

La identidad de usuario debe tener derechos suficientes para instalar e iniciar el servicio de herramientas de IBM Spectrum Protect Plus en el nodo, incluido el derecho a **Iniciar sesión como servicio**. Para obtener más información acerca de este derecho, consulte Añadir el inicio de sesión como servicio de derecho a una cuenta.

La política de seguridad predeterminada utiliza el protocolo NTLM de Windows y el formato de identidad de usuario sigue el formato *dominio**nombre*.

Cuando se utilizan objetos de política de grupo de Windows (GPO), el valor de objeto de política de grupo, el nivel de autenticación **Network security: LAN Manager** debe establecerse correctamente. Establézcalo con una de las opciones siguientes:

- No definido
- Enviar solo respuesta NTLMv2
- Enviar solo respuesta NTLMv2. Rechazar LM
- Enviar solo respuesta NTLMv2. Rechazar LM & NTLM

Requisitos de Kerberos

La autenticación basada en Kerberos se puede habilitar a través de un archivo de configuración en el dispositivo de IBM Spectrum Protect Plus. Esto alterará temporalmente el protocolo NTLM de Windows predeterminado.

Sólo para la autenticación basada en Kerberos, la identidad de usuario se debe especificar en el formato username@FQDN. El nombre de usuario debe poder autenticarse utilizando la contraseña registrada para obtener un tíquet de otorgamiento de tíquet (TGT) desde el centro de distribución de claves (KDC) en el dominio especificado por el nombre de dominio completo.

La autenticación de Kerberos también requiere que el desfase horario entre el controlador de dominio y el dispositivo de IBM Spectrum Protect Plus sea inferior a cinco minutos.

El protocolo NTLM de Windows predeterminado no depende del tiempo.

Privilegios

En el servidor de SQL Server, la credencial de inicio de sesión del sistema debe tener permisos públicos y sysadmin habilitados, además de permiso para acceder a los recursos de clúster en un entorno de SQL Server AlwaysOn. Si se utiliza una cuenta de usuario para todas las funciones de SQL Server, se debe habilitar un inicio de sesión de Windows para el servidor de SQL Server, con los permisos públicos y sysadmin habilitados.

Cada instancia de SQL Server puede utilizar una cuenta de usuario específica para acceder a los recursos de dicha instancia en particular.

Para completar operaciones de copia de seguridad de registro, el usuario de SQL Server registrado con IBM Spectrum Protect Plus debe tener el permiso sysadmin habilitado para gestionar trabajos de agente de SQL Server.

El Planificador de tareas de Windows se utiliza para planificar copias de seguridad de registro. Dependiendo del entorno, los usuarios pueden recibir el siguiente error: `Una sesión de inicio de sesión especificada no existe. Puede que ya se haya terminado.` Esto se debe a un valor de política de grupo de acceso de red que tiene que inhabilitarse. Para obtener más información sobre cómo inhabilitar este GPO, consulte el siguiente artículo de soporte de Microsoft: https://support.microsoft.com/en-us/help/968264/error-message-when-you-try-to-map-to-a-network-drive-of-a-dfs-share-by

Adición de un servidor de aplicaciones de SQL Server

Cuando se añade un servidor de aplicaciones de SQL Server, se captura un inventario de las instancias de bases de datos que están asociadas al servidor de aplicaciones y se añade a IBM Spectrum Protect Plus. Este proceso permite completar trabajos de copia de seguridad y restauración, así como informes de ejecución.

Procedimiento

Para suprimir un host de SQL Server, realice estos pasos.

1. En el panel de navegación, pulse **Gestionar protección** > **Aplicaciones** > **SQL** > **Copia de seguridad**.
2. Pulse **Gestionar servidores de aplicaciones**.
3. Pulse **Añadir servidor de aplicaciones**.
4. Rellene los campos en el panel **Propiedades de aplicación**:

   Dirección de host

   Especifique la dirección IP que se pueda resolver o una vía de acceso y un nombre de máquina que se puedan resolver.

   Utilizar usuario existente

   Habilite esta opción para seleccionar un nombre de usuario y una contraseña especificados anteriormente para el proveedor.

   ID de usuario

   Escriba el nombre de usuario y la contraseña para el proveedor. La identidad de usuario respeta el formato *dominio**nombre* si la máquina virtual está conectada a un dominio. El formato *administrador_local* se utiliza si el usuario es un administrador local.

   Solo para la autenticación basada en Kerberos, la identidad de usuario se debe especificar en el formato de nombre de usuario @FQDN. El nombre de usuario debe poderse autenticar utilizando la contraseña registrada para obtener un tíquet de otorgamiento de tíquet (TGT) del centro de distribución de claves (KDC) en el dominio que se especifica mediante el nombre de dominio completo.

   Contraseña

   Escriba la contraseña para el proveedor.

   Número máximo de bases de datos simultáneas

   Establezca el número máximo de bases de datos en las que se debe realizar una copia de seguridad simultáneamente en el servidor. El rendimiento del servidor se ve afectado cuando se realiza una copia de seguridad de un gran número de bases de datos simultáneamente, ya que cada base de datos utiliza múltiples hebras y consume ancho de banda al copiar datos. Utilice esta opción para controlar el impacto en los recursos del servidor y minimizar el impacto en las operaciones de producción.
5. Pulse **Guardar**. IBM Spectrum Protect Plus confirma una conexión de red, añade el servidor de aplicaciones a la base de datos de IBM Spectrum Protect Plus y a continuación, cataloga la instancia.

   Si aparece un mensaje que indica que la conexión no se ha realizado correctamente, revise las entradas. Si las entradas son correctas y la conexión no se ha realizado correctamente, póngase en contacto con un administrador del sistema para revisar las conexiones.

Qué hacer a continuación

Después de añadir el servidor de aplicaciones de SQL Server, realice la acción siguiente:

Acción	Cómo
Asigne permisos de usuario al servidor de aplicaciones.	Consulte “Creación de un rol” en la página 308.

Conceptos relacionados

“Gestión del acceso de usuarios” en la página 303

Al utilizar el control de acceso basado en roles, puede establecer los recursos y permisos disponibles en las cuentas de usuario de IBM Spectrum Protect Plus.

Tareas relacionadas

“Copia de seguridad de datos de SQL Server” en la página 229

Utilice un trabajo de copia de seguridad para realizar copias de seguridad de entornos SQL Server con instantáneas.

"Restauración de datos de SQL Server" en la página 233
Utilice un trabajo de restauración para restaurar un entorno de a Microsoft SQL Server desde las instantáneas. Después de ejecutar los trabajos de Restauración de disco instantánea de IBM Spectrum Protect Plus, los clones de SQL Server se pueden utilizar inmediatamente. IBM Spectrum Protect Plus cataloga y realiza el seguimiento de todas las instancias clonadas.

Detección de recursos de SQL Server
Los recursos de SQL Server se detectan automáticamente después de que se añada el servidor de aplicaciones a IBM Spectrum Protect Plus. Sin embargo, puede ejecutar un trabajo de inventario para detectar cualquier cambio que se haya producido desde que se añadió el servidor de aplicaciones.

Procedimiento

Para ejecutar un trabajo de inventario, realice los pasos siguientes:

1. En el panel de navegación, pulse **Gestionar protección** > **Aplicaciones** > **SQL** > **Copia de seguridad**.
2. En la lista de instancias de SQL Server, seleccione una instancia o pulse el enlace de la instancia para ir hasta el recurso que desea. Por ejemplo, si desea ejecutar un trabajo de inventario para una base de datos individual de la instancia, pulse el enlace de instancia y, a continuación, seleccione una máquina virtual.
3. Pulse **Ejecutar inventario**.

Prueba de conexión a un servidor de aplicaciones de SQL Server
Puede probar la conexión a un host de SQL Server. La función de prueba verifica la comunicación con el host y prueba los valores de DNS entre el dispositivo virtual de IBM Spectrum Protect y el host.

Procedimiento

Para probar la conexión, complete los pasos siguientes:

1. En el panel de navegación, pulse **Gestionar protección** > **Aplicaciones** > **SQL** > **Copia de seguridad**.
2. Pulse **Gestionar servidores de aplicaciones**.
3. En la lista de hosts, pulse **Probar** en el menú **Acciones** del host.

Copia de seguridad de datos de SQL Server

Utilice un trabajo de copia de seguridad para realizar copias de seguridad de entornos SQL Server con instantáneas.

Antes de empezar

Durante la copia de seguridad base inicial, IBM Spectrum Protect Plus crea un nuevo volumen de vSnap y crea una unidad compartida de NFS. Durante las copias de seguridad incrementales, se reutiliza el volumen creado previamente. El agente de IBM Spectrum Protect Plus monta el recurso compartido en el servidor de SQL Server en el que se va a completar la copia de seguridad.

Cuando la copia de seguridad se ha completado, el agente de IBM Spectrum Protect Plus desmonta el recurso compartido del servidor de SQL Server y crea una instantánea vSnap del volumen de copia de seguridad.

Revise la siguiente información:

- Para que un usuario pueda implementar operaciones de copia de seguridad y restauración de IBM Spectrum Protect Plus, deben asignarse roles y grupos de recursos al usuario. Otorgue a los usuarios acceso a los recursos y a las operaciones de copia de seguridad y restauración mediante el panel **Cuentas**. Para obtener más información, consulte Capítulo 13, "Gestión del acceso de usuarios", en la página 303.

- El iniciador iSCSI de Microsoft debe estar habilitado y en ejecución en el servidor de Windows. Debe habilitarse una ruta iSCSI entre el sistema SQL y el servidor vSnap. Para obtener más información, consulte Guía de paso a paso de Microsoft iSCSI Initiator.
- Evite configurar la copia de seguridad de registro para una única base de datos SQL a través de varios trabajos de copia de seguridad. Los registros se truncan durante las operaciones de copia de seguridad de registro. Si se añade una única base de datos de SQL a varias definiciones de trabajo con la copia de seguridad de registro habilitada, una copia de seguridad de registro de un trabajo truncará un registro antes de que se realice una copia de seguridad con el trabajo siguiente. Esto puede provocar que fallen los trabajos de restauración de un momento específico.
- IBM Spectrum Protect Plus no admite la copia de seguridad de registro de los modelos de recuperación simples.
- Antes de copiar registros en vSnap, SPP utiliza la carpeta de copia de seguridad configurada para la instancia de servidor SQL como el área de transferencia para recopilar registros. El volumen en el que se encuentra esta carpeta debe tener espacio suficiente disponible para contener todos los registros de transacciones entre trabajos de copia de seguridad. El área de transferencia se puede modificar cambiando la configuración de la carpeta de copia de seguridad utilizando SQL Server Management Studio (SSMS).
- La migración tras error de una instancia de clúster SQL durante la copia de seguridad no está soportada.
- Si tiene previsto realizar una copia de seguridad de un gran número de bases de datos, es posible que tenga que aumentar el número máximo de hebras Worker en cada instancia de SQL Server asociada para asegurarse de que los trabajos de copia de seguridad se completan correctamente. El valor predeterminado del número máximo de hebras Worker es 0. El servidor determina automáticamente el valor máximo de las hebras Worker basándose en el número de procesadores disponibles en el servidor. SQL Server utiliza las hebras de esta agrupación para las conexiones de red, los puntos de control de base de datos y las consultas. Además, una copia de seguridad de cada base de datos requiere una hebra adicional de esta agrupación. Si dispone de un gran número de bases de datos en un trabajo de copia de seguridad, es posible que el número máximo de hebras Worker predeterminado no sea suficiente para realizar una copia de seguridad de todas las bases de datos y el trabajo no se realizará correctamente. Para obtener más información sobre el aumento de número máximo de hebras Worker, consulte Configurar la opción de configuración de servidor de hebras Worker máximo.
- Cuando una copia de seguridad de registro de una base de datos de SQL secundaria de tipo Siempre activado genera el siguiente error, la preferencia de la copia de seguridad del grupo de disponibilidad debe cambiarse a Primario:

  ```
  La copia de seguridad de registro de la base de datos 'DatabaseName' en una réplica
  secundaria no se ha realizado correctamente porque no se ha podido establecer un punto de
  sincronización en la base de datos primaria.
  ```

  Si cambia la preferencia a Primario, se realizará una copia de seguridad del registro de la réplica primaria. Una vez completada una copia de seguridad de registro satisfactoria de la réplica primaria, la preferencia de copia de seguridad se puede cambiar.

Realice las acciones siguientes:

- Registre los proveedores cuya copia de seguridad desea realizar. Para obtener más información, consulte “Adición de un servidor de aplicaciones de SQL Server” en la página 227.
- Configure las políticas de SLA. Para obtener más información, consulte “Crear políticas de copia de seguridad” en la página 77.
- Antes de configurar y ejecutar trabajos de copia de seguridad de SQL, debe configurar los valores de almacenamiento de duplicación de los volúmenes en los que se encuentran las bases de datos de SQL. Este valor se configura una vez para cada volumen. Si se añaden nuevas bases de datos al trabajo, el valor debe configurarse para cualquier volumen nuevo que contenga bases de datos SQL. En Windows Explorer, pulse con el botón derecho del ratón en el volumen de origen y seleccione la pestaña **Instantáneas**. Establezca el **Tamaño máximo** en **Sin límite** o un tamaño razonable en función del tamaño de volumen de origen y las actividades de E/S y, a continuación, pulse **Aceptar**. El área de almacenamiento de la instantánea o la duplicación debe estar en el mismo volumen o en otro volumen disponible durante el tiempo de copia de seguridad.

Procedimiento

Para definir un trabajo de copia de seguridad de SQL, complete los pasos siguientes:

1. En el panel de navegación, pulse **Gestionar protección** > **Aplicaciones** > **SQL**.
2. Seleccione una instancia de SQL Server para realizar la copia de seguridad.

   Utilice la función de búsqueda para buscar las instancias disponibles y alternar entre las instancias visualizadas mediante el filtro **Ver**. Las opciones disponibles son **Clúster autónomo/migración tras error** y **Siempre activado**.
3. Pulse **Seleccionar una política de SLA** para añadir una o más políticas de SLA que cumplan los criterios de datos de copia de seguridad en la definición de trabajo.
4. Para crear la definición de trabajo utilizando las opciones predeterminadas, pulse **Guardar**.

   El trabajo se ejecuta según lo definido en las políticas de SLA que ha seleccionado. Para ejecutar el trabajo manualmente, pulse **Trabajos y operaciones** > **Planificación**. Seleccione el trabajo y pulse **Acciones** > **Iniciar**.

   Sugerencia: el botón **Ejecutar** solo se habilita para una copia de seguridad de base de datos individual, y la base de datos debe tener una política de SLA aplicada.
5. Para editar opciones antes de crear la definición de trabajo, pulse **Seleccionar opciones**. Establezca las opciones de definición de trabajo.

   Habilitar copia de seguridad de registro

   Seleccione esta opción para habilitar IBM Spectrum Protect Plus para realizar copias de seguridad de los registros de transacciones y, a continuación, proteja los discos subyacentes.

   IBM Spectrum Protect Plus trunca automáticamente las copias de seguridad de registros posterior de las bases de datos que las que realiza la copia de seguridad. Si no se realiza una copia de seguridad de los registros de base de datos con IBM Spectrum Protect Plus, IBM Spectrum Protect Plus no trunca los registros y deben gestionarse por separado.

   Cuando un trabajo de copia de seguridad de SQL se completa con las copias de seguridad de registros habilitadas, todos los registros de transacciones hasta el punto en que se completa el trabajo se depuran del servidor de SQL Server. La depuración del registro solo se produce si el trabajo de copia de seguridad de SQL se completa correctamente. Si las copias de seguridad de registros se inhabilitan durante una reejecución del trabajo, la depuración del registro no se realiza.

   Si se sobrescribe una base de datos de origen, todos los antiguos registros de transacciones hasta ese punto se colocan en un directorio de "condensación" una vez que se complete la restauración de la base de datos original. Cuando se complete la siguiente ejecución del trabajo de copia de seguridad de SQL, se eliminará el contenido de la carpeta de condensación.

   Para completar las copias de seguridad de registros, el usuario de servicio del agente de SQL Server debe ser un administrador de Windows local y debe tener habilitado el permiso sysadmin para gestionar los trabajos de agente de SQL Server. El agente utilizará dicha cuenta de administrador para habilitar y acceder a los trabajos de copia de seguridad de registro. El usuario del servicio de agente de IBM Spectrum Protect Plus SQL Server también debe ser el mismo que el servicio de SQL Server y la cuenta de servicio del agente de SQL Server para cada instancia de SQL Server que se debe proteger.

   Los archivos de registro de SQL se almacenan temporalmente en un área de transferencia local antes de copiarse en un recurso compartido CIFS. El destino de la copia de seguridad predeterminada del servidor SQL sirve de área de transferencia y debe disponer de espacio libre suficiente para almacenar temporalmente los archivos de registro de transacciones con el fin de que se puedan copiar en el recurso compartido CIFS.

   Para habilitar la creación de planificación de copia de seguridad de registro para varias bases de datos en la misma instancia de SQL Server, asegúrese de que todas las bases de datos se añaden a la misma política de SLA.

   Cuando se selecciona esta opción, las opciones de restauración de un momento específico están disponibles en las operaciones de restauración de SQL.

   Número máximo de streams paralelos por base de datos

Establezca el número máximo de stream de datos de cada base de datos en el almacenamiento de copias de seguridad. Este valor se aplica a cada base de datos de la definición de trabajo. Se pueden hacer copias de seguridad de varias bases de datos en paralelo si el valor de la opción se establece en **1**. Múltiples streams paralelos pueden mejorar la velocidad de copia de seguridad, pero el alto consumo de ancho de banda puede afectar al rendimiento general del sistema.

6. Cuando esté seguro de que la información específica del trabajo es correcta, pulse **Guardar**.

   El trabajo se ejecuta de acuerdo con lo definido en la política de SLA o bien se puede ejecutar manualmente desde el Supervisor de trabajos.

7. Para configurar opciones adicionales, pulse el campo **Opciones de política** que está asociado al trabajo en la sección **Estado de política de SLA**. Establezca las opciones de política adicionales:

   Scripts anteriores y scripts posteriores

   Ejecute un script anterior o script posterior. Los scripts anteriores y los scripts posteriores se pueden ejecutar antes o después de que se ejecute un trabajo. Los scripts Batch y PowerShell están soportados.

   En la sección **Script anterior** o **Script posterior**, seleccione un script cargado y un servidor de aplicaciones o de script donde se ejecutará el script. Para seleccionar un servidor de aplicaciones en el que se va a ejecutar el script, desmarque el recuadro de selección **Utilizar servidor de scripts**. Los scripts y los servidores de scripts se configuran en la página **Configuración del sistema** > **Script**.

   Para seguir ejecutando el trabajo si falla el script asociado con el trabajo, seleccione **Continuar trabajo/tarea en error de script**.

   Cuando esta opción está habilitada, si un script anterior o un script posterior completa el proceso con un código de retorno distinto de cero, se intenta la operación de copia de seguridad o restauración y se informa sobre el estado de la tarea previa del script anterior como COMPLETADO. Si un script posterior se completa con un código de retorno distinto de cero, se informa sobre el estado de la tarea del script posterior como COMPLETADO.

   Cuando esta opción está inhabilitada, no se intenta realizar la copia de seguridad o la restauración y se informa sobre el estado de la tarea del script anterior o del script posterior como FALLIDO.

   Excluir recursos

   Excluya recursos específicos del trabajo de copia de seguridad mediante patrones de exclusión únicos o múltiples. Los recursos se pueden excluir mediante una coincidencia exacta o con asteriscos comodín especificados antes del patrón (* test) o después del patrón (test *).

   También se admiten varios comodines de asterisco en un único patrón. Los patrones admiten caracteres alfanuméricos estándar, así como los siguientes caracteres especiales:-_ y *.

   Separe varios con un punto y coma.

   Forzar copia de seguridad completa de los recursos

   Fuerce operaciones de copia de seguridad base para máquinas virtuales o bases de datos específicas en la definición de trabajo de copia de seguridad Separe varios recursos con un punto y coma.

8. Para guardar las opciones adicionales que haya configurado, pulse **Guardar**.

Qué hacer a continuación

Después de crear la definición de trabajo de copia de seguridad, realice la acción siguiente:

Acción	Cómo
Cree una definición de trabajo de Restauración de SQL.	Consulte “Restauración de datos de SQL Server” en la página 233.

Conceptos relacionados

“Configuración de scripts para las operaciones de copia de seguridad y restauración” en la página 261
Los scripts anteriores y posteriores son scripts que se pueden ejecutar antes o después de que los trabajos de copia de seguridad y restauración se ejecuten en el nivel de trabajo. Los scripts soportados

incluyen scripts de shell para máquinas basadas en Linux y scripts Batch y PowerShell para máquinas basadas en Windows. Los scripts se crean localmente, se suben al entorno a través de la página **Script** y se aplican a continuación a las definiciones de trabajos.

Tareas relacionadas

"Inicio de trabajos" en la página 258
Puede ejecutar cualquier trabajo bajo demanda, incluso si el trabajo se ha establecido para que se ejecute en una planificación.

Restauración de datos de SQL Server

Utilice un trabajo de restauración para restaurar un entorno de a Microsoft SQL Server desde las instantáneas. Después de ejecutar los trabajos de Restauración de disco instantánea de IBM Spectrum Protect Plus, los clones de SQL Server se pueden utilizar inmediatamente. IBM Spectrum Protect Plus cataloga y realiza el seguimiento de todas las instancias clonadas.

Antes de empezar

Complete los siguientes requisitos previos:

- Cree y ejecute un trabajo de copia de seguridad de SQL. Para obtener instrucciones, consulte "Copia de seguridad de datos de SQL Server" en la página 229.
- Antes de que un usuario de IBM Spectrum Protect Plus pueda restaurar datos, deben asignarse los roles y los grupos de recursos adecuados al usuario. Otorgue a los usuarios acceso a los recursos y a las operaciones de copia de seguridad y restauración utilizando el panel **Cuentas** . Para obtener instrucciones, consulte Capítulo 13, "Gestión del acceso de usuarios", en la página 303.
- Si tiene previsto ejecutar una recuperación de un punto en el tiempo, asegúrese de que tanto el servicio de instancia SQL de destino de restauración como el servicio de IBM Spectrum Protect Plus SQL Server utilizan la misma cuenta de usuario.

Revise las siguientes restricciones y consideraciones:

- Si tiene previsto ejecutar una operación de restauración de producción en un clúster de migración tras error de SQL Server, el volumen raíz de la vía de acceso de archivo alternativa debe ser apto para la base de datos de host y los archivos de registro. El volumen debe pertenecer al grupo de recursos de servidor de clúster de SQL Server de destino, y ser una dependencia del servidor de clúster de SQL Server.
- No puede restaurar datos en un volumen comprimido de NTFS o FAT debido a las restricciones de base de datos de SQL Server. Para obtener más información, consulte Descripción del soporte para bases de datos de SQL Server en volúmenes comprimidos.
- Si tiene previsto restaurar los datos en una ubicación alternativa, el destino de SQL Server debe estar ejecutando la misma versión de SQL Server o una versión posterior. Para obtener más información, consulte Soporte de compatibilidad.
- Si restaurar datos en una instancia primaria en un entorno de grupo de disponibilidad Siempre activado de SQL, la base de datos se añade al grupo de bases de datos siempre activado de destino. Después de la operación de restauración primaria, la base de datos secundaria se inicializa mediante el SQL Server en entornos en los que la inicialización automática está soportada (Microsoft SQL Server 2016 y posterior). A continuación, la base de datos se habilita en el grupo de disponibilidad de destino. El tiempo de sincronización depende de la cantidad de datos que se transfieren y de la conexión entre las réplicas primaria y secundaria.

  Si la inicialización automática no está soportada o habilitada, se debe completar una restauración secundaria desde el punto de restauración con el espacio LSN más corto de la instancia primaria. Las copias de seguridad de registros del último momento específico que crea IBM Spectrum Protect Plus deben restaurarse si la copia de seguridad de registro estaba habilitada en la instancia primaria. La operación de restauración de base de datos secundaria se ha completado en el estado RESTORING y debe emitir el mandato **T-SQL** para añadir la base de datos al grupo de destino. Para obtener más información, consulte Referencia Transact-SQL (motor de base de datos).

- Cuando se realiza una restauración desde un archivado de IBM Spectrum Protect, los archivos se migrarán a una agrupación de transferencia desde la cinta antes del inicio del trabajo. Dependiendo del tamaño de la restauración, este proceso puede tardar varias horas.

Acerca de esta tarea

La restauración de disco instantáneo utiliza el protocolo iSCSI para montar inmediatamente los LUN sin transferir datos. Las bases de datos para las que se realizan instantáneas se catalogan y son recuperables al momento sin ninguna transferencia física de datos.

Se admiten las siguientes modalidades de restauración:

Modalidad de acceso instantáneo
En modalidad de acceso instantáneo, no se realiza ninguna acción adicional después del montaje de la unidad compartida. Los usuarios pueden completar cualquier recuperación personalizada utilizando los archivos del volumen vSnap. Una restauración de Acceso instantáneo de una base de datos de tipo Siempre activado se restaura a la instancia de destino local.

Modalidad de prueba
En la modalidad de prueba, el agente crea una nueva base de datos utilizando los archivos de datos directamente desde el volumen vSnap.

Modalidad de producción
En la modalidad de producción, el agente restaura primero los archivos del volumen de vSnap al almacenamiento primario y luego crea la nueva base de datos utilizando los archivos restaurados.

Procedimiento

Para definir un trabajo de restauración de SQL, realice los pasos siguientes:

1. En el panel de navegación, pulse **Gestionar protección** > **Aplicaciones** > **SQL** > **Crear trabajo de restauración** para abrir el asistente "Restauración de instantáneas".

   Sugerencias:

   - También puede abrir el asistente "Restauración de instantáneas" pulsando **Trabajos y operaciones** > **Crear trabajo de restauración** > **SQL**.
   - Para obtener un resumen en ejecución de las selecciones en el asistente "Restauración de instantáneas", mueva el cursor al icono de información en el panel de navegación del asistente.
   - Para omitir las páginas opcionales en el asistente, seleccione **Omitir pasos opcionales**.
2. En la página **Selección de origen**, lleve a cabo las acciones siguientes:
   a) Pulse un origen de la lista para mostrar las bases de datos que están disponibles para las operaciones de restauración. Puede conmutar los orígenes visualizados para mostrar instancias de SQL Server en un entorno autónomo o de clúster o grupos de disponibilidad Siempre activado utilizando el filtro **Ver**.

      También puede utilizar la función de búsqueda para buscar bases de datos en las instancias o en los grupos de disponibilidad.

   b) Haga clic en el icono de Signo más al lado de la base de datos que desea utilizar como origen de la operación de restauración. Puede seleccionar más de una base de datos en la lista.

      Los orígenes seleccionados se añaden a la lista de restauración situada junto a la lista de bases de datos. Para eliminar un elemento del origen de la lista, haga clic en el icono de signo menos al lado del elemento.

   c) Pulse **Siguiente** para continuar.
3. En la página **Instantánea de origen**, especifique la instancia de la base de datos que desee restaurar. Complete los siguientes campos y pulse **Siguiente** para continuar. Algunos campos no se visualizan hasta que se selecciona un campo relacionado.

Opción	Descripción
Tipo de restauración	Seleccione el tipo de trabajo de restauración: **Bajo demanda: instantánea** Ejecuta un trabajo de restauración puntual desde una instantánea de base de datos. El trabajo de restauración se inicia inmediatamente después de la finalización del asistente. **Bajo demanda: punto en el tiempo** Ejecuta un trabajo de restauración puntual desde una copia de seguridad de un punto en el tiempo de una base de datos. El trabajo de restauración se inicia inmediatamente después de la finalización del asistente. **Recurrente** Crea un trabajo de restauración de punto en el tiempo repetitivo que se ejecuta en una planificación.
Tipo de ubicación de restauración	Seleccione un tipo de ubicación desde donde se restauran los datos: **Sitio** El sitio en el que se hizo la copia de seguridad de las instantáneas. El sitio se define en el panel **Configuración del sistema** > **Sitio**. **Descarga de la nube** El servidor de nube en el que se han descargado las instantáneas. El servidor de nube se define en el panel **Configuración del sistema** > **Almacenamiento de copia de seguridad** > **Cloud**. **Descarga del repositorio** El servidor de repositorio donde se han descargado las instantáneas. El servidor de repositorio se define en el panel **Configuración del sistema** > **Almacenamiento de copia de seguridad** > **Servidor de repositorio**. **Archivado de nube** El servidor de nube en el que se han archivado las instantáneas. El servidor de nube se define en el panel **Configuración del sistema** > **Almacenamiento de copia de seguridad** > **Cloud**. **Archivado de repositorio** El servidor de repositorio en el que se han archivado las instantáneas. El servidor de repositorio se define en el panel **Configuración del sistema** > **Almacenamiento de copia de seguridad** > **Servidor de repositorio**.
Seleccionar una ubicación	Si está restaurando datos desde un sitio, seleccione una de las siguientes ubicaciones de restauración: **Demo** El sitio de demostración desde el que se restauran las instantáneas. **Primario** La ubicación del sitio primario desde la que se restauran las instantáneas. **Secundario** La ubicación del sitio secundario desde la que se restauran las instantáneas. Si está restaurando datos desde un servidor de nube o de repositorio, seleccione un servidor en el menú **Seleccionar una ubicación**.
Selector de fecha	Para las operaciones de restauración bajo demanda, especifique el rango de fechas para el que desea mostrar las instantáneas que están disponibles.
Punto de restauración	Para las operaciones de restauración bajo demanda, seleccione una instantánea en la lista de instantáneas disponibles en el rango de datos seleccionado.

Opción	Descripción
Utilizar el servidor vSnap alternativo para el trabajo de restauración	Si está restaurando datos desde un recurso de nube o un servidor de repositorio, seleccione este recuadro para especificar un servidor de vSnap alternativo y, a continuación, seleccione un servidor en el menú **Seleccionar vSnap alternativo**. Cuando restaura datos desde un punto de restauración que se ha descargado o archivado en un servidor de repositorio o de recursos de nube, se utiliza un servidor vSnap como pasarela para completar la operación. De forma predeterminada, el servidor vSnap que se utiliza para completar la operación de restauración es el mismo servidor vSnap que se utiliza para completar las operaciones de copia de seguridad y de descarga. Para reducir la carga en el servidor vSnap, puede seleccionar un servidor vSnap alternativo para que sirva como pasarela.

4. En la página **Establecer destino** , especifique dónde desea restaurar la base de datos y haga clic en **Siguiente**.

   Restaurar a la instancia original
   Seleccione esta opción para restaurar la base de datos en la instancia original.

   Restaurar a instancia primaria
   Para las operaciones de restauración en un entorno de SQL siempre activado, seleccione esta opción para restaurar la base de datos a la instancia primaria del grupo de disponibilidad siempre activado. La base de datos se vuelve a añadir al grupo.

   Restaurar a la instancia alternativa
   Seleccione esta opción para restaurar la base de datos en un destino local que sea diferente de la instancia original y, a continuación, seleccione la ubicación alternativa de la lista de servidores disponibles.

   Para las operaciones de restauración en un entorno de SQL Siempre activado en modalidad de prueba, la base de datos de disponibilidad de origen se restaura a la instancia de destino seleccionada.

   Para las operaciones de restauración en un entorno de SQL Siempre activado en modalidad de producción, la base de datos restaurada se añade al grupo de disponibilidad de destino si la instancia de destino es una réplica primaria. Si la instancia de destino es una réplica secundaria del grupo de disponibilidad de destino, la base de datos se restaura a la réplica secundaria y se deja en estado de restauración.

   Si la opción de inicialización automática está habilitada para el grupo de disponibilidad de destino, las vías de acceso del archivo de base de datos secundaria se sincronizan con la base de datos primaria. Si el registro de base de datos primario no se trunca, la base de datos secundaria se puede añadir al grupo de disponibilidad por SQL.

5. En la página **Método de restauración** , establezca el trabajo de restauración para que se ejecute en la modalidad de prueba, producción o acceso instantáneo de forma predeterminada.

   Para la modalidad de prueba o de producción, puede especificar opcionalmente un nombre nuevo para la base de datos restaurada.

   Para la modalidad de producción, también puede especificar una nueva carpeta para la base de datos restaurada expandiendo la base de datos e introduciendo un nuevo nombre de carpeta.

   Pulse **Siguiente** para continuar.

   Una vez que se ha creado el trabajo, puede ejecutarlo en la modalidad de prueba, producción o acceso instantáneo en el panel **Sesiones de trabajo**.

6. En la página **Opciones de trabajo**, configure opciones adicionales para el trabajo de restauración y pulse **Siguiente** para continuar.

   Opciones de recuperación
   Establezca las siguientes opciones de recuperación de un punto en el tiempo:

Sin recuperación
Establezca la base de datos seleccionada en un estado EN RESTAURACIÓN. Si gestiona copias de seguridad de registros de transacciones sin utilizar IBM Spectrum Protect Plus, puede restaurar manualmente los archivos de registro y añadir la base de datos a un grupo de disponibilidad, suponiendo que el LSN de las copias de base de datos secundaria y primaria cumple los criterios.

Restricción: La opción **Sin recuperación** no da soporte a las operaciones de restauración de modalidad de producción para los grupos SQL Siempre activado.

Recuperar hasta el final de la copia de seguridad
Restaure la base de datos seleccionada al estado que tenía en el momento en que se creó la copia de seguridad.

Recuperar hasta un momento específico
Cuando la copia de seguridad de registro se habilita utilizando una definición de trabajo de copia de seguridad de SQL, las opciones de restauración de punto en el tiempo estarán disponibles cuando cree una definición de trabajo de restauración de SQL. Seleccione una de las siguientes opciones:

- **Por horas**. Seleccione esta opción para configurar una recuperación de un punto en el tiempo a partir de una fecha y hora específicas.
- **Por ID de transacción**. Seleccione esta opción para configurar una recuperación de un momento específico por el ID de transacción.

En una operación de restauración autónoma, IBM Spectrum Protect Plus busca los puntos de restauración que continúan directamente y siguen el punto en el tiempo seleccionado. Durante la recuperación, se montan el volumen de copia de seguridad de datos más antiguo y el volumen de copia de seguridad de registro más reciente. Si el punto en el tiempo es posterior a la última operación de copia de seguridad, se crea un punto de restauración temporal.

Cuando ejecuta operaciones de restauración en un entorno de SQL Siempre activado en modalidad de prueba, la base de datos restaurada se unirá a la instancia en la que reside el grupo de disponibilidad.

Cuando ejecuta operaciones de restauración en un entorno de SQL Siempre activado en modalidad de producción, la base de datos primaria restaurada se une al grupo de disponibilidad. Si la opción de inicialización automática está habilitada para el grupo de disponibilidad de destino, las vías de acceso del archivo de base de datos secundaria se sincronizan con la base de datos primaria. Si el registro de base de datos primario no se trunca, la base de datos secundaria se puede añadir al grupo de disponibilidad por SQL.

Opciones de la aplicación
Establezca las opciones de la aplicación:

Sobrescribir base de datos existente
Habilite el trabajo de restauración para sobrescribir la base de datos seleccionada. De forma predeterminada, esta opción no está habilitada.

Consejo: Antes de ejecutar operaciones de restauración en un entorno de SQL Siempre activado utilizando la modalidad de producción con la opción **Sobrescribir la base de datos existente**, asegúrese de que la base de datos no esté presente en las réplicas del grupo de disponibilidad de destino. Para ello, debe limpiar manualmente las bases de datos originales (para que se sobrescriban) desde todas las réplicas del grupo de disponibilidad de destino.

Número máximo de streams paralelos por base de datos
Establezca el número máximo de secuencias de datos en paralelo desde el almacenamiento de copia de seguridad por base de datos. Este valor se aplica a cada base de datos de la definición de trabajo. Si el valor de la opción se establece en 1, todavía se pueden restaurar varias bases de datos en paralelo. Múltiples secuencias paralelas pueden mejorar la velocidad de restauración, pero el alto consumo de ancho de banda puede afectar al rendimiento general del sistema.

Esta opción solo es aplicable cuando restaura una base de datos de SQL Server a su ubicación original utilizando su nombre de base de datos original.

Opciones avanzadas
Establezca las opciones de definición de trabajo avanzadas:

Ejecutar la limpieza inmediatamente en caso de anomalía del trabajo
Limpia automáticamente los recursos asignados como parte de una operación de restauración si falla la recuperación.

Permitir la sobrescritura de sesión
Seleccione esta opción para sustituir una base de datos existente por una base de datos con el mismo nombre durante la recuperación. Cuando se realiza una restauración de disco instantánea para una base de datos y otra base de datos con el mismo nombre ya se está ejecutando en el host o clúster de destino, IBM Spectrum Protect Plus cierra la base de datos existente antes de iniciar la base de datos recuperada. Si esta opción no está seleccionada, el trabajo de restauración falla cuando IBM Spectrum Protect Plus detecta una base de datos en ejecución con el mismo nombre.

Continuar con las restauraciones de otras bases de datos incluso si una falla
Alterne la recuperación de un recurso en una serie si falla la recuperación del recurso anterior. Si esta opción no está habilitada, el trabajo de restauración se detiene si falla la recuperación de un recurso.

Prioridad de protocolo (solo acceso instantáneo)
Si hay disponible más de un protocolo de almacenamiento, seleccione el protocolo para que tenga prioridad en el trabajo. Los protocolos disponibles son **iSCSI** y **Canal de fibra**.

Prefijo de punto de montaje
Para las operaciones de restauración de acceso instantáneo, especifique el prefijo de la vía de acceso donde se va a dirigir el punto de montaje.

7. Opcional: En la página **Aplicar scripts**, especifique los scripts que se pueden ejecutar antes o después de que se ejecute una operación en el nivel de trabajo. Los scripts Batch y PowerShell están soportados.

Script anterior
Seleccione este recuadro de selección para elegir un script cargado y una aplicación o un servidor de scripts en el que se ejecutará el script anterior. Para seleccionar un servidor de aplicaciones en el que se va a ejecutar el script anterior, desmarque el recuadro de selección **Utilizar servidor de scripts**. Los scripts y los servidores de scripts se configuran en la página **Configuración del sistema** > **Script** .

Script posterior
Seleccione esta opción para elegir un script cargado y una aplicación o un servidor de scripts en el que se ejecutará el script posterior. Para seleccionar un servidor de aplicaciones en el que se ejecutará el script posterior, desmarque el recuadro de selección **Utilizar servidor de scripts**. Los scripts y los servidores de scripts se configuran en la página **Configuración del sistema** > **Script** .

Continuar trabajo/tarea en error de script
Seleccione este recuadro de selección para continuar ejecutando el trabajo si falla el script asociado con el trabajo.

Cuando selecciona este recuadro de selección, si un script anterior o script posterior completa el proceso con un código de retorno distinto de cero, se intenta la operación de copia de seguridad o restauración y se informa del estado de la tarea de script anterior como COMPLETADO. Si un script posterior completa el proceso con un código de retorno distinto de cero, se informa sobre el estado de la tarea del script posterior como COMPLETADO.

Si desmarca este recuadro de selección, no se intenta realizar la operación de copia de seguridad o restauración, y el estado de la tarea del script anterior o del script posterior se notifica como FALLIDO.

8. Realice una de las acciones siguientes en la página **Planificación** :

- Si está ejecutando un trabajo bajo demanda, pulse **Siguiente**.

- Si está configurando un trabajo recurrente, especifique un nombre para la planificación de trabajos y especifique la frecuencia y el momento en que se inicia el trabajo de restauración. Pulse **Siguiente**.

9. En la página **Revisar**, revise los valores del trabajo de restauración y pulse **Enviar** para crear el trabajo.

Resultados

Un trabajo bajo demanda empieza después de pulsar **Enviar** y unos momentos después, se añade el registro **onDemandRestore** al panel **Sesiones de trabajo**. Para ver el progreso de la operación de restauración, expanda el trabajo. También puede descargar el archivo de registro pulsando el icono de descarga  .

Un trabajo recurrente se iniciará a la hora de inicio planificada cuando inicie la planificación en la página **Trabajos y operaciones** > **Planificación**.

Todos los trabajos en ejecución se pueden visualizar en la página **Trabajos y operaciones** > **Trabajos en ejecución**.

Conceptos relacionados

"Configuración de scripts para las operaciones de copia de seguridad y restauración" en la página 261
Los scripts anteriores y posteriores son scripts que se pueden ejecutar antes o después de que los trabajos de copia de seguridad y restauración se ejecuten en el nivel de trabajo. Los scripts soportados incluyen scripts de shell para máquinas basadas en Linux y scripts Batch y PowerShell para máquinas basadas en Windows. Los scripts se crean localmente, se suben al entorno a través de la página **Script** y se aplican a continuación a las definiciones de trabajos.

Tareas relacionadas

"Adición de un servidor de aplicaciones de SQL Server" en la página 227
Cuando se añade un servidor de aplicaciones de SQL Server, se captura un inventario de las instancias de bases de datos que están asociadas al servidor de aplicaciones y se añade a IBM Spectrum Protect Plus. Este proceso permite completar trabajos de copia de seguridad y restauración, así como informes de ejecución.

"Copia de seguridad de datos de SQL Server" en la página 229
Utilice un trabajo de copia de seguridad para realizar copias de seguridad de entornos SQL Server con instantáneas.

Copia de seguridad y restauración de datos de Oracle

Para proteger contenido de Oracle, registre primero la instancia de Oracle para que IBM Spectrum Protect Plus la reconozca. A continuación, cree trabajos para las operaciones de copia de seguridad y restauración

Asegúrese de que el entorno de Oracle cumple los requisitos del sistema en "Requisitos de Oracle" en la página 39.

Adición de un servidor de aplicaciones Oracle

Cuando se añade un servidor de aplicaciones Oracle, se captura un inventario de las instancias y bases de datos asociadas al servidor de aplicaciones y se añade a IBM Spectrum Protect Plus. Este proceso permite completar trabajos de copia de seguridad y restauración, así como informes de ejecución.

Procedimiento

Para registrar un servidor de aplicaciones Oracle, complete los pasos siguientes.

1. En el panel de navegación, pulse **Gestionar protección** > **Aplicaciones** > **Oracle** > **Copia de seguridad**.
2. Pulse **Gestionar servidores de aplicaciones**.
3. Pulse **Añadir servidor de aplicaciones** para añadir la máquina host.

4. En el panel **Propiedades de aplicación**, especifique la dirección de host.

   La dirección de host es una dirección IP que se puede resolver, o una vía de acceso y un nombre de máquina que se pueden resolver.

5. Seleccione **Usuario** o **Clave SSH**.

Opción	Descripción
Usuario	Pulse en esta opción para especificar un usuario existente o especifique un ID de usuario y contraseña. El usuario debe tener configurados privilegios **sudo**. Rellene los campos según se indica a continuación: **Utilizar usuario existente** Marque este recuadro de selección para utilizar un nombre de usuario y una contraseña especificados anteriormente para el servidor de aplicaciones. Seleccione un nombre de usuario en la lista **Seleccionar usuario**. **ID de usuario** Especifique el nombre de usuario para el servidor de aplicaciones. Si la máquina virtual se conecta a un dominio, la identidad de usuario respeta el formato predeterminado *dominio\nombre*. Si el usuario es un administrador local, utilice el formato *local_administrator*. Solo para la autenticación basada en Kerberos, la identidad de usuario se debe especificar en el formato de nombre de usuario @FQDN. El nombre de usuario debe poderse autenticar utilizando la contraseña registrada para obtener un tíquet de otorgamiento de tíquet (TGT) del centro de distribución de claves (KDC) en el dominio que se especifica mediante el nombre de dominio completo. **Contraseña** Escriba la contraseña del servidor de aplicaciones.
Clave SSH	Pulse en esta opción para utilizar una clave SSH. Seleccione una clave de la lista **Seleccionar una clave SSH**.

6. Para proteger bases de datos multihebra en Oracle 12c y versiones posteriores, proporcione credenciales para la base de datos:
   a) Pulse **Obtener bases de datos** para detectar la lista de bases de datos de Oracle en el servidor de host que está agregando.

      Cada base de datos de Oracle se muestra con su nombre, estado y una indicación de si las credenciales se han especificado anteriormente para la base de datos.

   b) Para cada base de datos multihebra que quiera proteger, pulse **Establecer credencial** y especifique el ID de usuario y contraseña. Si quiere, puede seleccionar un usuario existente en la lista **Seleccionar usuario**.

      Debe especificar las credenciales de un usuario de base de datos de Oracle que tenga privilegios SYSDBA.

7. En **Número máximo de bases de datos simultáneas**, establezca el número máximo de bases de datos en las que se debe realizar una copia de seguridad simultáneamente en el servidor.

   El rendimiento del servidor se ve afectado cuando se realiza una copia de seguridad de muchas bases de datos de forma simultánea, ya que cada base de datos utiliza múltiples hebras y consume ancho de banda al copiar datos. Utilice esta opción para controlar el impacto en los recursos del servidor y minimizar el impacto en las operaciones de producción.

8. Pulse **Guardar**. IBM Spectrum Protect Plus confirma una conexión de red, añade el servidor de aplicaciones a la base de datos de IBM Spectrum Protect Plus y a continuación, cataloga la instancia.

   Si aparece un mensaje que indica que la conexión no se ha realizado correctamente, revise las entradas. Si las entradas son correctas y la conexión no se ha realizado correctamente, póngase en contacto con un administrador del sistema para revisar las conexiones.

Qué hacer a continuación

Después de añadir el servidor de aplicaciones Oracle, realice la acción siguiente:

Acción	Cómo
Asigne permisos de usuario al servidor de aplicaciones.	Consulte “Creación de un rol” en la página 308.

Conceptos relacionados

“Gestión del acceso de usuarios” en la página 303
Al utilizar el control de acceso basado en roles, puede establecer los recursos y permisos disponibles en las cuentas de usuario de IBM Spectrum Protect Plus.

Tareas relacionadas

“Copia de seguridad de datos de Oracle” en la página 241
Utilice un trabajo de copia de seguridad para realizar copias de seguridad de entornos Oracle con instantáneas.

“Restauración de datos de Oracle” en la página 244
Utilice un trabajo de restauración para restaurar un entorno de Oracle a partir de instantáneas. IBM Spectrum Protect Plus crea un clon vSnap a partir de la versión que se selecciona durante la creación de la definición de trabajo y crea una unidad compartida NFS (Network Files System). A continuación, el agente de IBM Spectrum Protect Plus monta el recurso compartido en el servidor de Oracle donde se va a ejecutar el trabajo de restauración. En el caso de Oracle Real Application Clusters (RAC), el trabajo de restauración se ejecuta en todos los nodos del clúster.

Detección de recursos de Oracle

Los recursos de Oracle se detectan automáticamente después de que el servidor de aplicaciones se añada a IBM Spectrum Protect Plus. Sin embargo, puede ejecutar un trabajo de inventario para detectar cualquier cambio que se haya producido desde que se añadió el servidor de aplicaciones.

Procedimiento

Para ejecutar un trabajo de inventario, realice los pasos siguientes:

1. En el panel de navegación, pulse **Gestionar protección** > **Aplicaciones** > **Oracle** > **Copia de seguridad**.
2. En la lista de instancias de Oracle, seleccione una instancia o pulse el enlace de la instancia para navegar hasta el recurso que desee. Por ejemplo, si desea ejecutar un trabajo de inventario para una base de datos individual de la instancia, pulse el enlace de instancia y, a continuación, seleccione una máquina virtual.
3. Pulse **Ejecutar inventario**.

Prueba de conexión con un servidor de aplicaciones Oracle

Puede probar la conexión con un host de Oracle. La función de prueba verifica la comunicación con el host y prueba los valores de DNS entre el dispositivo virtual de IBM Spectrum Protect y el host.

Procedimiento

Para probar la conexión, complete los pasos siguientes:

1. En el panel de navegación, pulse **Gestionar protección** > **Aplicaciones** > **Oracle** > **Copia de seguridad**.
2. Pulse **Gestionar servidores de aplicaciones**.
3. En la lista de hosts, pulse **Probar** en el menú **Acciones** del host.

Copia de seguridad de datos de Oracle

Utilice un trabajo de copia de seguridad para realizar copias de seguridad de entornos Oracle con instantáneas.

Antes de empezar

Revise la siguiente información:

- Para asegurarse de que los permisos del sistema de archivos se conservan correctamente cuando IBM Spectrum Protect Plus mueva los datos de Oracle entre servidores, asegúrese de que los ID de usuario y grupo de los usuarios de Oracle (por ejemplo, oracle, oinstall, dba) sean coherentes en todos los servidores. Consulte la documentación de Oracle para obtener los valores uid y gid recomendados.
- Si un trabajo de inventario de Oracle se ejecuta en el mismo período de tiempo o en un periodo de tiempo corto después de un trabajo de copia de seguridad de Oracle, es posible que se produzcan errores de copia debido a montajes temporales que se crean durante el trabajo de copia de seguridad. Como práctica recomendada, planifique los trabajos de inventario de Oracle para que no se solapen con los trabajos de copia de seguridad de Oracle.
- Evite configurar la copia de seguridad de registro para una única base de datos de Oracle utilizando varios trabajos de copia de seguridad. Si se añade una única base de datos Oracle a varias definiciones de trabajo con la copia de seguridad de registro habilitada, una copia de seguridad de registro de un trabajo podría truncar un registro antes de que se realice una copia de seguridad con el siguiente trabajo. Esto puede provocar que fallen los trabajos de restauración de un momento específico.
- La recuperación de un momento específico no está soportada cuando se añaden uno o más archivos de datos a la base de datos en el período comprendido entre el momento específico elegido y el tiempo en el que se ejecutó el trabajo de copia de seguridad anterior.

Realice las acciones siguientes:

- Para que un usuario pueda implementar operaciones de copia de seguridad y restauración de IBM Spectrum Protect Plus, deben asignarse roles y grupos de recursos al usuario. Otorgue a los usuarios acceso a los recursos y a las operaciones de copia de seguridad y restauración mediante el panel **Cuentas**. Para obtener más información, consulte el apartado Capítulo 13, “Gestión del acceso de usuarios”, en la página 303.
- Registre los proveedores cuya copia de seguridad desea realizar. Para obtener más información, consulte el apartado “Adición de un servidor de aplicaciones Oracle” en la página 239.
- Configure las políticas de SLA. Para obtener más información, consulte el apartado “Crear políticas de copia de seguridad” en la página 77.

Acerca de esta tarea

Durante la copia de seguridad base inicial, IBM Spectrum Protect Plus crea un volumen de vSnap y una unidad compartida de NFS. Durante las copias de seguridad incrementales, se reutiliza el volumen creado previamente. El agente de IBM Spectrum Protect Plus monta el recurso compartido en el servidor de Oracle en el que se va a completar la copia de seguridad.

En el caso de Oracle Real Application Clusters (RAC), la copia de seguridad se completa desde cualquier nodo del clúster. Cuando la copia de seguridad se ha completado, el agente de IBM Spectrum Protect Plus desmonta el recurso compartido del servidor de Oracle y crea una instantánea vSnap del volumen de copia de seguridad.

IBM Spectrum Protect Plus puede proteger bases de datos multihebra en Oracle 12c y versiones posteriores. Para obtener instrucciones sobre la habilitación de IBM Spectrum Protect Plus para proteger bases de datos multihebra, consulte “Adición de un servidor de aplicaciones Oracle” en la página 239.

Procedimiento

Para definir un trabajo de copia de seguridad de Oracle, complete los pasos siguientes:

1. En el panel de navegación, pulse **Gestionar protección** > **Aplicaciones** > **Oracle**.
2. Seleccione las páginas de inicio, bases de datos de Oracle y grupos de discos ASM para realizar una copia de seguridad. Utilice la función de búsqueda para buscar las instancias disponibles.
3. Pulse **Seleccionar una política de SLA** para añadir una o más políticas de SLA que cumplan los criterios de datos de copia de seguridad en la definición de trabajo.
4. Para crear la definición de trabajo utilizando las opciones predeterminadas, pulse **Guardar**.

El trabajo se ejecuta según lo definido en las políticas de SLA que ha seleccionado. Para ejecutar el trabajo manualmente, pulse **Trabajos y operaciones** > **Planificación**. Seleccione el trabajo y pulse **Acciones** > **Iniciar**.

Sugerencia: el botón **Ejecutar** solo se habilita para una copia de seguridad de base de datos individual, y la base de datos debe tener una política de SLA aplicada.

5. Para editar opciones antes de crear la definición de trabajo, pulse **Seleccionar opciones**. Establezca las opciones de definición de trabajo.

   Habilitar copia de seguridad de registro

   Habilitar copia de seguridad de registro debe estar seleccionado para permitir la restauración de un momento específico de Oracle.

   Seleccione **Habilitar copia de seguridad de registro** para permitir que IBM Spectrum Protect Plus cree automáticamente un volumen de copia de seguridad de registro y móntelo en el servidor de aplicaciones. A continuación, IBM Spectrum Protect Plus descubre automáticamente la ubicación de los registros archivados primarios existentes y utiliza cron para configurar un trabajo planificado. El trabajo planificado realiza una copia de seguridad de registro de transacción desde la ubicación primaria hasta el volumen de copia de seguridad de registro a la frecuencia especifica por el valor de **Frecuencia**.

   La **Frecuencia** se puede establecer en un valor independiente de la frecuencia de copia de seguridad de base de datos especificada en los valores de política de SLA. Por ejemplo, la Política de SLA se puede configurar para que realice una copia de seguridad de la base de datos una vez al día, mientras que la frecuencia de copia de seguridad de registro se puede establecer en una vez cada 30 minutos.

   En Oracle RAC, IBM Spectrum Protect Plus monta el volumen y configura el trabajo cron en cada uno de los nodos de clúster. Cuando se activa la planificación, los trabajos se coordinan internamente para asegurarse de que cualquier nodo activo complete la copia de seguridad de registro y que los otros nodos no emprendan ninguna acción.

   IBM Spectrum Protect Plus gestiona automáticamente la retención de registros en su propio volumen de copia de seguridad de registro basándose en los valores de retención de la política de SLA.

   Seleccione **Truncar registros de origen después de una copia de seguridad realizada correctamente** para suprimir automáticamente los registros archivados más antiguos de la ubicación de registro archivado primario de la base de datos. Si se borra la opción, los registros archivados en el destino de registro primario no se suprimen y los administradores de base de datos deben continuar gestionando esos registros utilizando sus políticas de retención de registro existentes. Si la opción está seleccionada, IBM Spectrum Protect Plus suprime los registros archivados no necesarios más antiguos de la ubicación de registro principal al final de cada copia de seguridad de base de datos correcta.

   Cuando se selecciona la opción **Truncar registros de origen después de una copia de seguridad realizada correctamente**, establezca la retención de registros primarios a través del valor **Retención de registro primario en días**. Este valor controla la cantidad de registros archivados que se retienen en las ubicaciones de registro archivado primario. Por ejemplo, si **Retención de registro primario en días** se establece en **3**, IBM Spectrum Protect Plus suprime todos los registros archivados de más de tres días de la ubicación de registro archivado primario al final de cada copia de seguridad de base de datos correcta.

   Número máximo de streams paralelos por base de datos

   Establezca el número máximo de stream de datos de cada base de datos en el almacenamiento de copias de seguridad. Este valor se aplica a cada base de datos de la definición de trabajo. Se pueden hacer copias de seguridad de varias bases de datos en paralelo si el valor de la opción se establece en **1**. Múltiples streams paralelos pueden mejorar la velocidad de copia de seguridad, pero el alto consumo de ancho de banda puede afectar al rendimiento general del sistema.
6. Cuando esté seguro de que la información específica del trabajo es correcta, pulse **Guardar**.
7. Para configurar opciones adicionales, pulse el campo **Opciones de política** que está asociado al trabajo en la sección **Estado de política de SLA**. Establezca las opciones de política adicionales:

   Scripts anteriores y scripts posteriores

Ejecute un script anterior o script posterior. Los scripts anteriores y posteriores son scripts que se pueden ejecutar antes o después de que se ejecute un trabajo en el nivel de trabajo. Las máquinas basadas en Windows scripts Batch y PowerShell mientras que las máquinas basadas en Linux admiten scripts de shell.

En la sección **Script anterior** o **Script posterior**, seleccione un script cargado y un servidor de aplicaciones o de script donde se ejecutará el script. Para seleccionar un servidor de aplicaciones en el que se va a ejecutar el script, desmarque el recuadro de selección **Utilizar servidor de scripts**. Los scripts y los servidores de scripts se configuran mediante la página **Configuración del sistema** > **Script**.

Para seguir ejecutando el trabajo si falla el script asociado con el trabajo, seleccione **Continuar trabajo/tarea en error de script**.

Cuando esta opción está habilitada, si un script anterior o un script posterior completa el proceso con un código de retorno distinto de cero, se intenta la operación de copia de seguridad o restauración y se informa sobre el estado de la tarea previa del script anterior como COMPLETADO. Si un script posterior se completa con un código de retorno distinto de cero, se informa sobre el estado de la tarea del script posterior como COMPLETADO.

Cuando esta opción está inhabilitada, no se intenta realizar la copia de seguridad o la restauración y se informa sobre el estado de la tarea del script anterior o del script posterior como FALLIDO.

Excluir recursos

Excluya recursos específicos del trabajo de copia de seguridad mediante patrones de exclusión únicos o múltiples. Los recursos se pueden excluir mediante una coincidencia exacta o con asteriscos comodín especificados antes del patrón (* test) o después del patrón (test *).

También se admiten varios comodines de asterisco en un único patrón. Los patrones admiten caracteres alfanuméricos estándar, así como los siguientes caracteres especiales:-_ y *.

Separe varios con un punto y coma.

Forzar copia de seguridad completa de los recursos

Fuerce operaciones de copia de seguridad base para máquinas virtuales o bases de datos específicas en la definición de trabajo de copia de seguridad. Separe varios recursos con un punto y coma.

Qué hacer a continuación

Después de crear la definición de trabajo de copia de seguridad, realice la acción siguiente:

Acción	Cómo
Cree una definición de trabajo de Restauración de Oracle.	Consulte “Restauración de datos de Oracle” en la página 244.

Conceptos relacionados

“Configuración de scripts para las operaciones de copia de seguridad y restauración” en la página 261
Los scripts anteriores y posteriores son scripts que se pueden ejecutar antes o después de que los trabajos de copia de seguridad y restauración se ejecuten en el nivel de trabajo. Los scripts soportados incluyen scripts de shell para máquinas basadas en Linux y scripts Batch y PowerShell para máquinas basadas en Windows. Los scripts se crean localmente, se suben al entorno a través de la página **Script** y se aplican a continuación a las definiciones de trabajos.

Restauración de datos de Oracle

Utilice un trabajo de restauración para restaurar un entorno de Oracle a partir de instantáneas. IBM Spectrum Protect Plus crea un clon vSnap a partir de la versión que se selecciona durante la creación de la definición de trabajo y crea una unidad compartida NFS (Network Files System). A continuación, el agente de IBM Spectrum Protect Plus monta el recurso compartido en el servidor de Oracle donde se va a ejecutar el trabajo de restauración. En el caso de Oracle Real Application Clusters (RAC), el trabajo de restauración se ejecuta en todos los nodos del clúster.

Antes de empezar

Complete los siguientes requisitos previos:

- Cree y ejecute un trabajo de copia de seguridad de Oracle. Para obtener instrucciones, consulte “Copia de seguridad de datos de Oracle” en la página 241.
- Antes de que un usuario de IBM Spectrum Protect Plus pueda restaurar datos, deben asignarse los roles y los grupos de recursos adecuados al usuario. Otorgue a los usuarios acceso a los recursos y a las operaciones de copia de seguridad y restauración utilizando el panel **Cuentas** . Para obtener instrucciones, consulte Capítulo 13, “Gestión del acceso de usuarios”, en la página 303.

Revise las restricciones siguientes:

- La recuperación de un punto en el tiempo no está soportada si se han añadido uno o más archivos de datos a la base de datos en el período comprendido entre el punto en el tiempo elegido y el momento en que se ejecutó el trabajo de copia de seguridad anterior.
- Si una base de datos Oracle se monta pero no se abre durante un trabajo de copia de seguridad, IBM Spectrum Protect Plus no puede determinar los valores **tempfile** de la base de datos que están relacionados con **autoextensibilidad** y el tamaño máximo. Cuando se restaura una base de datos a partir de este punto de restauración, IBM Spectrum Protect Plus no puede volver a crear **tempfiles** con los valores originales porque son desconocidos. En su lugar, se crean **tempfiles** con los valores predeterminados, "AUTOEXTEND ON" y "MAXSIZE 32767M". Una vez que se haya completado el trabajo de restauración, puede actualizar manualmente los valores.
- Cuando se realiza una restauración desde un archivado de IBM Spectrum Protect, los archivos se migrarán a una agrupación de transferencia desde la cinta antes del inicio del trabajo. Dependiendo del tamaño de la restauración, este proceso puede tardar varias horas.

Acerca de esta tarea

Se admiten las siguientes modalidades de restauración:

Modalidad de acceso instantáneo
En modalidad de acceso instantáneo, no se realiza ninguna acción adicional después del montaje de la unidad compartida. Los usuarios pueden completar cualquier recuperación personalizada utilizando los archivos del volumen vSnap.

Modalidad de prueba
En la modalidad de prueba, el agente crea una nueva base de datos utilizando los archivos de datos directamente desde el volumen vSnap.

Modalidad de producción
En la modalidad de producción, el agente restaura primero los archivos del volumen de vSnap al almacenamiento primario y luego crea la nueva base de datos utilizando los archivos restaurados.

Procedimiento

Para definir un trabajo de restauración de Oracle, complete los pasos siguientes:

1. En el panel de navegación, pulse **Gestionar protección** > **Aplicaciones** > **Oracle** > **Crear trabajo de restauración** para abrir el asistente "Restauración de instantáneas".

   Sugerencias:

   - También puede abrir el asistente "Restauración de instantáneas" pulsando **Trabajos y operaciones** > **Crear trabajo de restauración** > **Oracle**.
   - Para obtener un resumen en ejecución de las selecciones en el asistente "Restauración de instantáneas", mueva el cursor al icono de información en el panel de navegación del asistente.
   - Para omitir las páginas opcionales en el asistente, seleccione **Omitir pasos opcionales**.
2. En la página **Selección de origen**, complete los pasos siguientes:

a) Pulse un origen de la lista para mostrar las bases de datos que están disponibles para las operaciones de restauración. También puede utilizar la función de búsqueda para buscar las instancias disponibles y alternar entre las instancias visualizadas mediante el filtro **Ver**.

b) Haga clic en el icono de Signo más al lado de la base de datos que desea utilizar como origen de la operación de restauración. Puede seleccionar más de una base de datos en la lista.

Los orígenes seleccionados se añaden a la lista de restauración situada junto a la lista de bases de datos. Para eliminar un elemento de la lista, haga clic en el icono de signo Menos al lado del elemento.

c) Pulse **Siguiente** para continuar.

3. En la página **Instantánea de origen**, especifique la instancia de la base de datos que desee restaurar. Complete los siguientes campos y pulse **Siguiente** para continuar. Algunos campos no se visualizan hasta que se selecciona un campo relacionado.

Opción	Descripción
Tipo de restauración	Seleccione el tipo de trabajo de restauración: **Bajo demanda: instantánea** Ejecuta un trabajo de restauración puntual desde una instantánea de base de datos. El trabajo de restauración se inicia inmediatamente después de la finalización del asistente. **Bajo demanda: punto en el tiempo** Ejecuta un trabajo de restauración puntual desde una copia de seguridad de un punto en el tiempo de una base de datos. El trabajo de restauración se inicia inmediatamente después de la finalización del asistente. **Recurrente** Crea un trabajo de restauración de punto en el tiempo repetitivo que se ejecuta en una planificación.
Tipo de ubicación de restauración	Seleccione un tipo de ubicación desde donde se restauran los datos: **Sitio** El sitio en el que se hizo la copia de seguridad de las instantáneas. El sitio se define en el panel **Configuración del sistema** > **Sitio**. **Descarga de la nube** El servidor de nube en el que se han descargado las instantáneas. El servidor de nube se define en el panel **Configuración del sistema** > **Almacenamiento de copia de seguridad** > **Cloud**. **Descarga del repositorio** El servidor de repositorio donde se han descargado las instantáneas. El servidor de repositorio se define en el panel **Configuración del sistema** > **Almacenamiento de copia de seguridad** > **Servidor de repositorio**. **Archivado de nube** El servidor de nube en el que se han archivado las instantáneas. El servidor de nube se define en el panel **Configuración del sistema** > **Almacenamiento de copia de seguridad** > **Cloud**. **Archivado de repositorio** El servidor de repositorio en el que se han archivado las instantáneas. El servidor de repositorio se define en el panel **Configuración del sistema** > **Almacenamiento de copia de seguridad** > **Servidor de repositorio**.
Seleccionar una ubicación	Si está restaurando datos desde un sitio, seleccione una de las siguientes ubicaciones de restauración: **Demo** El sitio de demostración desde el que se restauran las instantáneas.

Opción	Descripción
	Primario La ubicación del sitio primario desde la que se restauran las instantáneas. **Secundario** La ubicación del sitio secundario desde la que se restauran las instantáneas. Si está restaurando datos desde un servidor de nube o de repositorio, seleccione un servidor en el menú **Seleccionar una ubicación**.
Selector de fecha	Para las operaciones de restauración de instantánea bajo demanda, especifique un rango de fechas para mostrar las instantáneas disponibles dentro de ese rango de fechas.
Punto de restauración	Para las operaciones de restauración de instantánea bajo demanda, seleccione una instantánea de la lista de instantáneas disponibles en el rango de datos seleccionado.
Utilizar el servidor vSnap alternativo para el trabajo de restauración	Si está restaurando datos desde un recurso de nube o un servidor de repositorio, seleccione este recuadro para especificar un servidor de vSnap alternativo y, a continuación, seleccione un servidor en el menú **Seleccionar vSnap alternativo**. Cuando restaura datos desde un punto de restauración que se ha descargado o archivado en un servidor de repositorio o de recursos de nube, se utiliza un servidor vSnap como pasarela para completar la operación. De forma predeterminada, el servidor vSnap que se utiliza para completar la operación de restauración es el mismo servidor vSnap que se utiliza para completar las operaciones de copia de seguridad y de descarga. Para reducir la carga en el servidor vSnap, puede seleccionar un servidor vSnap alternativo para que sirva como pasarela.

4. En la página **Establecer destino** , especifique dónde desea restaurar la base de datos y haga clic en **Siguiente**.

   Restaurar a ubicación original
   Seleccione esta opción para restaurar la base de datos en el servidor original.

   Restaurar a ubicación alternativa
   Seleccione esta opción para restaurar la base de datos en un destino local que es diferente del servidor original y, a continuación, seleccione la ubicación alternativa de la lista de servidores disponibles.

5. En la página **Método de restauración** , establezca el trabajo de restauración para que se ejecute en la modalidad de prueba, producción o acceso instantáneo de forma predeterminada.

   Para la modalidad de prueba o de producción, puede especificar opcionalmente un nombre nuevo para la base de datos restaurada.

   Para la modalidad de producción, también puede especificar una nueva carpeta para la base de datos restaurada expandiendo la base de datos e introduciendo un nuevo nombre de carpeta.

   Pulse **Siguiente** para continuar.

   Una vez que se ha creado el trabajo, se puede ejecutar en la modalidad de prueba, producción o acceso instantáneo en el panel **Sesiones de trabajo** .

6. En la página **Opciones de trabajo**, configure opciones adicionales para el trabajo de restauración y pulse **Siguiente** para continuar.

   Opciones de recuperación
   Establezca las siguientes opciones de recuperación de un punto en el tiempo:

Recuperar hasta el final de la copia de seguridad
Restaure la base de datos seleccionada al estado que tenía en el momento en que se creó la copia de seguridad.

Recuperar hasta un momento específico
Cuando la copia de seguridad de registro se habilita utilizando una definición de trabajo de copia de seguridad de Oracle, las opciones de restauración de un punto en el tiempo estarán disponibles cuando cree una definición de trabajo de restauración de Oracle. Seleccione una de las opciones siguientes y, a continuación, pulse **Guardar**:

- **Por horas**. Seleccione esta opción para configurar una recuperación de un punto en el tiempo a partir de una fecha y hora específicas.
- **Por SCN**. Seleccione esta opción para configurar una recuperación de un momento específico por el número de cambio de sistema (SCN).

IBM Spectrum Protect Plus busca los puntos de restauración que continúan directamente y siguen el punto en el tiempo seleccionado. Durante la recuperación, se montan el volumen de copia de seguridad de datos más antiguo y el volumen de copia de seguridad de registro más reciente. Si se ha producido el punto en el tiempo después de la última copia de seguridad, se crea un punto de restauración temporal.

Opciones de la aplicación
Establezca las opciones de la aplicación:

Sobrescribir base de datos existente
Habilite esta opción para permitir que el trabajo de restauración sobrescriba la base de datos seleccionada. De forma predeterminada, esta opción no está seleccionada.

Número máximo de streams paralelos por base de datos
Establezca el número máximo de secuencias de datos en paralelo desde el almacenamiento de copia de seguridad por base de datos. Este valor se aplica a cada base de datos de la definición de trabajo. Si el valor de la opción se establece en 1, todavía se pueden restaurar varias bases de datos en paralelo. Múltiples secuencias paralelas pueden mejorar la velocidad de restauración, pero el alto consumo de ancho de banda puede afectar al rendimiento general del sistema.

Esta opción solo es aplicable cuando restaura una base de datos Oracle a su ubicación original utilizando su nombre de base de datos original.

Parámetros de inicialización
Esta opción controla los parámetros de inicialización que se utilizan para iniciar la base de datos recuperada en los flujos de trabajo de prueba y producción de Oracle.

Origen. Esta es la opción predeterminada. IBM Spectrum Protect Plus utiliza los mismos parámetros de inicialización que la base de datos de origen, pero con los cambios siguientes:

- Los parámetros que contienen vías de acceso como, por ejemplo, **control_files**, **db_recovery_file_dest** o **log_archive_dest_*** se actualizan para reflejar las nuevas vías de acceso basadas en los puntos de montaje renombrados de los volúmenes recuperados.
- Los parámetros como **audit_file_dest** y **diagnostic_dest** se actualizan para que apunten a la ubicación adecuada bajo el directorio base de Oracle en el servidor de destino si la vía de acceso difiere del servidor de origen.
- Si se especifica un nombre nuevo para la base de datos, los parámetros **db_name** y **db_unique_name** se actualizan para reflejar el nuevo nombre.
- Los parámetros relacionados con el clúster, como por ejemplo, **instance_number**, **thread** y **cluster_database**, los establece automáticamente IBM Spectrum Protect Plus, en función de los valores adecuados para el destino.

Destino. Personalice los parámetros de inicialización especificando un archivo de plantilla que contenga los parámetros de inicialización que utiliza IBM Spectrum Protect Plus.

La vía de acceso especificada debe apuntar a un archivo de texto sin formato que existe en el servidor de destino y que el usuario de IBM Spectrum Protect Plus puede leer. El archivo debe estar en el formato `pfile` de Oracle, que consta de líneas en el formato siguiente:

```
name = value
```

Los comentarios que empiezan por el carácter # se ignoran.

IBM Spectrum Protect Plus lee el `pfile` de plantilla y copia las entradas en el nuevo `pfile` que se utiliza para iniciar la base de datos recuperada. Sin embargo, se ignoran los parámetros siguientes de la plantilla. En lugar de ello, IBM Spectrum Protect Plus establece sus valores para reflejar los valores apropiados de la base de datos de origen o para reflejar las nuevas vías de acceso basadas en los puntos de montaje renombrados de los volúmenes recuperados.

- **control_files**
- **db_block_size**
- **db_create_file_dest**
- **db_recovery_file_dest**
- **log_archive_dest**
- **spfile**
- **undo_tablespace**

Además, los parámetros relacionados con el clúster como por ejemplo, **instance_number**, **thread** y **cluster_database** los establece automáticamente IBM Spectrum Protect Plus, en función de los valores adecuados para el destino.

Opciones avanzadas
Establezca las opciones de definición de trabajo avanzadas:

Ejecutar la limpieza inmediatamente en caso de anomalía del trabajo
Habilite esta opción para limpiar automáticamente los recursos asignados como parte de una operación de restauración si falla la recuperación.

Permitir la sobrescritura de sesión
Seleccione esta opción para sustituir una base de datos existente por una base de datos con el mismo nombre durante la recuperación. Cuando se realiza una restauración de disco instantánea para una base de datos y otra base de datos con el mismo nombre ya se está ejecutando en el host o clúster de destino, IBM Spectrum Protect Plus cierra la base de datos existente antes de iniciar la base de datos recuperada. Si esta opción no está seleccionada, el trabajo de restauración falla cuando IBM Spectrum Protect Plus detecta una base de datos en ejecución con el mismo nombre.

Continuar con las restauraciones de otras bases de datos incluso si una falla
Alterne la recuperación de un recurso en una serie si falla la recuperación del recurso anterior. Si esta opción no está habilitada, el trabajo de restauración se detiene si falla la recuperación de un recurso.

Prioridad de protocolo (solo acceso instantáneo)
Si hay disponible más de un protocolo de almacenamiento, seleccione el protocolo para que tenga prioridad en el trabajo. Los protocolos disponibles son **iSCSI** y **Canal de fibra**.

Prefijo de punto de montaje
Para las operaciones de restauración de acceso instantáneo, especifique el prefijo de la vía de acceso donde se va a dirigir el punto de montaje.

7. Opcional: En la página **Aplicar scripts**, especifique los scripts que se pueden ejecutar antes o después de que se ejecute una operación en el nivel de trabajo. Los scripts de proceso por lotes y PowerShell están soportados en sistemas operativos Windows, y los scripts de shell están soportados en sistemas operativos Linux.

Script anterior
Seleccione este recuadro de selección para elegir un script cargado y una aplicación o un servidor de scripts en el que se ejecutará el script anterior. Para seleccionar un servidor de aplicaciones en

el que se va a ejecutar el script anterior, desmarque el recuadro de selección **Utilizar servidor de scripts**. Los scripts y los servidores de scripts se configuran en la página **Configuración del sistema** > **Script** .

Script posterior
Seleccione este recuadro de selección para elegir un script cargado y un servidor de aplicaciones o de scripts en el que se ejecutará el script posterior. Para seleccionar un servidor de aplicaciones en el que se ejecutará el script posterior, desmarque el recuadro de selección **Utilizar servidor de scripts**. Los scripts y los servidores de scripts se configuran en la página **Configuración del sistema** > **Script** .

Continuar trabajo/tarea en error de script
Seleccione este recuadro de selección para continuar ejecutando el trabajo si falla el script asociado con el trabajo.

Cuando selecciona este recuadro de selección, si un script anterior o script posterior completa el proceso con un código de retorno distinto de cero, se intenta la operación de copia de seguridad o restauración y se informa del estado de la tarea de script anterior como COMPLETADO. Si un script posterior completa el proceso con un código de retorno distinto de cero, se informa sobre el estado de la tarea del script posterior como COMPLETADO.

Si desmarca este recuadro de selección, la copia de seguridad o la restauración no se intentan, y el estado de la tarea del script anterior o del script posterior se notifica como FALLIDO.

8. Realice una de las acciones siguientes en la página **Planificación** :
   - Si está ejecutando un trabajo bajo demanda, pulse **Siguiente**.
   - Si está configurando un trabajo recurrente, especifique un nombre para la planificación de trabajos y especifique la frecuencia y el momento en que se inicia el trabajo de restauración. Pulse **Siguiente**.
9. En la página **Revisar**, revise los valores del trabajo de restauración y pulse **Enviar** para crear el trabajo.

Resultados

Un trabajo bajo demanda empieza después de pulsar **Enviar** y unos momentos después, se añade el registro **onDemandRestore** al panel **Sesiones de trabajo**. Para ver el progreso de la operación de restauración, expanda el trabajo. También puede descargar el archivo de registro pulsando el icono de descarga  .

Un trabajo recurrente se iniciará a la hora de inicio planificada cuando inicie la planificación en la página **Trabajos y operaciones** > **Planificación**.

Todos los trabajos en ejecución se pueden visualizar en la página **Trabajos y operaciones** > **Trabajos en ejecución**.

Qué hacer a continuación

Las bases de datos de Oracle siempre se restauran en modalidad que no es multihebra. Si las bases de datos que restaura estaban originalmente en modalidad multihebra, una vez finalizada la operación de restauración, debe configurar manualmente las credenciales y cambiar las bases de datos a modalidad multihebra.

Conceptos relacionados

"Configuración de scripts para las operaciones de copia de seguridad y restauración" en la página 261
Los scripts anteriores y posteriores son scripts que se pueden ejecutar antes o después de que los trabajos de copia de seguridad y restauración se ejecuten en el nivel de trabajo. Los scripts soportados incluyen scripts de shell para máquinas basadas en Linux y scripts Batch y PowerShell para máquinas basadas en Windows. Los scripts se crean localmente, se suben al entorno a través de la página **Script** y se aplican a continuación a las definiciones de trabajos.

Tareas relacionadas

"Adición de un servidor de aplicaciones Oracle" en la página 239

Cuando se añade un servidor de aplicaciones Oracle, se captura un inventario de las instancias y bases de datos asociadas al servidor de aplicaciones y se añade a IBM Spectrum Protect Plus. Este proceso permite completar trabajos de copia de seguridad y restauración, así como informes de ejecución.

Capítulo 9. Protección de IBM Spectrum Protect Plus

Proteja la aplicación de IBM Spectrum Protect Plus realizando una copia de seguridad de las bases de datos subyacentes para los escenarios de recuperación ante desastre. Se realiza una copia de seguridad de los valores de configuración, los recursos registrados, los puntos de restauración, los valores de almacenamiento de copia de seguridad, los datos de búsqueda y la información de trabajo en un servidor vSnap definido en la política de SLA asociada.

Copia de seguridad de la aplicación de IBM Spectrum Protect Plus

Realice una copia de seguridad de los valores de configuración de IBM Spectrum Protect Plus, de las políticas de SLA, los recursos registrados, los valores de almacenamiento de copias de seguridad, los puntos de restauración, los datos de búsqueda y las claves y certificados importados a un servidor vSnap que esté definido en la política de SLA asociada.

Antes de empezar

Asegúrese de que la política de SLA apropiada está disponible. Para optimizar los trabajos de copia de seguridad, cree políticas de SLA específicamente para realizar la copia de seguridad de IBM Spectrum Protect Plus. Para reducir la carga del sistema, asegúrese de que no se han planificado otros trabajos para ejecutarlos durante el trabajo de copia de seguridad de IBM Spectrum Protect Plus. Para crear una política de SLA, consulte “Creación de una política de SLA” en la página 93.

Restricción: No puede seleccionar el servidor de vSnap incorporado como destino de la política de SLA de copia de seguridad de IBM Spectrum Protect Plus. El servidor de vSnap incorporado se denomina localhost y se instala automáticamente cuando inicialmente el dispositivo de IBM Spectrum Protect Plus se despliega. Seleccione un servidor de vSnap externo secundario como destino cuando cree una política de SLA para la copia de seguridad

Un catálogo de IBM Spectrum Protect Plus se puede restaurar a la misma ubicación o a una ubicación alternativa de IBM Spectrum Protect Plus en los casos de ejemplo de recuperación tras desastre.

Procedimiento

Para realizar una copia de seguridad de los datos de IBM Spectrum Protect Plus:

1. En el panel de navegación, pulse **Gestionar protección** > **IBM Spectrum Protect Plus** > **Copia de seguridad**.
2. Seleccione una política de SLA para asociarla a la operación de copia de seguridad del catálogo de IBM Spectrum Protect Plus. La política de SLA define la planificación de la copia de seguridad del catálogo, junto con los valores de destino de copia de seguridad, de réplica y de descarga. Los datos de copia de seguridad de catálogo también se pueden descargar en los recursos de nube y en los servidores de repositorio
3. Pulse **Guardar** para crear la definición de trabajo.

Resultados

El trabajo se ejecuta según lo definido en las políticas de SLA que ha seleccionado, o bien puede ejecutar manualmente el trabajo pulsando **Trabajos y operaciones** > **Planificación**. A continuación, seleccione el trabajo en la pestaña **Planificación** y pulse **Acciones** > **Iniciar**. Para obtener instrucciones, consulte “Iniciar un trabajo de copia de seguridad” en la página 84.

Restauración de la aplicación de IBM Spectrum Protect Plus

Restaure los valores de configuración, los puntos de restauración, los datos de búsqueda y la información de trabajos de IBM Spectrum Protect Plus cuya copia de seguridad se realizó en el servidor vSnap. Los datos se pueden restaurar a la misma ubicación o a otra ubicación de IBM Spectrum Protect Plus.

Acerca de esta tarea

Atención: Una operación de restauración de IBM Spectrum Protect Plus sobrescribe todos los datos en el dispositivo virtual de IBM Spectrum Protect Plus o en la ubicación de dispositivo virtual alternativo. Se detienen todas las operaciones de IBM Spectrum Protect Plus mientras se restauran los datos. La interfaz de usuario no es accesible y todos los trabajos que se están ejecutando se cancelan. Las instantáneas que se crean entre las operaciones de copia de seguridad y restauración no se guardan.

Si se restaura una copia de seguridad en la nube descargada, el recurso de nube o el servidor de repositorio debe estar registrado en la ubicación de IBM Spectrum Protect Plus alternativa.

Procedimiento

Para restaurar datos de IBM Spectrum Protect Plus:

1. En el panel de navegación, pulse **Gestionar protección** > **IBM Spectrum Protect Plus** > **Restaurar**.
2. Seleccione un servidor vSnap, un recurso de nube o un servidor de repositorio.

   Los datos se pueden restaurar a la misma ubicación, o a una ubicación alternativa en los casos de ejemplo de recuperación tras desastre.

   Se visualizan las instantáneas disponibles del servidor.
3. Pulse **Restaurar** para la instantánea del catálogo que desea restaurar.
4. Seleccione una de los siguientes modalidades de restauración:

   Restaurar el catálogo y suspender todos los trabajos planificados
   El catálogo se restaura y todos los trabajos planificados se dejan en un estado suspendido. No se inician los trabajos planificados, lo que permite validar y probar entradas de catálogo así como crear nuevos trabajos. Normalmente, esta opción se utiliza en los casos de uso de DevOps.

   Restaurar el catálogo
   El catálogo se restaura y todos los trabajos planificados continúan ejecutándose en la copia de seguridad del catálogo. Normalmente, esta opción se utiliza en la recuperación tras desastre.
5. Pulse **Restaurar**.
6. Para ejecutar el trabajo de restauración, en el recuadro de diálogo, pulse **Sí**.

Gestión de puntos de restauración de IBM Spectrum Protect Plus

Puede utilizar el panel **Retención del punto de restauración** para buscar puntos de restauración en el catálogo de IBM Spectrum Protect Plus por el nombre de trabajo de copia de seguridad, ver las fechas de creación y de caducidad y alterar temporalmente la retención asignada.

Acerca de esta tarea

Cuando una sesión de trabajo caduca, no se eliminarán una instantánea y el punto de recuperación relacionado si la instantánea está bloqueada por una relación de réplica o descarga. Ejecute el trabajo de réplica o habilitado para la descarga para cambiar el bloqueo en una instantánea posterior. La instantánea y el punto de recuperación se eliminarán durante la siguiente ejecución del trabajo de mantenimiento.

Procedimiento

Para establecer una sesión de trabajo para que caduque:

1. En el panel de navegación, pulse **Gestionar protección** > **IBM Spectrum Protect Plus** > **Retención del punto de restauración**.
2. En la pestaña Sesiones de copia de seguridad, busque la sesión de trabajo o el punto de restauración deseado. Para obtener más información sobre el uso de la función de búsqueda, consulte Apéndice A, “Directrices de búsqueda”, en la página 321.
3. Utilice filtros para ajustar la búsqueda entre tipos de trabajo y rangos de fechas cuando se inicie el trabajo de copia de seguridad asociado.
4. Pulse el icono de búsqueda .
5. Seleccione las sesiones de trabajo que desea que caduquen.
6. En la lista **Acciones**, seleccione una de las opciones siguientes:
   - **Caducar** para que caduque una única sesión de trabajo.
   - **Caducar todas las sesiones de trabajo** para que caduquen todas las sesiones de trabajo no caducadas para el trabajo seleccionado.
7. Para confirmar la caducidad, en el recuadro de diálogo, pulse **Sí**.

Resultados
La sesión de trabajo se elimina durante la siguiente ejecución del trabajo de mantenimiento.
Conceptos relacionados
“Tipos de trabajo” en la página 257
Los trabajos se utilizan para ejecutar operaciones de copia de seguridad, restauración, mantenimiento e inventario en IBM Spectrum Protect Plus.

Supresión de recursos de IBM Spectrum Protect Plus del catálogo

Puede utilizar la pestaña **Máquinas virtuales/bases de datos** en el panel **Retención del punto de restauración** para que caduquen los metadatos del catálogo asociados a un recurso en el catálogo IBM Spectrum Protect Plus. Los recursos se añaden al catálogo a través de trabajos de inventario. Cuando un recurso caduca, se eliminan los metadatos asociados a un punto de restauración del catálogo, lo cual libera espacio en el catálogo y elimina el punto de restauración de las pantallas de recuperación.

Acerca de esta tarea
Cuando caduca un recurso del catálogo no se elimina las instantáneas asociadas de un servidor vSnap o almacenamiento secundario de copia de seguridad.

Procedimiento

Para que un recurso del catálogo caduque:

1. En el panel de navegación, pulse **Gestionar protección** > **IBM Spectrum Protect Plus** > **Retención del punto de restauración**.
2. Pulse la pestaña **Máquinas virtuales/bases de datos**.
3. Utilice el filtro para buscar por el tipo de recurso y, a continuación, especifique una serie de búsqueda para buscar un recurso por el nombre. Para obtener más información sobre el uso de la función de búsqueda, consulte Apéndice A, “Directrices de búsqueda”, en la página 321.
4. Pulse el icono de búsqueda .
5. Pulse el icono de suprimir que está asociado a un recurso.
6. Para confirmar la caducidad, en el recuadro de diálogo, pulse **Sí**.

Resultados
Los metadatos del catálogo asociados al recurso se eliminan del catálogo.
Conceptos relacionados
“Tipos de trabajo” en la página 257

Los trabajos se utilizan para ejecutar operaciones de copia de seguridad, restauración, mantenimiento e inventario en IBM Spectrum Protect Plus.

Capítulo 10. Trabajos y operaciones

Utilice la ventana **Trabajos y operaciones** para supervisar trabajos, revisar el historial de trabajos, planificar trabajos, ver los recursos activos y volver a ejecutar o poner en pausa los trabajos y las planificaciones.

Para ver y gestionar trabajos y recursos, pulse **Trabajos y operaciones** y pulse en la pestaña correspondiente:

- **Trabajos en ejecución** Muestra los trabajos de copia de seguridad, inventario, mantenimiento y restauración que se están ejecutando.
- **Historial de trabajos** Muestra los trabajos que han fallado, se han completado con avisos o se han ejecutado correctamente. Puede descargar un registro de trabajo de la página seleccionando el trabajo y pulsando **Descargar.zip**.
- **Recursos activos** Muestra los recursos activos de la aplicación y el hipervisor.
- **Planificación** Muestra las planificaciones de trabajos. Puede iniciar un trabajo bajo demanda o poner en pausa una planificación para un trabajo seleccionado. Utilizando el icono de edición,  , también puede editar una planificación de trabajo.

También puede crear trabajos de restauración bajo demanda o recurrentes pulsando **Crear trabajo de restauración**. Para obtener instrucciones sobre cómo crear trabajos de restauración, pulse en los enlaces de la tabla siguiente:

Tabla 22. Creación de trabajos de restauración

Tarea	Instrucciones
Crear trabajos de restauración para hipervisores	Consulte los temas siguientes: • “Restauración de datos de VMware” en la página 116 • “Restauración de datos de Hyper-V” en la página 132
Crear trabajos de restauración para aplicaciones	Consulte los temas siguientes: • “Restauración de datos de Db2 ” en la página 155 • “Restauración de bases de datos de Microsoft Exchange ” en la página 172 • “Restauración de datos de MongoDB ” en la página 212 • “Restauración de datos de Oracle” en la página 244 • “Restauración de datos de SQL Server” en la página 233

Tipos de trabajo

Los trabajos se utilizan para ejecutar operaciones de copia de seguridad, restauración, mantenimiento e inventario en IBM Spectrum Protect Plus.

Los trabajos de copia de seguridad y restauración están definidos por el usuario. Tras crear estos trabajos, puede modificarlos en cualquier momento. Los trabajos de mantenimiento e inventario están predefinidos y no se pueden modificar.

Puede ejecutar todos los trabajos bajo demanda, incluso si se han establecido para ejecutarse en una planificación. También puede retener y liberar trabajos que están establecidos para ejecutarse en una planificación.

Están disponibles los siguientes tipos de trabajo:

Copia de seguridad
Un trabajo de copia de seguridad define los recursos de los que desea realizar una copia de seguridad y la políticas o las políticas de acuerdo de nivel de servicio (SLA) que desea aplicar a estos recursos. Cada política de SLA define cuándo se ejecuta el trabajo. Puede ejecutar el trabajo utilizando la planificación que está definida por la política de SLA o puede ejecutar el trabajo bajo demanda.

El nombre del trabajo se genera automáticamente y se construye del tipo de recurso seguido de la política de SLA que se utiliza para el trabajo. Por ejemplo, un trabajo de copia de seguridad para los recursos de SQL Server que están asociados a la política de SLA Gold es `sql_Gold`.

Restaurar
Un trabajo de restauración define el punto de restauración desde el que desea restaurar los datos. Por ejemplo, si está restaurando datos de hipervisor, el punto de restauración puede ser una máquina virtual. Si está restaurando datos de aplicación, el punto de restauración puede ser una base de datos. Puede crear una planificación para ejecutar el trabajo o puede ejecutar el trabajo bajo demanda.

El nombre del trabajo depende de si se ejecuta el trabajo bajo demanda o en una planificación. Si ejecuta una operación de restauración bajo demanda, el nombre del trabajo `onDemandRestore` se genera automáticamente.

Si se crea un trabajo para que se ejecute en una planificación, debe especificar un nombre de trabajo.

Mantenimiento
El trabajo de mantenimiento se ejecuta una vez al día para eliminar los recursos y los objetos asociados que crea IBM Spectrum Protect Plus cuando se suprime un trabajo que está en un estado pendiente.

El procedimiento de limpieza reclama el espacio en dispositivos de almacenamiento, limpia el catálogo de IBM Spectrum Protect Plus y elimina instantáneas relacionadas. El trabajo de mantenimiento también elimina datos catalogados que están asociados con trabajos suprimidos.

El nombre de trabajo es `Mantenimiento`

Inventario
Un trabajo de inventario se ejecuta automáticamente al añadir un recurso a IBM Spectrum Protect Plus. Sin embargo, puede ejecutar un trabajo de inventario en cualquier momento para detectar cualquier cambio que se haya producido desde que se añadió el recurso.

Los nombres de trabajo de inventarios son `Inventario de servidor de aplicaciones predeterminado`, `Inventario de hipervisor predeterminado` e `Inventario de servidor de almacenamiento predeterminado`.

Inicio de trabajos

Puede ejecutar cualquier trabajo bajo demanda, incluso si el trabajo se ha establecido para que se ejecute en una planificación.

Procedimiento

Complete los pasos siguientes para iniciar un trabajo:

1. En el panel de navegación, haga clic en **Trabajos y operaciones** y pulse la pestaña **Planificación**.
2. Seleccione el trabajo que desee ejecutar y pulse **Acciones** > **Iniciar**.
   El trabajo se inicia y se añade a la pestaña **Trabajos en ejecución**.

Qué hacer a continuación
Para ver el registro de trabajo en detalle, pulse el trabajo en la pestaña **Trabajos en ejecución**.

La pantalla de registro muestra los siguientes detalles:

- Estado: muestra si el mensaje es un mensaje de error, aviso o información.
- Hora: muestra la indicación de fecha y hora del mensaje.
- ID: muestra el identificador exclusivo del mensaje, si es aplicable.
- Descripción: muestra el texto del mensaje.

Puede descargar un registro de trabajo de la página pulsando **Descargar.zip**. Para cancelar el trabajo, pulse **Acciones** > **Cancelar**.

Cómo poner en pausa y reanudar trabajos

Puede poner en pausa y reanudar un trabajo planificado o un trabajo que se esté ejecutando. Cuando ponga en pausa un trabajo planificado, el trabajo no se ejecutará hasta que se reanude.

Procedimiento

Para poner en pausa y liberar planificaciones de trabajos, siga estos pasos:

1. En el panel de navegación, haga clic en **Trabajos y operaciones** y pulse la pestaña **Planificación**.
2. Seleccione el trabajo que desee poner en pausa y pulse **Acciones** > **Pausar planificación**.
3. Para reanudar la planificación de trabajos, pulse **Acciones** > **Liberar planificación**.

Cancelación de trabajos

Puede cancelar un trabajo que se esté ejecutando.

Procedimiento

Para cancelar un trabajo, realice los pasos siguientes:

1. En el panel de navegación, pulse **Trabajos y operaciones**y, a continuación, pulse la pestaña **Planificación** .
2. Para iniciar la sesión de trabajo en ejecución, pulse el menú **Acciones** que está asociado al trabajo y, a continuación, pulse **Iniciar**.

Volver a ejecutar trabajos de copia de seguridad parcialmente completados

Si la última instancia de un trabajo de copia de seguridad se ha completado parcialmente, puede volver a ejecutar el trabajo para realizar la copia de seguridad de las máquinas virtuales y las bases de datos que se han omitido.

Acerca de esta tarea

Un trabajo de copia de seguridad solo se puede volver a ejecutar en el mismo ID de sesión que el trabajo de copia de seguridad original parcialmente completado. No se puede haber completado ninguna copia de seguridad satisfactoria del mismo recurso desde el trabajo de copia de seguridad parcial que eligió volver a ejecutar.

Nota: Los trabajos de copia de seguridad se pueden volver a ejecutar únicamente como respuesta a un error de copia de seguridad del hipervisor o de la base de datos. Los siguientes sucesos no cumplen los requisitos en operaciones para volver a ejecutar un trabajo de copia de seguridad:

- Una copia de seguridad de la máquina virtual se ha completado con un error FLI.

- Se ha producido un error de condensación de instantánea para un sistema de almacenamiento.
- Un trabajo de copia de seguridad ha fallado con un problema desconocido como, por ejemplo, un error de catalogación.
- En el vCenter, falta un recurso.

En las aplicaciones en las que se admiten copias de seguridad de registro, las copias de seguridad de registro no se inhabilitan cuando se utiliza la función de volver a ejecutar. Las copias de seguridad de registro se inhabilitarán en las bases de datos aplicables la próxima vez que se inicie el trabajo sin utilizar la función de copia de seguridad o de volver a ejecutar bajo demanda.

Procedimiento

Complete los pasos siguientes para volver a ejecutar una operación de copia de seguridad completada parcialmente:

1. En el panel de navegación, pulse **Trabajos y operaciones** y, a continuación, pulse la pestaña **Historial de trabajos**.
2. Utilice la función de búsqueda y los filtros para buscar la última instancia del trabajo de copia de seguridad que se completó parcialmente.
3. Seleccione la instancia de trabajo y, a continuación, pulse **Volver a ejecutar**.

   Nota:

   Si no se puede volver a ejecutar el trabajo de copia de seguridad, la opción **Volver a ejecutar** no estará disponible.

   Todas las opciones de SLA y las exclusiones asociadas al trabajo original se incluyen en la operación de volver a ejecutar. No se aplican cambios de opción o exclusión desde que se completó la copia de seguridad parcial. Si el trabajo que se vuelve a ejecutar se completa correctamente, el resumen del trabajo se actualiza para mostrar el éxito de la operación.

Copia de seguridad de un único recurso

Si un hipervisor o un servidor de aplicaciones está asociado a una política de SLA, se puede realizar una copia de seguridad inmediata de una única máquina virtual o aplicación ejecutando una operación de copia de seguridad bajo demanda. Seleccione **Ejecutar** en una pantalla de copia de seguridad de hipervisor o de servidor de aplicaciones para ejecutar una operación de copia de seguridad bajo demanda. Esta opción se habilita cuando se asocia una política de SLA existente al recurso.

Acerca de esta tarea

Volver a ejecutar un trabajo de copia de seguridad para un único recurso solo es válido en las operaciones de copia de seguridad, no en las operaciones de réplica o descarga.

En el caso de aplicaciones cuyas copias de seguridad de registro están soportadas, las copias de seguridad de registro no se inhabilitan cuando se utiliza la función de copia de seguridad bajo demanda o de reejecución. Las copias de seguridad de registro se inhabilitarán en las bases de datos aplicables la próxima vez que se inicie el trabajo sin utilizar la función de copia de seguridad o de volver a ejecutar bajo demanda.

Procedimiento

Complete los pasos siguientes para ejecutar un trabajo de copia de seguridad bajo demanda de una única máquina virtual o un único servidor de aplicaciones:

1. En el panel de navegación, pulse **Gestionar protección**. En función del tipo de operación de copia de seguridad, seleccione **Hipervisores** > **Copia de seguridad** o **Aplicaciones** > **Copia de seguridad**.
2. Pulse una de las instancias de la lista para mostrar los recursos de la máquina virtual o de la aplicación asociados.

   El hipervisor o el servidor de aplicaciones deben estar asociados a una política de SLA existente.

3. Pulse **Ejecutar**.

   Si la máquina virtual o la aplicación es miembro de varias políticas de SLA, seleccione la política de SLA que va a ejecutar para el trabajo bajo demanda.
4. Para confirmar el trabajo de copia de seguridad, en el recuadro de diálogo, pulse **Aceptar**.

Configuración de scripts para las operaciones de copia de seguridad y restauración

Los scripts anteriores y posteriores son scripts que se pueden ejecutar antes o después de que los trabajos de copia de seguridad y restauración se ejecuten en el nivel de trabajo. Los scripts soportados incluyen scripts de shell para máquinas basadas en Linux y scripts Batch y PowerShell para máquinas basadas en Windows. Los scripts se crean localmente, se suben al entorno a través de la página **Script** y se aplican a continuación a las definiciones de trabajos.

Antes de empezar

Revise las consideraciones siguientes para utilizar scripts con hipervisores:

- El usuario que ejecuta el script debe tener el derecho a **Iniciar sesión como servicio** habilitado, que es necesario para ejecutar scripts anteriores y posteriores. Para obtener más información acerca de este derecho, consulte Añadir el inicio de sesión como servicio de derecho a una cuenta.
- Se debe habilitar el shell remoto de Windows (WinRM).

Carga de un script

Los scripts soportados incluyen scripts de shell para máquinas basadas en Linux y scripts Batch y PowerShell para máquinas basadas en Windows. Los scripts se deben crear utilizando el formato de archivo asociado correspondiente al sistema operativo.

Procedimiento

Complete los pasos siguientes para cargar un script:

1. En el panel de navegación, pulse **Configuración del sistema** > **Script**.
2. En la sección **Scripts**, pulse **Cargar script**.

   Se muestra el panel **Cargar script**.
3. Pulse **Examinar** para seleccionar un script local para cargar.
4. Pulse **Guardar**.

   El script se muestra en la tabla **Scripts** y se puede aplicar a los trabajos soportados.

Qué hacer a continuación

Después de cargar el script, realice la acción siguiente:

Acción	Cómo
Añada el script a un servidor desde el que se ejecutará.	Consulte “Adición de un script a un servidor” en la página 261.

Adición de un script a un servidor

Añada el script a un servidor desde el que se ejecutará.

Procedimiento

Complete los pasos siguientes para designar un script en un servidor:

1. En el panel de navegación, pulse **Configuración del sistema** > **Script**.
2. En la sección **Servidores de scripts**, pulse **Añadir servidor de script**.

Se muestra el panel **Propiedades del servidor de script**.

3. Establezca las opciones del servidor.

   Dirección de host

   Especifique la dirección IP que se pueda resolver o una vía de acceso y un nombre de máquina que se puedan resolver.

   Utilizar usuario existente

   Habilite esta opción para seleccionar un nombre de usuario y una contraseña especificados anteriormente para el proveedor.

   Nombre de usuario

   Escriba el nombre de usuario del proveedor. Si se accede a un servidor SQL, la identidad de usuario respeta el formato *dominio**nombre* predeterminado si la máquina virtual está conectada a un dominio. El formato *administrador_local* se utiliza si el usuario es un administrador local.

   Contraseña

   Escriba la contraseña para el proveedor.

   Tipo de SO

   Seleccione el sistema operativo del servidor de aplicaciones.

4. Pulse **Guardar**.

Capítulo 11. Configuración y mantenimiento del entorno del sistema IBM Spectrum Protect Plus

Las tareas de gestión del sistema incluyen añadir almacenamiento de copia de seguridad, gestionar sitios, registrar servidores Lightweight Directory Access Protocol (LDAP) o Simple Mail Transfer Protocol (SMTP) y gestionar claves y certificados para los recursos de la nube.

Las tareas de mantenimiento incluyen la revisión de la configuración del dispositivo virtual de IBM Spectrum Protect Plus, la recopilación de archivos de registro para resolución de problemas y la gestión de certificados de capa de sockets seguros (SSL).

En la mayoría de los casos, IBM Spectrum Protect Plus se instala en un dispositivo virtual. El dispositivo virtual contiene la aplicación y el inventario. Las tareas de mantenimiento se completan en vSphere Client, utilizando la línea de mandatos de IBM Spectrum Protect Plus o en una consola de gestión basada en web.

Las tareas de mantenimiento las completa un administrador del sistema. Un administrador del sistema es normalmente un usuario de nivel superior que ha diseñado o implementado la infraestructura vSphere y ESX, o bien un usuario con conocimientos del uso de la línea de mandatos de IBM Spectrum Protect Plus, VMware y Linux.

Las actualizaciones de infraestructura están gestionadas por las instalaciones de actualización de IBM. La consola administrativa sirve como el medio principal para actualizar las características de IBM Spectrum Protect Plus los componentes de infraestructura subyacentes, incluido el sistema operativo y el sistema de archivos. Los paquetes de actualización ZFS (Sistema de archivos Z) también se proporcionan para instancias autónomas de vSnap.

Atención: Actualice los componentes subyacentes de IBM Spectrum Protect Plus únicamente utilizando los recursos de actualización que proporcione IBM.

Gestión del almacenamiento de copia de seguridad secundario

El servidor vSnap es la ubicación de copia de seguridad primaria para las instantáneas. Todos los entornos de IBM Spectrum Protect Plus tienen al menos un servidor vSnap. Opcionalmente, puede descargar instantáneas de un servidor vSnap en un sistema de almacenamiento en la nube o en un servidor de repositorio.

Para obtener información sobre la descarga de datos de instantánea en el almacenamiento secundario, consulte “Descargar en almacenamiento de copia de seguridad secundario” en la página 6.

Gestión del almacenamiento en la nube

Puede descargar el almacenamiento en la nube para la protección de datos a largo plazo.

Adición del almacenamiento en la nube Amazon S3 como proveedor de almacenamiento de copias de seguridad

Añada almacenamiento en la nube de Amazon S3 para que IBM Spectrum Protect Plus pueda descargar datos en S3.

Antes de empezar

Configure la clave que es necesaria para el objeto en la nube. Para obtener instrucciones, consulte “Adición de una clave de acceso” en la página 274.

Asegúrese de que se han creado grupos de almacenamiento en la nube para los datos de IBM Spectrum Protect Plus antes de añadir el almacenamiento en la nube en los pasos siguientes. Para obtener información sobre cómo crear grupos, consulte Documentación de Amazon Simple Storage Service.

Procedimiento

Para añadir almacenamiento en la nube Amazon S3 como proveedor de almacenamiento de copias de seguridad, siga estos pasos:

1. En el menú de navegación, pulse **Configuración del sistema** > **Almacenamiento de copias de seguridad** > **Nube**.
2. Pulse **Añadir nube**.
3. En la lista **Proveedor**, seleccione **Amazon S3**.
4. Complete los campos en el panel **Registro de nube**:

   Nombre
   Especifique un nombre significativo para ayudar a identificar el almacenamiento en la nube.

   Región
   Seleccione el punto final regional del almacenamiento en la nube de Amazon Web Services (AWS).

   Utilizar clave existente
   Habilite esta opción para seleccionar una clave introducida previamente para el almacenamiento y, a continuación, seleccione la clave en la lista **Seleccionar una clave**.

   Si no selecciona esta opción, complete los campos siguientes para añadir una clave:

   Nombre de clave
   Especifique un nombre significativo para ayudar a identificar la clave.

   Clave de acceso
   Escriba la clave de acceso AWS. Las claves de acceso se crean a través de la consola de gestión de AWS.

   Clave secreta
   Especifique la clave secreta de AWS. Las claves secretas se crean a través de la consola de gestión de AWS.
5. Pulse **Obtener grupos** y, a continuación, seleccione un grupo que sirva de destino de la descarga.

   Una vez generados los grupos, se visualizan los campos **Descargar grupo** y **Archivar grupo**.
6. En el campo **Descargar grupo**, seleccione el grupo que desee como destino de descarga.
7. Opcional: En el campo **Archivar grupo**, seleccione el recurso de almacenamiento en la nube que desee como destino de archivado.

   El archivado de datos crea una copia de datos completa y puede proporcionar beneficios de protección, coste y seguridad a más largo plazo. Para obtener más información sobre el archivado de datos, consulte la información sobre la copia de datos en un almacenamiento de archivado de nube en "Descargar en almacenamiento de copia de seguridad secundario" en la página 6.
8. Pulse **Registrar**.

   El almacenamiento en la nube se añade a la tabla de servidores de nube.

Qué hacer a continuación
Después de añadir el almacenamiento S3, realice la acción siguiente:

Acción	Cómo
Asocie el almacenamiento en la nube con la política de SLA que se utiliza para el trabajo de copia de seguridad.	Para crear una política de SLA, consulte "Creación de una política de SLA" en la página 93. Para modificar una política de SLA existente, consulte "Edición de una política de SLA" en la página 97.

Adición de IBM Cloud Object Storage como proveedor de almacenamiento de copias de seguridad
Añada IBM Cloud Object Storage para habilitar IBM Spectrum Protect Plus para descargar datos a IBM Cloud.

Antes de empezar

Configure la clave y el certificado que son necesarios para el objeto en la nube. Para obtener instrucciones, consulte "Adición de una clave de acceso" en la página 274 y "Adición de un certificado" en la página 275.

Asegúrese de que se han creado grupos de almacenamiento en la nube para los datos de IBM Spectrum Protect Plus antes de añadir el almacenamiento en la nube en los pasos siguientes. Para obtener información sobre cómo crear grupos, consulte Acerca de IBM Cloud Object Storage.

Procedimiento

Para añadir IBM Cloud Object Storage como proveedor de almacenamiento de copias de seguridad, siga estos pasos:

1. En el menú de navegación, pulse **Configuración del sistema** > **Almacenamiento de copias de seguridad** > **Nube**.
2. Pulse **Añadir nube**.
3. En la lista **Proveedor**, seleccione **IBM Cloud Object Storage**.
4. Complete los campos en el panel **Registro de nube**:

   Nombre
   Especifique un nombre significativo para ayudar a identificar el almacenamiento en la nube.

   Punto final
   Seleccione el punto final del almacenamiento en la nube.

   Utilizar clave existente
   Habilite esta opción para seleccionar una clave introducida previamente para el almacenamiento y, a continuación, seleccione la clave en la lista **Seleccionar una clave**.

   Si no selecciona esta opción, complete los campos siguientes para añadir una clave:

   Nombre de clave
   Especifique un nombre significativo para ayudar a identificar la clave.

   Clave de acceso
   Escriba la clave de acceso.

   Clave secreta
   Escriba la clave secreta.

   Certificado
   Seleccione un método de asociación de un certificado al recurso:

   Cargar
   Seleccione y pulse **Examinar** para localizar el certificado y, a continuación, pulse **Cargar**.

   Copiar y pegar
   Seleccione esta opción para especificar el nombre del certificado, copiar y pegar su contenido y, a continuación, pulse **Crear**.

   Utilizar existente
   Seleccione esta opción para utilizar un certificado cargado previamente.

   No es necesario un certificado si está añadiendo almacenamiento público de IBM Cloud Object Storage.
5. Pulse **Obtener grupos** y, a continuación, seleccione un grupo que sirva de destino de la descarga.
   Una vez generados los grupos, se visualizan los campos **Descargar grupo** y **Archivar grupo**.
6. En el campo **Descargar grupo**, seleccione el grupo que desee como destino de descarga.
7. Opcional: En el campo **Archivar grupo**, seleccione el recurso de almacenamiento en la nube que desee como destino de archivado.

   El archivado de datos crea una copia de datos completa y puede proporcionar beneficios de protección, coste y seguridad a más largo plazo. Para obtener más información sobre el archivado de

datos, consulte la información sobre la copia de datos en un almacenamiento de archivado de nube en "Descargar en almacenamiento de copia de seguridad secundario" en la página 6.

8. Pulse **Registrar**.

   El almacenamiento en la nube se añade a la tabla de servidores de nube.

Qué hacer a continuación

Después de añadir IBM Cloud Object Storage, realice la acción siguiente:

Acción	Cómo
Asocie el almacenamiento en la nube con la política de SLA que se utiliza para el trabajo de copia de seguridad.	Para crear una política de SLA, consulte "Creación de una política de SLA" en la página 93. Para modificar una política de SLA existente, consulte "Edición de una política de SLA" en la página 97.

Adición del almacenamiento en la nube de Microsoft Azure como proveedor de almacenamiento de copias de seguridad

Añada un almacenamiento en la nube de Microsoft Azure para que IBM Spectrum Protect Plus pueda descargar datos en el almacenamiento en la nube de Microsoft Azure Blob.

Antes de empezar

Asegúrese de que se han creado grupos de almacenamiento en la nube para los datos de IBM Spectrum Protect Plus antes de añadir el almacenamiento en la nube en los pasos siguientes. Para obtener información sobre cómo crear cubos, consulte la documentación de Azure.

Procedimiento

Para añadir almacenamiento en la nube de Microsoft Azure como proveedor de almacenamiento de copias de seguridad, siga estos pasos:

1. En el panel de navegación, pulse **Configuración del sistema** > **Almacenamiento de copias de seguridad** > **Nube**.
2. Pulse **Añadir nube**.
3. En la lista **Proveedor**, seleccione **Almacenamiento de Microsoft Blob Azure**.
4. Complete los campos en el panel **Registro de nube**:

   Nombre
   Especifique un nombre significativo para ayudar a identificar el almacenamiento en la nube.

   Punto final
   Seleccione el punto final del almacenamiento en la nube.

   Utilizar clave existente
   Habilite esta opción para seleccionar una clave introducida previamente para el almacenamiento y, a continuación, seleccione la clave en la lista **Seleccionar una clave**.

   Si no selecciona esta opción, complete los campos siguientes para añadir una clave:

   Nombre de clave
   Especifique un nombre significativo para ayudar a identificar la clave.

   Nombre de cuenta de almacenamiento
   Especifique el nombre de cuenta de almacenamiento de acceso de Microsoft Azure. Es la opción Azure Management Portal.

   Clave compartida de la cuenta de almacenamiento
   Escriba la clave de Microsoft Azure desde una cualquiera de los campos de clave del Portal de administración de Azure, clave1 o clave2.
5. Pulse **Obtener grupos** y, a continuación, seleccione un grupo que sirva de destino de la descarga.

Una vez generados los grupos, se visualizan los campos **Descargar grupo** y **Archivar grupo**.

6. En el campo **Descargar grupo**, seleccione el grupo que desee como destino de descarga.
7. Opcional: En el campo **Archivar grupo**, seleccione el recurso de almacenamiento en la nube que desee como destino de archivado.

   El archivado de datos crea una copia de datos completa y puede proporcionar beneficios de protección, coste y seguridad a más largo plazo. Para obtener más información sobre el archivado de datos, consulte la información sobre la copia de datos en un almacenamiento de archivado de nube en "Descargar en almacenamiento de copia de seguridad secundario" en la página 6.
8. Pulse **Registrar**.

   El almacenamiento en la nube se añade a la tabla de servidores de nube.

Qué hacer a continuación

Después de añadir el almacenamiento de Microsoft Azure, realice la acción siguiente:

Acción	Cómo
Asocie el almacenamiento en la nube con la política de SLA que se utiliza para el trabajo de copia de seguridad.	Para crear una política de SLA, consulte "Creación de una política de SLA" en la página 93. Para modificar una política de SLA existente, consulte "Edición de una política de SLA" en la página 97.

Edición de valores para el almacenamiento en la nube

Edite los valores de un proveedor de almacenamiento en la nube para que refleje los cambios en el entorno de la nube.

Procedimiento

Para editar un proveedor de almacenamiento en la nube, complete los pasos siguientes:

1. En el menú de navegación, pulse **Configuración del sistema** > **Almacenamiento de copias de seguridad** > **Nube**.
2. Pulse el icono de edición que está asociado a un proveedor de nube.

   Se visualiza el panel **Actualizar nube**.
3. Revise los valores del proveedor de nube, y a continuación, pulse **Guardar**.

Supresión de almacenamiento en la nube

Suprima un proveedor de almacenamiento en la nube para que refleje los cambios en el entorno de nube. Asegúrese de que el proveedor no está asociado a ninguna política de SLA antes de suprimirlo.

Procedimiento

Para suprimir un proveedor de almacenamiento en la nube, complete los pasos siguientes:

1. En el menú de navegación, pulse **Configuración del sistema** > **Almacenamiento de copias de seguridad** > **Nube**.
2. Pulse el icono de suprimir que está asociado a un proveedor.
3. Pulse **Sí** para suprimir el proveedor.

Gestión del almacenamiento del servidor de repositorio

Puede descargar en un servidor de repositorio para la protección de datos a largo plazo. Para el release actual de IBM Spectrum Protect Plus, el servidor de repositorio debe ser un servidor IBM Spectrum Protect Versión 8.1.7 o posterior. Para el archivado en cinta, se requiere servidor IBM Spectrum Protect Version 8.1.8 o posterior.

Configuración de un servidor IBM Spectrum Protect como destino de descarga
Para descargar datos en un servidor IBM Spectrum Protect, primero debe configurar IBM Spectrum Protect Plus como un cliente objeto en el servidor.

Acerca de esta tarea

Después de configurar un cliente objeto, se proporcionan claves y un certificado para habilitar una conexión segura con el servidor IBM Spectrum Protect. Estos elementos son necesarios para añadir el servidor de repositorio en IBM Spectrum Protect Plus.

Para añadir el cliente objeto, debe estar familiarizado con el entorno de servidor IBM Spectrum Protect y tener experiencia trabajando con el Centro de operaciones o con los mandatos administrativos de servidor IBM Spectrum Protect . Para obtener ayuda, póngase en contacto con el administrador de IBM Spectrum Protect .

IBM Spectrum Protect Plus tiene en cuenta las descargas en servidor IBM Spectrum Protect, pero no tiene en cuentas posteriores operaciones de réplica de servidor IBM Spectrum Protect.

Puede encontrar documentación sobre cómo configurar IBM Spectrum Protect como un destino de descarga en el IBM Knowledge Center como se especifica a continuación:

- Para obtener una descripción general del proceso de configuración, consulte Descarga de datos de IBM Spectrum Protect Plus
- Para conocer los requisitos previos para el proceso de descarga, consulte Preparación para la descarga de datos de IBM Spectrum Protect Plus
- Para obtener información sobre el sistema operativo AIX, consulte Configuración para descargar datos en entornos de AIX®
- Para obtener información sobre los sistemas operativos Linux o Windows, consulte Configuración para descargar datos en entornos de Linux o Windows

Tareas relacionadas

“Adición de un servidor de repositorio como proveedor de almacenamiento de copias de seguridad” en la página 272
Añada un servidor de repositorio para habilitar IBM Spectrum Protect Plus para descargar datos en el servidor.

Preparación para la descarga de datos de IBM Spectrum Protect Plus
Antes de descargar datos de IBM Spectrum Protect Plus a IBM Spectrum Protect, complete los pasos de preparación en el entorno de IBM Spectrum Protect.

Procedimiento

1. Verifique si puede abrir un puerto del servidor IBM Spectrum Protect en el cliente objeto de IBM Spectrum Protect Plus que tiene previsto utilizar en las operaciones de descarga de datos. El número de puerto predeterminado es 9000. Si hay algún cortafuegos entre el cliente objeto y el agente objeto, configure el agente objeto para acceder al puerto adecuado a través del cortafuegos.
2. Verifique los valores del dominio de políticas que tiene previsto utilizar en las operaciones de descarga de datos. Un nodo de cliente objeto se asocia a este dominio de políticas cuando el nodo se registra o se actualiza utilizando los mandatos administrativos del servidor IBM Spectrum Protect **REGISTER NODE** o **UPDATE NODE**.

   Las consideraciones para especificar los dominios de políticas de las operaciones de descarga de IBM Spectrum Protect Plus incluyen entre otras, las siguientes:

   - El dominio al que se asigna el nodo debe tener un grupo de copias de seguridad. Los objetos que se almacenan en un nodo de cliente objeto son siempre objetos de copia de seguridad. No se necesita un grupo de copias archivadas.
   - Debe utilizar una agrupación de almacenamiento de contenedores. La agrupación de almacenamiento que se especifica en el grupo de copias `Copy Destination` debe ser una agrupación de almacenamiento de contenedores de directorio o de contenedores de nube.

- Todos los objetos se nombran de forma exclusiva. No hay versiones inactivas de objetos; por lo tanto, puede establecer el campo `Versions Data Exists` en 1.
- Los grupos de copias de seguridad solo contienen versiones activas; por lo tanto, puede establecer los campos `Retain Extra Versions` y `Retain Only Version` en el valor 0.
- El servidor IBM Spectrum Protect controla la hora a la que se suprimen los objetos. Asegúrese de que el nodo de cliente objeto esté habilitado para permitir la supresión del grupo de copias de seguridad.

Ejemplo: visualizar información detallada sobre un dominio de políticas en una operación de descarga de IBM Spectrum Protect Plus

Valores de visualización para un grupo de copias para un nodo de cliente objeto.

```
query copygroup format=detailed
```

```
                Policy Domain Name: TAPSRV03_OBJECT
                   Policy Set Name: SET1
                   Mgmt Class Name: BACK_DISK
                   Copy Group Name: STANDARD
                   Copy Group Type: Backup
              Versions Data Exists: 1
             Versions Data Deleted: 0
             Retain Extra Versions: 0
               Retain Only Version: 0
                         Copy Mode: Modified
                Copy Serialization: Shared Static
                    Copy Frequency: 0
                  Copy Destination: DEDUPPOOL
Table of Contents (TOC) Destination:
     Last Update by (administrator): JBASIL
              Last Update Date/Time: 01/17/2019 14:38:05
                   Managing profile:
                    Changes Pending: No
```

Descarga de datos en sistemas AIX

Puede descargar datos de IBM Spectrum Protect Plus en un servidor IBM Spectrum Protect en AIX.

Acerca de esta tarea

Un agente objeto de IBM Spectrum Protect no se puede ejecutar directamente en un sistema operativo de IBM AIX. Sin embargo, puede descargar datos de IBM Spectrum Protect Plus a un cliente objeto de IBM Spectrum Protect en un sistema AIX configurando primero un agente objeto en un sistema operativo Linux x86_64. El agente objeto autónomo solo está disponible en el sistema operativo Linux x86_64.

Después de que el cliente objeto de IBM Spectrum Protect Plus envíe datos al agente objeto de IBM Spectrum Protect en Linux x86_64, el agente objeto transfiere datos a un cliente objeto de IBM Spectrum Protect en AIX.

Procedimiento

Para descargar datos de IBM Spectrum Protect Plus a un servidor IBM Spectrum Protect en AIX, complete los pasos siguientes:

1. En el servidor AIX, emita el siguiente mandato de administración del servidor IBM Spectrum Protect:

   ```
   setopt EnableAIXS3Interface Yes
   ```

2. En el servidor AIX, defina un agente objeto emitiendo el siguiente mandato administrativo del servidor IBM Spectrum Protect. Para establecer la dirección de alto nivel (HLA) y la dirección de bajo nivel (LLA), utilice la dirección IP del sistema host y el puerto que el agente objeto va a utilizar.

   ```
   define server nombre_agente_objeto
   hla=dirección_ip_sistema_host_agente_objeto
   lla=puerto_agente_objeto objectagent=yes
   ```

Consejo: El valor predeterminado del puerto del agente objeto es 9000. Si un agente objeto local ya se está ejecutando en el sistema, el agente objeto que se está configurando para el servidor AIX debe utilizar un número de puerto distinto del agente objeto existente.

3. Descargue los scripts siguientes en el sistema host del agente objeto:
   - ftp://public.dhe.ibm.com/storage/tivoli-storage-management/maintenance/objectagent/v8r1/Linux/8.1.7.000/x86_64/spObjectAgent
   - ftp://public.dhe.ibm.com/storage/tivoli-storage-management/maintenance/objectagent/v8r1/Linux/8.1.7.000/x86_64/startObjectAgent.sh
   - ftp://public.dhe.ibm.com/storage/tivoli-storage-management/maintenance/objectagent/v8r1/Linux/8.1.7.000/x86_64/spObjectAgent.rc
   - ftp://public.dhe.ibm.com/storage/tivoli-storage-management/maintenance/objectagent/v8r1/Linux/8.1.7.000/x86_64/spObjectAgent.rc.u
   - ftp://public.dhe.ibm.com/storage/tivoli-storage-management/maintenance/objectagent/v8r1/Linux/8.1.7.000/x86_64/delObjectAgentSvc.sh

   Se puede instalar IBM Spectrum Protect Plus o un servidor IBM Spectrum Protect en el sistema host del agente objeto.

   Si se instala el servidor IBM Spectrum Protect, puede utilizar el archivo `spObjectAgent` en el directorio del servidor y no tiene que volver a descargar el agente y sus scripts.
4. Asegúrese de que los archivos siguientes tienen permisos ejecutables:
   - `spObjectAgent`
   - `startObjectAgent.sh`
   - `spObjectAgent.rc`
   - `spObjectAgent.rc.u`
   - `delObjectAgentSvc.sh`
5. Desde el sistema de servidor AIX, copie los dos elementos siguientes en un directorio del sistema host del agente objeto en Linux:
   - Directorio del servidor de agentes objeto
   - Certificado público de servidor

   El directorio del servidor de agentes objeto se ha creado al ejecutar el mandato **DEFINE SERVER**. El directorio incluye el archivo y los certificados siguientes:
   - Un archivo de configuración para crear e iniciar un servicio de agente objeto
   - Certificados para la comunicación entre el agente objeto y el servidor

   El directorio de servidores de agentes objeto se crea en el directorio de instancia de servidor: /*dir_inicio_instancia_servidor*/*nombre_agente_objeto*. Por ejemplo,

   `/home/tsminst1/OBJAGENT1`

   El certificado público del servidor (`cert256.arm`) se encuentra normalmente en el directorio de instancia de servidor.
6. En el directorio de servidores de agentes objeto que copió en el paso anterior, localice el archivo de configuración del agente objeto (`spObjectAgent_`*`nombre_objeto_puertoservidor`*`.config`).

   Por ejemplo: `spObjectAgent_OBJAGENT1_1500.config`

   En el archivo de configuración, actualice las ubicaciones de los siguientes archivos. Por ejemplo:

```
objagentexe=\"/opt/tivoli/tsm/server/bin/spObjectAgent\"
   keystore="/home/tsminst1/OBJAGENT1/agentcert.p12"
   pwdfile="/home/tsminst1/OBJAGENT1/agentcert.pwd"
   serverkeypub="/home/tsminst1/OBJAGENT1/cert256.arm"
   agentconfig=\"/home/tsminst1/OBJAGENT1/spObjectAgent_OBJAGENT1_1500.config\"
```

7. Altere temporalmente el parámetro **SERVERHLA** en el archivo de configuración del agente objeto utilizando la dirección IP del servidor AIX:

   ```
   serverhla=dirección_ip_servidor_aix
   ```

   Consejo: El agente objeto utiliza este valor para localizar el servidor IBM Spectrum Protect.
8. Para crear e iniciar el agente objeto en el sistema host, ejecute el script `startObjectAgent.sh` con el archivo de configuración:

   ```
   startObjectAgent.sh spObjectAgent_nombreagenteobjeto_puertoservidor.config
   ```
9. Registre un cliente de agente objeto en el servidor AIX emitiendo el siguiente mandato de servidor IBM Spectrum Protect:

   ```
   register node nombrenodo type=objectclient
   ```

   Importante: Registre el ID de usuario y la contraseña de inicio de sesión que se generan automáticamente. Necesitará las credenciales para conectarse al agente objeto.
10. Para conectar el cliente objeto de IBM Spectrum Protect Plus con el agente objeto, vaya a la documentación en línea de IBM Spectrum Protect Plus y siga las instrucciones de Adición de un servidor de repositorio como proveedor de almacenamientos de copia de seguridad.

Descarga de datos en los sistemas Linux y Windows

Puede descargar datos de IBM Spectrum Protect Plus a un servidor IBM Spectrum Protect en Linux o Windows.

Procedimiento

Para descargar datos de IBM Spectrum Protect Plus a un servidor IBM Spectrum Protect en Linux o Windows, complete los pasos siguientes:

1. Configure un agente objeto.
   a) En la barra de menús del Centro de operaciones, pulse **Servidores**.
   b) Seleccione una fila de un servidor y pulse **Detalles**.
   c) Seleccione **agente objeto** en el panel de navegación de la izquierda y complete los pasos para crear un agente objeto e iniciar un servicio de agente objeto. Para autenticarse en el agente objeto, utilice el certificado que se genera.

   Consejo: O bien, utilice el mandato administrativo de servidor IBM Spectrum Protect: **DEFINE SERVER** para crear un agente objeto. Especifique OBJECTAGENT=YES. Complete la configuración iniciando un servicio de agente objeto en el sistema que aloja el servidor IBM Spectrum Protect.
2. Configure un cliente objeto.

   Consejo: Si crea un cliente objeto antes de crear el agente objeto correspondiente, el asistente Añadir cliente fuerza la creación del agente objeto.

   a) En la barra de menús del Centro de operaciones, pulse **Clientes**.
   b) En la tabla Clientes, pulse **+ Cliente**.
   c) Seleccione Cliente objeto y siga las instrucciones del asistente **Añadir cliente**.

   Cuando complete el asistente, éste le proporcionará el punto final para comunicarse con el agente objeto en el servidor, así como el ID de la clave de acceso y la clave de acceso secreta para conectarse de forma segura. Cuando IBM Spectrum Protect Plus se utiliza como un cliente objeto, debe dirigir sus solicitudes al punto final y debe utilizar el ID de clave de acceso y la clave de acceso secreta.

   Consejo: O bien, utilice el mandato **REGISTER NODE** para crear un cliente objeto. Especifique TYPE=OBJECTCLIENT.

Supresión de un servicio de agente objeto
Cuando se suprime un agente objeto del servidor IBM Spectrum Protect, el servicio del agente objeto se debe suprimir del sistema host. Para completar el proceso de supresión de un agente objeto, suprima el servicio correspondiente.

Antes de empezar

Para suprimir el servicio de agente objeto en un sistema operativo Linux, debe ejecutar el script `delObjectAgentSvc.sh` con el archivo de configuración del agente objeto. Asegúrese de que puede iniciar la sesión en el host de agente objeto con el ID de usuario root.

Para suprimir el servicio de agente objeto en un sistema operativo Windows, debe ejecutar el archivo de proceso por lotes `delObjectAgentSvc.cmd` con el archivo de configuración del agente objeto. Asegúrese de que dispone de privilegios de administrador de Windows para iniciar la sesión en el sistema host del agente objeto.

Procedimiento

1. Verifique si el agente objeto se ha suprimido del servidor IBM Spectrum Protect emitiendo el mandato administrativo del servidor **QUERY SERVER**.
2. Abra una línea de mandatos.
3. Emita el siguiente mandato en una línea. Los directorios de servidor predeterminados se utilizan en los ejemplos.

   Linux

   ```
   /opt/tivoli/tsm/server/bin/delObjectAgentSvc.sh
   /vía_acceso_config_agente_objeto/spObjectAgent_nombreagenteobjeto_puerto_servidor.config
   ```

   Windows

   ```
   "C:\Program Files\Tivoli\TSM\server\delObjectAgentSvc.cmd"
   "vía_acceso_config_agente_objeto\spObjectAgent_nombreagenteobjeto_puerto_servidor.config"
   ```

   donde

   vía_acceso_config_agente_objeto

   Especifica la vía de acceso de configuración del agente objeto.

   nombreagenteobjeto

   Especifica el nombre del agente objeto.

   puerto_servidor

   Especifica el número de puerto del servidor IBM Spectrum Protect.

Adición de un servidor de repositorio como proveedor de almacenamiento de copias de seguridad
Añada un servidor de repositorio para habilitar IBM Spectrum Protect Plus para descargar datos en el servidor.

Antes de empezar

Configure la clave y el certificado que son necesarios para el repositorio en la nube. Para obtener instrucciones, consulte “Adición de una clave de acceso” en la página 274 y “Adición de un certificado” en la página 275.

Para el release actual de IBM Spectrum Protect Plus, el servidor de repositorio debe ser un servidor IBM Spectrum Protect.

Configure IBM Spectrum Protect Plus como un cliente objeto en el servidor de IBM Spectrum Protect. El nodo de cliente objeto transfiere y almacena los datos descargados. Después de completar el

procedimiento de configuración, el asistente le proporciona el punto final para comunicarse con el agente objeto en el servidor, y el ID de acceso, la clave secreta y el certificado para conectarse de forma segura. "Configuración de un servidor IBM Spectrum Protect como destino de descarga" en la página 268.

Los certificados se pueden obtener en el Centro de operaciones del servidor IBM Spectrum Protect desplazándose hasta el siguiente panel: **Servidor** > **Agente objeto** > **Certificado de agente**. Como alternativa, el certificado se puede obtener del dispositivo IBM Spectrum Protect Plus ejecutando el mandato siguiente: `openssl s_client -showcerts -connect <ip-address>:9000 </dev/null 2>/dev/null | openssl x509`

Los valores de retención de descarga se controlan por completo mediante políticas de SLA asociadas en IBM Spectrum Protect Plus. Los valores de retención del grupo de copias del servidor IBM Spectrum Protect no se utilizan en operaciones de descarga.

Procedimiento

Para añadir un servidor IBM Spectrum Protect como proveedor de almacenamiento de copias de seguridad, complete los pasos siguientes:

1. En el menú de navegación, pulse **Configuración del sistema** > **Almacenamiento de copias de seguridad** > **Servidor de repositorio**.
2. Pulse **Añadir servidor de repositorio**.
3. Complete los campos en el panel **Registrar servidor de repositorio** :

   Nombre
   Especifique un nombre significativo para ayudar a identificar el servidor de repositorio.

   Nombre de host
   Especifique la dirección de alto nivel (HLA) del agente de objetos del servidor de repositorio. Ejecutando el mandato IBM Spectrum Protect `q serv OBJAGENT f=d` se recupera esta información.

   Puerto
   Especifique el puerto de comunicaciones del servidor de repositorio.

   Utilizar clave existente
   Habilite esta opción para seleccionar una clave introducida previamente para el repositorio y, a continuación, seleccione la clave en la lista **Seleccionar una clave**.

   Si no selecciona esta opción, complete los campos siguientes para añadir una clave:

   Nombre de clave
   Especifique un nombre significativo para ayudar a identificar la clave.

   Clave de acceso
   Escriba la clave de acceso.

   Clave secreta
   Escriba la clave secreta.

   Certificado
   Seleccione un método para asociar un certificado con el recurso. Si se copia el certificado, se deben incluir las líneas de texto BEGIN y END.

   Cargar
   Seleccione y pulse **Examinar** para localizar el certificado y, a continuación, pulse **Cargar**.

   Copiar y pegar
   Seleccione esta opción para especificar el nombre del certificado, copiar y pegar su contenido y, a continuación, pulse **Crear**.

   Utilizar existente
   Seleccione esta opción para utilizar un certificado cargado previamente.
4. Pulse **Registrar**.

   El servidor de IBM Spectrum Protect se añade a la tabla de servidores de repositorio.

Qué hacer a continuación
Después de añadir un servidor de repositorio, realice la acción siguiente:

Acción	Cómo
Asocie el servidor de repositorio con la política de SLA que se utiliza para el trabajo de copia de seguridad.	Para crear una política de SLA, consulte "Creación de una política de SLA" en la página 93. Para modificar una política de SLA existente, consulte "Edición de una política de SLA" en la página 97.

Edición de valores para un servidor de repositorio

Edite los valores para un proveedor de servidores de repositorio para que refleje los cambios en el entorno de nube.

Procedimiento

Para editar un proveedor de servidores de repositorio, complete los pasos siguientes:

1. En el menú de navegación, pulse **Configuración del sistema** > **Almacenamiento de copias de seguridad** > **Servidor de repositorio**.
2. Pulse el icono de edición que está asociado a un proveedor de servidores de repositorio.
   Se muestra el panel **Actualizar servidor de repositorio**.
3. Revise los valores del proveedor del servidor de repositorio y, a continuación, pulse **Actualizar**.

Supresión de un servidor de repositorio

Suprima un proveedor de servidores de repositorio para que refleje los cambios en el entorno. Asegúrese de que el proveedor no está asociado a ninguna política de SLA antes de suprimirlo.

Procedimiento

Para suprimir un proveedor de servidores de repositorio, complete los pasos siguientes:

1. En el menú de navegación, pulse **Configuración del sistema** > **Almacenamiento de copias de seguridad** > **Servidor de repositorio**.
2. Pulse el icono de suprimir que está asociado a un proveedor de servidores de repositorio.
3. Pulse **Sí** para suprimir el proveedor.

Gestión de claves y certificados

Los recursos en la nube y los servidores de repositorio requieren credenciales que sirvan como destinos de descarga. Las claves de acceso y las claves secretas las proporciona el recurso en la nube o la interfaz del servidor de repositorio. Estas claves sirven como nombre de usuario y contraseña de los destinos de descarga y permiten que IBM Spectrum Protect Plus acceda a ellos. Algunos destinos de descarga también requieren certificados para la seguridad de datos adicional.

Al utilizar un recurso en IBM Spectrum Protect Plus que requiere credenciales para acceder a un destino de descarga, seleccione **Utilizar clave existente** o **Utilizar certificado existente** y seleccione la clave o el certificado asociados.

Adición de una clave de acceso

Añada una clave de acceso para proporcionar credenciales de un recurso de nube o de servidor de repositorio.

Procedimiento

Para añadir una clave, complete los pasos siguientes:

1. Cree la clave de acceso y la clave secreta a través de la interfaz del recurso de nube o del servidor de repositorio. Anote la clave de acceso y la clave secreta.

2. En el menú de navegación, pulse **Configuración del sistema** > **Claves y certificados**.
3. En la sección **Claves de acceso**, pulse **Añadir clave de acceso**.
4. Complete los campos en el panel **Propiedades de clave**:

   Nombre

   Especifique un nombre significativo para ayudar a identificar la clave de acceso.

   Clave de acceso

   Escriba la clave de acceso del recurso de nube o del servidor de repositorio. En el caso de Microsoft Azure, especifique el nombre de la cuenta de almacenamiento.

   Clave secreta

   Escriba la clave secreta del recurso de nube o del servidor de repositorio. En el caso de Microsoft Azure, especifique la clave desde uno de los campos de la clave, clave1 o clave2.
5. Pulse **Guardar**.

   La clave se muestra en la tabla **Claves de acceso** y se puede seleccionar cuando se utiliza una característica que requiere credenciales para acceder a un recurso mediante la opción **Utilizar clave existente**.

Supresión de una clave de acceso

Suprima una política de acceso cuando esté obsoleta. Asegúrese de volver a asignar una nueva clave de acceso al recurso de nube o al servidor de repositorio.

Procedimiento

Para suprimir una clave de acceso, complete los pasos siguientes:

1. En el menú de navegación, pulse **Configuración del sistema** > **Claves y certificados**.
2. Pulse el icono de suprimir  que está asociado a una clave de acceso.
3. Pulse **Sí** para suprimir la clave de acceso.

Adición de un certificado

Añada un certificado para proporcionar credenciales de un recurso de nube o de servidor de repositorio

Procedimiento

Para añadir un certificado, complete los pasos siguientes:

1. Exporte un certificado desde el recurso de nube o el servidor de repositorio.
2. En el menú de navegación, pulse **Configuración del sistema** > **Claves y certificados**.
3. En la sección **Certificados**, pulse **Añadir certificado**.
4. Complete los campos en el panel **Propiedades de certificado**:

   Tipo

   Seleccione el tipo de recurso de nube o de servidor de repositorio.

   Certificado

   Seleccione un método para añadir el certificado:

   Cargar
   Seleccione esta opción para buscar el certificado localmente.

   Copiar y pegar
   Seleccione esta opción para escribir el nombre del certificado, y copiar y pegar su contenido.
5. Pulse **Guardar**.

   La clave se muestra en la tabla **Certificados** y se puede seleccionar cuando se utiliza una característica que requiera credenciales para acceder a un recurso mediante la opción **Utilizar certificado existente**.

Supresión de un certificado

Suprima un certificado cuando esté obsoleto. Asegúrese de volver a asignar un nuevo certificado al recurso de nube o al servidor de repositorio.

Procedimiento

Para suprimir un certificado, siga los pasos siguientes:

1. En el menú de navegación, pulse **Configuración del sistema** > **Claves y certificados**.
2. Pulse el icono de suprimir que está asociado a un certificado.
3. Pulse **Sí** para suprimir el certificado.

Adición de una clave SSH

Añada una clave SSH para suministrar credenciales para los recursos basados en Linux, incluidas las operaciones de restauración e indexación de archivos en vCenter y Hyper-V, así como los servidores de aplicaciones Oracle, Db2 y MongoDB. Las claves SSH proporcionan una conexión segura entre los recursos e IBM Spectrum Protect Plus.

Antes de empezar

- El servicio SSH debe estar en ejecución en el puerto 22 en el servidor y debe configurarse algún cortafuegos para que IBM Spectrum Protect Plus se pueda conectar mediante SSH. El subsistema SFTP para SSH también debe estar habilitado.
- Asegúrese de que la clave SSH pública está en el archivo authorized_keys adecuado para el usuario agente de IBM Spectrum Protect Plus. Normalmente, el archivo se encuentra en /home/<username>/.ssh/authorized_keys. El directorio .ssh y todos los archivos que contiene deben tener sus permisos establecidos en 600.

Procedimiento

Para añadir una clave, complete los pasos siguientes:

1. En el recurso, genere una clave SSH. Por ejemplo, en un servidor de Oracle, especifique el mandato `ssh-keygen` y siga las instrucciones.
2. Cuando aparezca el mensaje de solicitud `Enter file in which to save the key` (Especificar el archivo en el que se va a guardar la clave), especifique un archivo y una ubicación; por ejemplo: `/root/sshkey`.
3. En la ubicación/directorio root del servidor especificado en el paso 2, el archivo `sshkey.pub` contiene la clave pública. Posteriormente se copiará, se pegará y se guardará en el archivo `authorized_keys` después de ejecutar `cd ~/.ssh` mientras se inicia la sesión como el usuario asignado a IBM Spectrum Protect Plus
4. En el panel de navegación de IBM Spectrum Protect Plus, pulse **Configuración del sistema** > **Claves y certificados**.
5. En la sección **Claves de acceso**, pulse **Añadir clave SSH**.
6. Complete los campos en el panel **Propiedades de clave SSH**:

   Nombre

   Escriba un nombre significativo para ayudar a identificar la clave SSH.

   Usuario

   Escriba el usuario asociado al recurso y la clave SSH.

   Clave privada

   Copie y pegue la clave privada, que se encuentra en el archivo sshkey.
7. Pulse **Guardar**.

   La clave se muestra en la tabla **Claves SSH** y se puede seleccionar cuando se selecciona una característica que requiere credenciales para acceder a un recurso mediante la opción **Clave**.

Supresión de una clave SSH

Suprima una clave SSH cuando esté obsoleta. Asegúrese de volver a asignar una nueva clave SSH a los recursos.

Procedimiento

Para suprimir una clave SSH, complete los pasos siguientes:

1. En el menú de navegación, pulse **Configuración del sistema** > **Claves y certificados**.
2. Pulse el icono de suprimir que está asociado a una clave SSH.
3. Pulse **Sí** para suprimir la clave de acceso.

Gestión de sitios

Un *sitio* es una construcción de política de IBM Spectrum Protect Plus que se utiliza para gestionar la ubicación de datos en un entorno.

Un sitio puede ser físico, por ejemplo, un centro de datos; o lógico, por ejemplo, un departamento o una organización. Los componentes de IBM Spectrum Protect Plus se asignan a los sitios para localizar y optimizar las vías de acceso de datos. Un despliegue de IBM Spectrum Protect Plus siempre tiene al menos un sitio por ubicación física.

De forma predeterminada, el entorno de IBM Spectrum Protect Plus tiene un sitio primario, un sitio secundario y un sitio de demostración.

Adición de un sitio

Después de añadir un sitio a IBM Spectrum Protect Plus, puede asignar servidores de almacenamiento de copias de seguridad al sitio.

Procedimiento

Para añadir un sitio, complete los pasos siguientes:

1. En el panel de navegación, pulse **Configuración del sistema** > **Sitio**.
2. Pulse **Añadir sitio**.

   Se muestra el panel **Propiedades del sitio**.
3. Especifique un nombre de sitio.
4. Opcional: Para gestionar la actividad de red en una planificación definida, cambie el rendimiento de las operaciones de descarga y réplica de sitios:
   a) Seleccione el recuadro de selección **Habilitar regulador**.
   b) En el campo **Índice**, ajuste el rendimiento:
      1) Cambie el índice de rendimiento numérico pulsando las flechas arriba o abajo.
      2) Seleccione una unidad para el rendimiento. Las opciones son **bytes/s**, **KB/s**, **MB/s** y **GB/s**.

   El rendimiento predeterminado es 100 MB/s (megabytes por segundo).

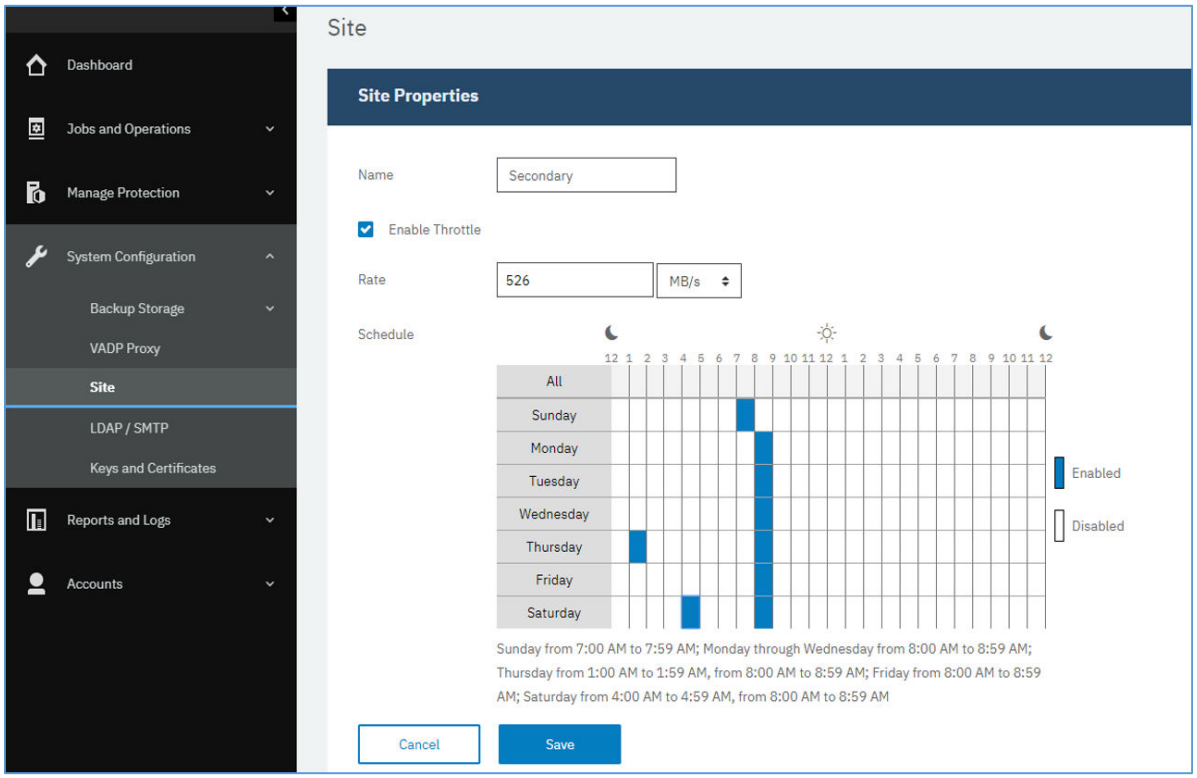


Figura 29. Habilitación de distintos índices de regulación para diferentes horas para mejorar el rendimiento

c) En la tabla de planificación semanal, seleccione una periodicidad diaria de regulación o unos días y horas específicos para la regulación.

Consejo: Para seleccionar una periodicidad, pulse un periodo de tiempo en la tabla. El periodo de tiempo seleccionado se resalta. Para borrar un periodo de tiempo, pulse un periodo de tiempo resaltado. Para seleccionar el mismo periodo de tiempo para cada día de la semana, pulse un periodo de tiempo en la fila **Todos**.

Después de realizar las selecciones, los días y horas de regulación se listan debajo de la tabla de planificación.

5. Pulse **Guardar** para confirmar los cambios y cerrar el panel.

Resultados

El sitio se muestra en la tabla de sitios y se puede aplicar a los servidores de almacenamiento de copias de seguridad nuevos y existentes.

Edición de un sitio

Revise la información del sitio para que refleje los cambios en el entorno de IBM Spectrum Protect Plus.

Procedimiento

Para editar un sitio, complete los pasos siguientes:

1. En el panel de navegación, pulse **Configuración del sistema** > **Sitio**.
2. Pulse el icono de edición que está asociado a un sitio.
   Se muestra el panel **Propiedades del sitio**.
3. Revise el nombre del sitio.
4. Opcional: Para gestionar la actividad de red en una planificación definida, cambie el rendimiento de las operaciones de descarga y réplica de sitios:

a) Seleccione el recuadro de selección **Habilitar regulador**.

b) En el campo **Índice**, ajuste el rendimiento:

1) Cambie el índice de rendimiento numérico pulsando las flechas arriba o abajo.

2) Seleccione una unidad para el rendimiento. Las opciones son **bytes/s**, **KB/s**, **MB/s** y **GB/s**.

El rendimiento predeterminado es 100 MB/s (megabytes por segundo).

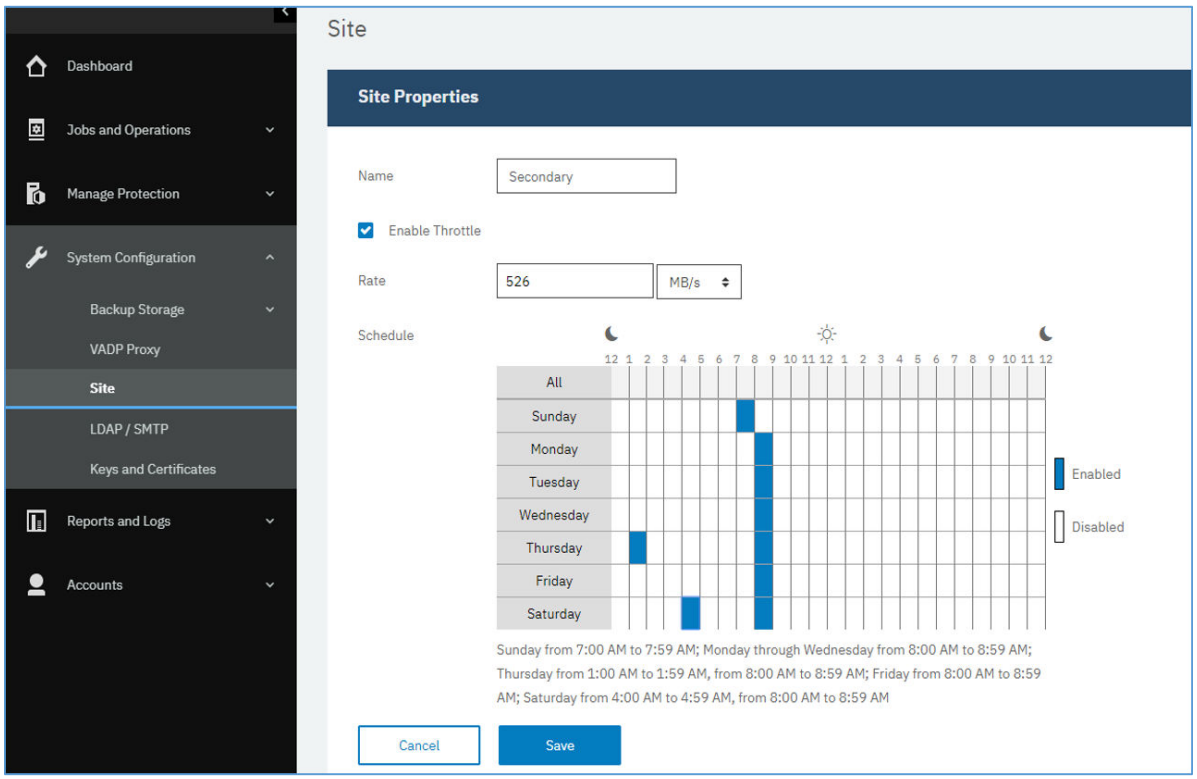


Figura 30. Habilitación de distintos índices de regulación para diferentes horas para mejorar el rendimiento

c) En la tabla de planificación semanal, seleccione una periodicidad diaria de regulación o unos días y horas específicos para la regulación.

Consejo: Para seleccionar una periodicidad, pulse un periodo de tiempo en la tabla. El periodo de tiempo seleccionado se resalta. Para borrar un periodo de tiempo, pulse un periodo de tiempo resaltado. Para seleccionar el mismo periodo de tiempo para cada día de la semana, pulse un periodo de tiempo en la fila **Todos**.

Después de realizar las selecciones, los días y horas de regulación se listan debajo de la tabla de planificación.

5. Pulse **Guardar** para confirmar los cambios y cerrar el panel.

Supresión de un sitio

Suprima un sitio cuando esté obsoleto. Asegúrese de que reasigna el almacenamiento de copias de seguridad a distintos sitios antes de suprimir el sitio.

Procedimiento

Para suprimir un sitio, complete los pasos siguientes:

1. En el panel de navegación, pulse **Configuración del sistema** > **Sitio**.
2. Pulse el icono de suprimir ✕ que está asociado a un sitio.
3. Pulse **Sí** para suprimir el sitio.

Gestión de servidores LDAP y SMTP

Puede añadir un servidor Lightweight Directory Access Protocol (LDAP) y Simple Mail Transfer Protocol (SMTP) para utilizarlos en IBM Spectrum Protect Plus en las características de cuenta de usuario y de informe.

Tareas relacionadas

"Creación de una cuenta de usuario para un grupo LDAP" en la página 312
Añada una cuenta de usuario para un grupo de LDAP a IBM Spectrum Protect Plus.

"Planificación de un informe" en la página 301
Puede planificar informes personalizados en IBM Spectrum Protect Plus para que se ejecuten en momentos específicos.

Adición de un servidor LDAP

Debe añadir un servidor LDAP para crear cuentas de usuario de IBM Spectrum Protect Plus utilizando un grupo de LDAP. Estas cuentas permiten que los usuarios accedan a IBM Spectrum Protect Plus utilizando los nombres de usuario y las contraseñas de LDAP. Solo se puede asociar un servidor LDAP con una instancia del dispositivo virtual de IBM Spectrum Protect Plus.

Acerca de esta tarea

Puede añadir un servidor de Microsoft Active Directory u OpenLDAP. Tenga en cuenta que OpenLDAP no admite el filtro de usuario sAMAaccountName que se utiliza normalmente con Active Directory. Adicionalmente, la opción **memberOf** debe estar habilitada en el servidor OpenLDAP.

Procedimiento

Para registrar un servidor LDAP, complete los pasos siguientes:

1. En el panel de navegación, pulse **Configuración del sistema** > **LDAP/SMTP**.
2. En el panel **Servidores LDAP**, pulse **Añadir servidor LDAP**.
3. Cumplimente los campos de la sección **Servidores LDAP**:

Dirección de host

La dirección IP del host o el nombre lógico del servidor LDAP.

Puerto

El puerto en el que el servidor LDAP está a la escucha. El puerto predeterminado típico es 389 para las conexiones no SSL o 636 para las conexiones SSL.

SSL

Habilite la opción SSL para establecer una conexión segura con el servidor LDAP.

Utilizar usuario existente

Habilite esta opción para seleccionar un nombre de usuario y una contraseña especificados anteriormente para el servidor LDAP.

Nombre de enlace

El nombre distinguido de enlace que se utiliza para autenticar la conexión con el servidor LDAP. IBM Spectrum Protect Plus soporta el enlace simple.

Contraseña

La contraseña asociada con el nombre distinguido de enlace.

DN base

La ubicación donde se pueden encontrar usuarios y grupos.

Filtro de usuario

Un filtro para seleccionar únicamente a aquellos usuarios en el DN base que coinciden con determinados criterios. Un ejemplo de filtro de usuario predeterminado válido es `cn={0}`.

Sugerencias:

- Para habilitar la autenticación utilizando el atributo de denominación de usuarios de Windows **sAMAccountName**, establezca el filtro en `samaccountname={0}`. Cuando se establece este filtro, los usuarios inician la sesión en IBM Spectrum Protect Plus utilizando únicamente un nombre de usuario. No se incluye un dominio.
- Para habilitar la autenticación utilizando el atributo de denominación de nombre principal de usuario (UPN), establezca el filtro en `userprincipalname={0}`. Cuando se establece este filtro, los usuarios inician la sesión en IBM Spectrum Protect Plus utilizando el formato username@domain.
- Para habilitar la autenticación utilizando una dirección de correo electrónico asociada a LDAP, establezca el filtro en `mail={0}`.

El valor **Filtro de usuario** también controla el tipo de nombre de usuario que aparece en la pantalla de IBM Spectrum Protect Plus de usuarios.

RDN de usuario

Vía de acceso distinguida relativa del usuario. Especifique la vía de acceso donde se pueden encontrar los registros de usuario. Un ejemplo de RDN predeterminado válido es `cn=Users`.

RDN de grupo

Vía de acceso distinguida relativa del grupo. Si el grupo está en un nivel distinto al de la vía de acceso de usuario, especifique la vía de acceso donde se pueden encontrar los registros de grupo.

4. Pulse **Guardar**.

Resultados

IBM Spectrum Protect Plus realiza las acciones siguientes:

1. Confirma si se ha realizado una conexión de red.
2. Añade el servidor LDAP a la base de datos.

Una vez añadido el servidor SMTP, el botón **Añadir servidor LDAP** deja de estar disponible.

Qué hacer a continuación

Si se devuelve un mensaje que indica que la conexión no se ha realizado correctamente, revise las entradas. Si las entradas son correctas y la conexión no se ha realizado correctamente, póngase en contacto con un administrador de red para revisar las conexiones.

Tareas relacionadas

"Creación de una cuenta de usuario para un grupo LDAP" en la página 312
Añada una cuenta de usuario para un grupo de LDAP a IBM Spectrum Protect Plus.

Adición de un servidor SMTP

Debe añadir un servidor SMTP para enviar informes planificados a destinatarios de correo electrónico. Solo se puede asociar un servidor SMTP a un dispositivo virtual de IBM Spectrum Protect Plus.

Procedimiento

Para añadir un servidor SMTP, complete los pasos siguientes:

1. En el panel de navegación, pulse **Configuración del sistema** > **LDAP/SMTP**.
2. En el panel **Servidores SMTP**, pulse **Añadir servidor SMTP**.
3. Cumplimente los siguientes campos en la sección **Servidores SMTP**:

Dirección de host

La dirección IP del host, o la vía de acceso y el nombre de host del servidor SMTP.

Puerto

El puerto de comunicaciones del servidor que va a añadir. El puerto predeterminado típico es 25 para conexiones no SSL o 443 para conexiones SSL.

Nombre de usuario

El nombre que se utiliza para acceder al servidor SMTP.

Contraseña

La contraseña asociada al nombre de usuario.

Tiempo de espera excedido

El valor de tiempo de espera excedido del correo electrónico en milisegundos

Desde dirección

La dirección asociada a las comunicaciones de correo electrónico de IBM Spectrum Protect Plus.

Prefijo del asunto

El prefijo para añadir a las líneas de asunto de correo electrónico enviadas desde IBM Spectrum Protect Plus.

4. Pulse **Guardar**.

Resultados

IBM Spectrum Protect Plus realiza las acciones siguientes:

1. Confirma si se ha realizado una conexión de red.
2. Añade el servidor a la base de datos.

Si se devuelve un mensaje que indica que la conexión no se ha realizado correctamente, revise las entradas. Si las entradas son correctas y la conexión no se ha realizado correctamente, póngase en contacto con un administrador de red para revisar las conexiones.

Para probar la conexión SMTP, pulse el botón **Probar servidor SMTP** y, a continuación, especifique una dirección de correo electrónico. Pulse **Enviar**. Se envía un mensaje de correo electrónico de prueba a la dirección de correo electrónico para verificar la conexión.

Después de añadir el servidor SMTP, el botón **Añadir servidor SMTP** ya no está disponible.

Qué hacer a continuación

Tareas relacionadas

“Planificación de un informe” en la página 301

Puede planificar informes personalizados en IBM Spectrum Protect Plus para que se ejecuten en momentos específicos.

Edición de valores de un servidor LDAP o SMTP

Edite los valores de un servidor LDAP o SMTP para que refleje los cambios en el entorno de IBM Spectrum Protect Plus.

Procedimiento

Para editar los valores de un servidor LDAP o SMTP, complete los pasos siguientes:

1. En el menú de navegación, pulse, **Configuración del sistema** > **LDAP/SMTP**.
2. Pulse el icono de edición que está asociado al servidor.
   Se visualiza el panel de edición.

3. Revise los valores del servidor y, a continuación, pulse **Guardar**.

Supresión de un servidor LDAP o SMTP

Suprima un servidor LDAP o SMTP cuando esté obsoleto. Asegúrese de que el servidor no lo está utilizando IBM Spectrum Protect Plus antes de suprimir el servidor.

Procedimiento

Para suprimir un servidor LDAP o SMTP, complete los pasos siguientes:

1. En el menú de navegación, pulse, **Configuración del sistema** > **LDAP/SMTP**.
2. Pulse el icono de suprimir ✕ que está asociado al servidor.
3. Pulse **Sí** para suprimir el servidor.

Aplicación de preferencias globales

Como administrador, puede gestionar las preferencias que se aplican a todas las operaciones de IBM Spectrum Protect Plus en el panel **Preferencias globales** .

Antes de empezar

Únicamente el usuario con credenciales de administrador puede gestionar las preferencias globales.

Acerca de esta tarea

El panel **Preferencias globales** contiene los valores predeterminados para los parámetros que se aplican a todas las operaciones de IBM Spectrum Protect Plus . Las preferencias se organizan en tres categorías. aplicación, protección y seguridad.

Los valores predeterminados para las preferencias globales se muestran en la tabla siguiente.

Tabla 23. Valores predeterminados para las preferencias globales

Preferencia	Valor predeterminado	Unidad (si procede)
Servidores de aplicaciones simultáneos para la sesión de copia de seguridad	0	
Porcentaje de advertencias libres de vSnap (%)	30	Porcentaje (%)
Porcentaje de errores libres de vSnap (%)	20	Porcentaje (%)
VM de grupo por tamaño de grupo de VM (GB)	5120	Gigabytes
VM de grupo por número de VM en el grupo	20	
Tiempo de espera de conexión de VMware	300	Segundos
Intervalo de actualización de copia de seguridad	300	Segundos
Longitud mínima de contraseña	8	Caracteres

Puede cambiar los valores predeterminados en el panel **Preferencias globales**.

Procedimiento

1. En el panel de navegación, pulse **Configuración del sistema** > **Preferencias globales**.
2. Actualice los valores para las preferencias globales. Para revertir al valor predeterminado de un valor especificado anteriormente, pulse el icono de restablecimiento .

Preferencia	Descripción
Aplicación	**Servidores de aplicaciones simultáneos para la sesión de copia de seguridad** El número máximo de servidores de aplicaciones simultáneos por sesión de copia de seguridad.
Copia de seguridad (Hipervisor/ Aplicación)	**Porcentaje de advertencias libres de vSnap (%)** El umbral de porcentaje de espacio libre restante en la agrupación de almacenamiento de vSnap. Las advertencias se visualizan en el registro de trabajo. Por ejemplo, si se especifica un valor de 10, se visualiza un aviso si la agrupación de almacenamiento de vSnap tiene un 10% o menos de espacio libre restante. **Porcentaje de errores libres de vSnap (%)** El umbral de porcentaje de espacio libre restante en la agrupación de almacenamiento de vSnap. Los errores se visualizan en el registro de trabajo. Por ejemplo, si se especifica un valor de 5, se visualiza un error si la agrupación de almacenamiento de vSnap tiene un 5% o menos de espacio libre restante.
Hipervisor	**MV de grupo** Las máquinas virtuales se pueden agrupar juntas. El grupo se puede definir mediante un recuento de las máquinas virtuales contenidas o por el tamaño de las máquinas virtuales contenidas en el grupo. **Tiempo de espera de conexión de VMware** La cantidad de tiempo que IBM Spectrum Protect Plus espera a que los mandatos que se emiten a los vCenters conectados hayan finalizado. Si las operaciones no finalizan dentro de la cantidad de tiempo especificada, se registran como errores. Este valor se aplica sólo a hipervisores de VMware. **Intervalo de actualización de copia de seguridad** La frecuencia con la que se actualizan los mensajes sobre el progreso de la transferencia de datos en el registro de trabajo.
Seguridad	**Longitud mínima de contraseña** La longitud mínima de las contraseñas para IBM Spectrum Protect Plus. De forma predeterminada, la contraseña tiene una longitud mínima de 8 caracteres, pero puede especificar una contraseña más larga. Este valor se aplica a todas las cuentas de usuario.

Nota: Para la agrupación de VM, hay cuatro grupos de VM y cada grupo de VM puede tener un máximo de cinco VM. Cada grupo corresponde a un volumen de destino (stream de datos). Puede ejecutarse un máximo de 20 VM (4 streams de datos) a la vez dependiendo de los cálculos de tamaño.

Inicio de sesión en la consola de administración

Inicie la sesión en la consola de administración para revisar la configuración del dispositivo virtual de IBM Spectrum Protect Plus. La información disponible incluye los valores generales del sistema, los valores de red y de proxy.

Procedimiento

Para iniciar la sesión en la consola de administración, complete los pasos siguientes:

1. Desde un navegador soportado, especifique el URL siguiente:

   ```
   https://HOSTNAME:8090/
   ```

   Donde *HOSTNAME* es la dirección IP de la máquina virtual en la que se despliega la aplicación.
2. En la ventana de inicio de sesión, seleccione uno de los tipos de autenticación siguientes en la lista **Tipo de autenticación**:

Tipo de autentificación	Información de inicio de sesión
IBM Spectrum Protect Plus	Para iniciar la sesión como un usuario de IBM Spectrum Protect Plus con privilegios SYSADMIN, especifique el nombre de usuario y la contraseña del administrador.
Sistema	Para iniciar la sesión como un usuario del sistema, especifique la contraseña de `serveradmin`. La contraseña predeterminada es `sppDP758`. Se le solicitará que cambie esta contraseña durante el primer inicio de sesión.

Qué hacer a continuación

Revise la configuración del dispositivo virtual de IBM Spectrum Protect Plus.

Conceptos relacionados

“Requisitos del sistema ” en la página 13

Antes de instalar IBM Spectrum Protect Plus, revise los requisitos de hardware y software para el producto y los demás componentes que tiene previsto instalar en el entorno de almacenamiento.

“Gestión de roles” en la página 307

Los roles definen las acciones que se pueden completar para los recursos que están definidos en un grupo de recursos. Mientras que un grupo de recursos define los recursos que están disponibles para una cuenta, un rol establece los permisos para interactuar con los recursos.

Establecimiento del huso horario

Utilice la consola de administración para establecer el huso horario del dispositivo de IBM Spectrum Protect Plus.

Procedimiento

Para establecer el huso horario, complete los pasos siguientes:

1. Desde un navegador soportado, especifique el URL siguiente:

   ```
   https://HOSTNAME:8090/
   ```

   Donde *HOSTNAME* es la dirección IP de la máquina virtual en la que se despliega la aplicación.
2. En la ventana de inicio de sesión, seleccione uno de los tipos de autenticación siguientes en la lista **Tipo de autenticación**:

Tipo de autentificación	Información de inicio de sesión
IBM Spectrum Protect Plus	Para iniciar la sesión como un usuario de IBM Spectrum Protect Plus con privilegios SYSADMIN, especifique el nombre de usuario y la contraseña del administrador.

Tipo de autentificación	Información de inicio de sesión
Sistema	Para iniciar la sesión como un usuario del sistema, escriba la contraseña de `serveradmin`. La contraseña predeterminada es `sppDP758`. Se le solicitará que cambie esta contraseña durante el primer inicio de sesión.

3. Pulse **Realizar acciones del sistema**.
4. En la sección **Cambiar huso horario**, seleccione el huso horario.

   Aparece un mensaje que indica que la operación se ha realizado correctamente. Todos los registros y planificaciones de IBM Spectrum Protect Plus reflejarán el huso horario seleccionado. El huso horario seleccionado también se mostrará en el dispositivo de IBM Spectrum Protect Plus cuando se haya iniciado la sesión con el ID de usuario **serveradmin**.
5. Para ver el huso horario actual, seleccione **Información sobre el producto** en la página principal de la consola de administración.

Carga de un certificado SSL desde la consola de administración

Para establecer conexiones seguras en IBM Spectrum Protect Plus, puede cargar un certificado SSL como, por ejemplo, un certificado HTTPS o un certificado LDAP utilizando la consola de administración.

Acerca de esta tarea

En los certificados HTTPS, se admiten los certificados codificados PEM con las extensiones `.cer o .crt`.

En los certificados LDAP/Hyper-V, se admiten certificados codificados DER con las extensiones `.cer o .crt`. Si carga un certificado SSL de LDAP, asegúrese de que IBM Spectrum Protect Plus tenga conectividad con el servidor LDAP y que el servidor LDAP esté en ejecución.

Se aceptan certificados en formato ASCII y binario con las extensiones de archivo estándar `.pem`, `.cer` y `.crt`. Sin embargo, no se puede utilizar la función de importación de certificados de la consola administrativa para actualizar las comunicaciones de servidor web SSL del dispositivo. Para cargar certificados en formato ASCII y binario, utilice la línea de mandatos tal como se describe en "Carga de un certificado SSL desde la línea de mandatos" en la página 287

Procedimiento

Para cargar un certificado SSL, complete los pasos siguientes:

1. Póngase en contacto con el administrador de red para obtener el nombre del certificado que se va a exportar.
2. Desde un navegador soportado, exporte el certificado a su sistema. Anote la ubicación del certificado en el sistema. El proceso de exportación de certificados varía en función del navegador.
3. Desde un navegador soportado, especifique el URL siguiente:

   ```
   https://HOSTNAME:8090/
   ```

   Donde *HOSTNAME* es la dirección IP de la máquina virtual en la que se despliega la aplicación.
4. En la ventana de inicio de sesión, seleccione uno de los tipos de autenticación siguientes en la lista **Tipo de autenticación**:

Tipo de autentificación	Información de inicio de sesión
IBM Spectrum Protect Plus	Para iniciar la sesión como un usuario de IBM Spectrum Protect Plus con privilegios SYSADMIN, especifique el nombre de usuario y la contraseña del administrador.

Tipo de autentificación	Información de inicio de sesión
Sistema	Para iniciar la sesión como un usuario del sistema, especifique la contraseña de `serveradmin`. La contraseña predeterminada es `sppDP758`. Se le solicitará que cambie esta contraseña durante el primer inicio de sesión.

5. Pulse **Gestionar los certificados**.
6. Pulse **Examinar** y seleccione el certificado que desea cargar.
7. Pulse **Cargar el certificado SSL para HTTPS**.
8. Reinicie la máquina virtual en la que se despliega la aplicación.

Carga de un certificado SSL desde la línea de mandatos

Para cargar los certificados en formato ASCII y binario, utilice la línea de mandatos para el dispositivo virtual de IBM Spectrum Protect Plus. Se aceptan los certificados con las extensiones de archivo estándar `.pem`, `.cer` y `.crt`.

Acerca de esta tarea

Este proceso requiere empaquetar los certificados de clave privada, clave pública y de cadena en un archivo en formato PKCS12 (a menudo denominado archivo PFX con extensión .p12) e importarlo todo manualmente al almacén de claves Java de IBM Spectrum Protect Plus. El procedimiento presupone que ya dispone de los objetos de seguridad privados, públicos y de soporte proporcionados por el proveedor de seguridad empaquetados en un archivo de formato PKCS12 denominado *nombre*`.p12`.

Si no dispone de este archivo, debe trabajar con el proveedor de seguridad utilizando un servidor y/o OpenSSL aparte para generar la solicitud de firma de certificado necesaria. Una vez recibida, empaquete los objetos de certificados privados, públicos y de cadena resultantes en el archivo necesario al que se hace referencia a continuación.

Procedimiento

Para importar el archivo *nombre*`.p12`, complete los pasos siguientes:

1. Inicie la sesión con el ID de usuario **serveradmin** en el dispositivo virtual de IBM Spectrum Protect Plus.

   La contraseña inicial es `sppDP758`.
2. En la línea de mandatos, ejecute el mandato siguiente:

   ```
   /usr/java/latest/bin/keytool -importkeystore -deststorepass ecx-beta -
   destkeystore /opt/virgo/configuration/keystore -srckeystore NAME.p12 -
   srcstoretype PKCS12
   ```
3. Reinicie el dispositivo virtual.

Inicio de sesión en el dispositivo virtual

Inicie la sesión en el dispositivo virtual de IBM Spectrum Protect Plus utilizando vSphere Client para acceder a la línea de mandatos. Puede acceder a la línea de mandatos en un entorno VMware o en un entorno Hyper-V.

Acceso al dispositivo virtual en VMware

En un entorno VMware, inicie la sesión en el dispositivo virtual de IBM Spectrum Protect Plus a través de vSphere Client para acceder a la línea de mandatos.

Procedimiento

Complete los pasos siguientes para acceder a la línea de mandatos del dispositivo virtual:

1. En vSphere Client, seleccione la máquina virtual donde se despliega IBM Spectrum Protect Plus.
2. En la pestaña **Resumen**, seleccione **Abrir consola** y pulse en la consola.
3. Seleccione **Iniciar sesión** y especifique el nombre de usuario y la contraseña. El nombre de usuario predeterminado es `serveradmin` y la contraseña predeterminada es sppDP758.

Qué hacer a continuación

Especifique mandatos para administrar el dispositivo virtual. Para cerrar la sesión, escriba `exit`.

Acceso al dispositivo virtual en Hyper-V

En un entorno Hyper-V, inicie la sesión en el dispositivo virtual de IBM Spectrum Protect Plus mediante vSphere Client para acceder a la línea de mandatos.

Procedimiento

Complete los pasos siguientes para acceder a la línea de mandatos del dispositivo virtual:

1. En Hyper-V Manager, seleccione la máquina virtual donde se despliega IBM Spectrum Protect Plus.
2. Pulse el botón derecho del ratón en la máquina virtual y seleccione **Conectar**
3. Seleccione **Iniciar sesión** y especifique el nombre de usuario y la contraseña. El nombre de usuario predeterminado es `serveradmin` y la contraseña predeterminada es sppDP758.

Qué hacer a continuación

Especifique mandatos para administrar el dispositivo virtual. Para cerrar la sesión, escriba `exit`.

Cómo probar la conectividad de red

La herramienta de servicio de IBM Spectrum Protect Plus prueba direcciones y puertos de host para determinar si se puede establecer una conexión. Puede utilizar la herramienta de servicio para verificar si se puede establecer una conexión entre IBM Spectrum Protect Plus y un nodo

Puede ejecutar la herramienta de servicio desde la línea de mandatos de IBM Spectrum Protect Plus o de forma remota utilizando un archivo .jar. Si se puede establecer una conexión, la herramienta devuelve una marca de selección verde. Si no se puede establecer una conexión, se visualiza la condición de error, junto con las posibles causas y acciones.

La herramienta proporciona una guía para las condiciones de error siguientes:

- Tiempo de espera excedido
- Conexión rechazada
- Host desconocido
- No hay ruta

Ejecución de la herramienta de servicio desde una interfaz de línea de mandatos

Puede iniciar la herramienta de servicio desde la interfaz de línea de mandatos del dispositivo virtual de IBM Spectrum Protect Plus y ejecutar la herramienta en un navegador web. A continuación, puede utilizar la herramienta de servicio para verificar la conectividad de red entre IBM Spectrum Protect Plus y un nodo

Procedimiento

1. Inicie la sesión en el dispositivo virtual de IBM Spectrum Protect Plus utilizando el ID de usuario `serveradmin` y acceda al indicador de mandatos. Emita el mandato siguiente:

   ```
   # sudo bash
   ```

2. Abra el puerto 9000 en el cortafuegos emitiendo el mandato siguiente:

   ```
   # firewall-cmd –add-port=9000/tcp
   ```

3. Ejecute la herramienta emitiendo el mandato siguiente:

   ```
   # java -Dserver.port=9000 -jar /opt/ECX/spp/public/assets/tool/ngxdd.jar
   ```

4. Para conectarse a la herramienta, escriba el siguiente URL en un navegador:

   ```
   http://hostname:9000
   ```

   donde *hostname* especifica la dirección IP de la máquina virtual en la que se despliega la aplicación.

5. Para especificar el nodo que desea probar, cumplimente los campos siguientes:

   Host
   El nombre de host o la dirección IP del nodo que desea probar.

   Puerto
   El puerto de conexión a probar.

6. Pulse **Guardar**.
7. Para ejecutar la herramienta, pase el cursor por encima de la herramienta y, a continuación, pulse el botón **Ejecutar** verde.

   Si no se puede establecer una conexión, se visualiza la condición de error, junto con las posibles causas y acciones.

8. Detenga la herramienta emitiendo el mandato siguiente en la línea de mandatos:

   ```
   ctl-c
   ```

9. Proteja el entorno de almacenamiento reconfigurando el cortafuegos. Emita los mandatos siguientes:

   ```
   # firewall-cmd --zone=public --remove-port=9000/tcp
   # firewall-cmd --runtime-to-permanent
   # firewall-cmd --reload
   ```

Nota: Si el mandato `firewall-cmd` no está disponible en el sistema, edite el cortafuegos manualmente para añadir los puertos necesarios y reinicie el cortafuegos utilizando `iptables`. Para obtener más información sobre la edición de reglas de cortafuegos, consulte la sección **Configuración de cortafuegos utilizando iptables** en: https://www.ibm.com/support/knowledgecenter/en/STXKQY_5.0.3/com.ibm.spectrum.scale.v5r03.doc/bl1adv_firewallportopenexamples.htm.

Ejecución remota de la herramienta de servicio

Puede descargar la herramienta de servicio como un archivo .jar desde la interfaz de usuario de IBM Spectrum Protect Plus. A continuación, puede utilizar la herramienta de servicio para probar de forma remota la conectividad entre IBM Spectrum Protect Plus y un nodo.

Procedimiento

1. En la interfaz de usuario de IBM Spectrum Protect Plus, pulse el menú de usuario y, a continuación, pulse **Descargar herramienta de servicio**.

   Se descarga un archivo .jar en la estación de trabajo.

2. Inicie la herramienta desde una interfaz de línea de mandatos. Java™ solo es necesario en el sistema en el que se lanzará la herramienta. Los puntos finales o los sistemas de destino que están probados con la herramienta no requieren Java.

El mandato siguiente lanza la herramienta en un entorno Linux:

```
# java -jar -Dserver.port=9000 /<tool path >/ngxdd.jar
```

3. Para conectarse a la herramienta, escriba el siguiente URL en un navegador:

   ```
   http://hostname:9000
   ```

   donde *hostname* especifica la dirección IP de la máquina virtual en la que se despliega la aplicación.
4. Para especificar el nodo que desea probar, cumplimente los campos siguientes:

   Host
   El nombre de host o la dirección IP del nodo que desea probar.

   Puerto
   El puerto de conexión a probar.
5. Pulse **Guardar**.
6. Para ejecutar la herramienta, pase el cursor por encima de la herramienta y, a continuación, pulse el botón **Ejecutar** verde.

   Si no se puede establecer una conexión, se visualiza la condición de error, junto con las posibles causas y acciones.
7. Detenga la herramienta emitiendo el mandato siguiente en la línea de mandatos:

   ```
   ctl-c
   ```

Adición de discos virtuales

Puede añadir discos virtuales nuevos (discos duros) al dispositivo virtual de IBM Spectrum Protect Plus utilizando vCenter.

Cuando despliega el dispositivo virtual de IBM Spectrum Protect Plus, puede desplegar todos los discos virtuales a un almacén de datos que especifique en el momento del despliegue. Puede añadir un disco dentro del dispositivo virtual y configurarlo como un gestor de volúmenes lógicos (LVM). A continuación, puede montar el nuevo disco como un nuevo volumen o adjuntar el nuevo disco a los volúmenes existentes en el dispositivo virtual.

Puede revisar las particiones de disco utilizando el mandato **`fdisk -l`**. Puede revisar los volúmenes físicos y los grupos de volúmenes en el dispositivo virtual de IBM Spectrum Protect Plus utilizando los mandatos **`pvdisplay`** y **`vgdisplay`**.

Adición de un disco al dispositivo virtual

Utilice el cliente de vCenter para editar los valores de la máquina virtual.

Antes de empezar

Para ejecutar mandatos, debe conectarse a la línea de mandatos del dispositivo virtual de IBM Spectrum Protect Plus utilizando Secure Shell (SSH) e iniciar la sesión con el ID de usuario `serveradmin`. La contraseña inicial predeterminada es `sppDP758` y se le solicitará que cambie la contraseña cuando inicie la sesión por primera vez.

Procedimiento

Para añadir un disco a un dispositivo virtual de IBM Spectrum Protect Plus, complete los pasos siguientes desde el cliente de vCenter:

1. Desde el cliente de vCenter, complete los pasos siguientes:
   a) En la pestaña **Hardware**, pulse **Añadir**.
   b) Seleccione **Crear un nuevo disco virtual**.

c) Seleccione el tamaño de disco necesario. En la sección **Ubicación**, seleccione una de las opciones siguientes:

- Para utilizar el almacén de datos actual, seleccione **Almacenar con la máquina virtual**.
- Para especificar uno o más almacenes de datos para el disco virtual, seleccione **Especificar un almacén de datos o un clúster de almacenes de datos**. Pulse **Examinar** para seleccionar los nuevos almacenes de datos.

d) En la pestaña **Opciones avanzadas**, deje los valores predeterminados.

e) Revise y guarde los cambios.

f) Pulse la opción **Editar valores** para que la máquina virtual visualice el nuevo disco duro.

2. Añada el nuevo dispositivo SCSI sin volver a arrancar el dispositivo virtual. Desde la consola del dispositivo de IBM Spectrum Protect Plus, emita el mandato siguiente:

```
echo "-- -" > /sys/class/scsi_host/host#/scan
```

Donde # es el último número de host.

Adición de capacidad de almacenamiento de un nuevo disco al volumen de dispositivo

Después de añadir un disco al dispositivo virtual, puede adjuntar el nuevo disco a los volúmenes existentes dentro del dispositivo virtual.

Antes de empezar

Para ejecutar mandatos, debe conectarse a la consola del dispositivo virtual de IBM Spectrum Protect Plus utilizando SSH e iniciar la sesión con el ID de usuario **serveradmin**. La contraseña inicial predeterminada es sppDP758 y se le solicitará que cambie la contraseña cuando inicie la sesión por primera vez.

Acerca de esta tarea

Únicamente debe completar esta tarea si desea añadir la capacidad de almacenamiento de un nuevo disco a un volumen de dispositivo existente. Si ha añadido el disco como un nuevo volumen, no es necesario que complete esta tarea.

Procedimiento

Para añadir capacidad de almacenamiento de un nuevo disco al volumen de dispositivo, complete los pasos siguientes desde la consola del dispositivo virtual:

1. Complete los pasos siguientes para configurar una partición para el nuevo disco y establezca la partición para que sea de tipo Linux LVM:
   a) Abra el nuevo disco utilizando el mandato **fdisk**:

```
[serveradmin@localhost ~]# fdisk /dev/sdd
```

   El programa de utilidad **fdisk** se inicia en modalidad interactiva. Se muestra una salida similar a la siguiente:

```
Device contains neither a valid DOS partition table, nor Sun, SGI or
OSF disklabel
Building a new DOS disklabel with disk identifier 0xb1b293df.
Changes will remain in memory only, until you decide to write them.
After that, of course, the previous content won't be recoverable.
Warning: invalid flag 0x0000 of partition table 4 will be corrected by
w(rite)
WARNING: DOS-compatible mode is deprecated. It's strongly recommended
to
switch off the mode (command 'c') and change display units to
sectors (command 'u').
Command (m for help):
```

a) En la línea de mandatos **fdisk**, especifique el submandato **n** para añadir una partición.

```
Command (m for help): n
```

Se muestran las siguientes opciones de acción de mandato:

```
Command (m for help): n
Command action
e extended
p primary partition (1-4)
```

b) Especifique la acción del mandato **p** para seleccionar la partición primaria.
Se le solicitará un número de partición:

```
Command (m for help): n
Command action
e extended
p primary partition (1-4)
Partition number (1-4):
```

c) En el indicador del número de partición, escriba el número de partición 1.

```
Partition number (1-4): 1
```

Se muestra la siguiente solicitud:

```
First cylinder (1-2610, default 1):
```

d) No escriba nada en la solicitud First cylinder. Pulse la tecla **Intro**.
Se muestra la salida y solicitud siguiente:

```
First cylinder (1-2610, default 1):
Using default value 1
Last cylinder, +cylinders or +size{K,M,G} (1-2610, default 2610):
```

e) No escriba nada en la solicitud Last cylinder. Pulse la tecla **Intro**.
Aparecerán los siguientes resultados:

```
Last cylinder, +cylinders or +size{K,M,G} (1-2610, default 2610):
Using default value 2610
Command (m for help):
```

f) En la línea de mandatos **fdisk**, especifique el submandato **t** para cambiar el ID de sistema de una partición.

```
Command (m for help): t
```

Se le solicitará un código hexadecimal que identifique el tipo de partición:

```
Selected partition 1
Hex code (type L to list codes):
```

g) En la solicitud de Hex code, escriba el código hexadecimal 8e para que especifique el tipo de partición Linux LVM.
Aparecerán los siguientes resultados:

```
Hex code (type L to list codes): 8e
Changed system type of partition 1 to 8e (Linux LVM)
Command (m for help):
```

h) En la línea de mandatos **fdisk**, especifique el submandato **w** para escribir la tabla de particiones y para salir del programa de utilidad **fdisk**.

```
Command (m for help): w
```

Aparecerán los siguientes resultados:

```
Command (m for help): w (write table to disk and exit)
The partition table has been altered!
Calling ioctl() to re-read partition table.
Syncing disks.
```

2. Para revisar los cambios en el disco, emita el mandato **fdisk -1**.
3. Para revisar la lista actual de Volúmenes físicos (PV), emita el mandato **pvdisplay**.
4. Para crear un nuevo volumen físico (PV), emita el mandato **pvcreate /dev/sdd1**.
5. Para ver el nuevo volumen físico de /dev/sdd1, emita el mandato **pvdisplay**.
6. Para revisar el grupo de volúmenes (VG), emita el mandato **vgdisplay**.
7. Para añadir el volumen físico (PV) al grupo de volúmenes (VG) e incrementar el espacio del grupo de volúmenes, emita el mandato siguiente:

```
vgextend data_vg /dev/sdd1
```

8. Para verificar si data_vg se ha ampliado y si el espacio libre está disponible para que los volúmenes lógicos (o el volumen /data) lo utilicen, emita el mandato **vgdisplay**.
9. Para revisar el volumen de volumen lógico (LV) /data, emita el mandato **lvdisplay**. Se muestra el uso del volumen /data.
10. Para añadir el espacio del volumen lógico /data a la capacidad de volumen total, emita el mandato **lvextend**.
    En este ejemplo, se están añadiendo 20 GB de espacio a un volumen de 100 GB.

```
[serveradmin@localhost ~]# lvextend -L120gb -r /dev/data_vg/data
Size of logical volume data_vg/data changed from 100.00 GiB to 120.00 GiB .
Logical volume data successfully resized
resize2fs 1.41.12 (date)
Filesystem at /dev/mapper/data_vg-data is mounted on /data; on-line
resizing required
old desc_blocks = 7, new_desc_blocks = 8
Performing an on-line resize of /dev/mapper/data_vg-data to 31195136
(4k) blocks.
The filesystem on /dev/mapper/data_vg-data is now 31195136 blocks
long.
```

Después de ejecutar el mandato anterior, el tamaño del volumen /data se muestra en la salida del mandato **lvdisplay** como 120 GB:

```
[serveradmin@localhost ~]# lvdisplay
--- Logical volume ---
LV Path: /dev/data_vg/data
LV Name: data
VG Name: data_vg
LV UUID: [uuid]
LV Write Access: read/write
LV Creation host, time localhost.localdomain, [date, time]
LV Status: available
# open: 1
LV Size: 120.00 GiB
Current LE: 30208
Segments : 2
Allocation inherit
Read ahead sectors: auto
- currently set to: 256
Block device: 253:1
[serveradmin@localhost ~]# df -h
Filesystem Size Used Avail Use% Mounted on
/dev/sda3 14G 2.6G 11G 20% /
tmpfs 16G 0 16G 0% /dev/shm
/dev/sda1 240M 40M 188M 18% /boot
/dev/mapper/data_vg-data
118G 6.4G 104G 6% /data
/dev/mapper/data2_vg-data2
246G 428M 234G 1% /data2
```

Capítulo 12. Gestión de informes y registros

IBM Spectrum Protect Plus proporciona un número de informes predefinidos que puede personalizar para cumplir los requisitos de creación de informes. También se proporciona un registro de las acciones que los usuarios completan en IBM Spectrum Protect Plus.

Tipos de informes

Puede personalizar los informes predefinidos para supervisar la utilización del almacenamiento de copia de seguridad y otros aspectos del entorno del sistema.

Los informes se basan en los datos recopilados por el trabajo de inventario más reciente. Puede generar informes después de que se hayan completado todos los trabajos de catalogación y los trabajos de condensación de base de datos posteriores. Puede ejecutar los tipos de informes siguientes:

- Informes de utilización de almacenamiento de copia de seguridad
- Informes de protección
- Informes del sistema
- Informes de entorno de máquina virtual

Los informes incluyen elementos interactivos, como la búsqueda de valores individuales dentro de un informe, el desplazamiento vertical y la ordenación de columnas.

Informes de utilización de almacenamiento de copia de seguridad

IBM Spectrum Protect Plus proporciona informes de utilización de almacenamiento de copia de seguridad que muestran la utilización del almacenamiento y el estado del almacenamiento de copia de seguridad, como por ejemplo servidores vSnap.

Para ver informes de utilización de almacenamiento de copia de seguridad, complete los pasos siguientes:

1. En el panel de navegación, pulse **Informes y registros** > **Informes**.
2. Expanda **Utilización de almacenamiento de copia de seguridad** en el panel **Informes** .

Están disponibles los siguientes informes:

Uso de copias de seguridad de VM
Revise la utilización de las copias de seguridad de la máquina virtual (VM) en el almacenamiento de copias de seguridad, incluidos los datos siguientes:

- El nombre de cada máquina virtual, su ubicación y el hipervisor asociado.
- La política SLA que se utiliza para proteger la máquina virtual.
- La ubicación del almacenamiento de copias de seguridad. El almacenamiento de copias de seguridad puede ser el nombre de host o la dirección IP de un disco, el nombre de un servidor de nube o el nombre del servidor de repositorio.
- El tamaño de cada copia de seguridad de máquina virtual.
- El número de puntos de restauración que están disponibles para cada máquina virtual.

En las máquinas virtuales de VMware, para acotar los resultados para mostrar las máquinas virtuales que tienen etiquetas de VMware, seleccione una o varias etiquetas disponibles en el menú desplegable **Etiquetas**. El valor predeterminado es **Todos**, que muestra datos para todas las copias de seguridad de máquina virtual.

Informe de utilización de almacenamiento vSnap
Revise la utilización de almacenamiento de los servidores vSnap, incluidos el estado de disponibilidad, el espacio libre y el espacio utilizado. El informe de utilización de almacenamiento

vSnap muestra una visión general de los servidores vSnap y una vista detallada de las máquinas virtuales y de las bases de datos individuales que están protegidas en cada servidor vSnap.

Utilice las opciones de informe para filtrar los servidores vSnap específicos que hay que visualizar. Para ver una vista detallada de las máquinas virtuales y de las base de datos individuales que están protegidas en cada servidor vSnap, seleccione **Mostrar recursos protegidos por Snap Storage**. Este área del informe muestra los nombres de las máquinas virtuales, el hipervisor asociado, la ubicación y la proporción de compresión/deduplicación del servidor vSnap.

La capacidad de almacenamiento y los valores de uso que muestra IBM Spectrum Protect Plus pueden variar entre los que aparecen en el panel de instrumentos frente a los que aparecen en el informe de utilización de almacenamiento vSnap. El panel de instrumentos muestra información activa, mientras que el informe refleja los datos de la última ejecución del trabajo de inventario. Las variaciones también se deben a los diferentes algoritmos de redondeo.

Conceptos relacionados

"Acciones de informes" en la página 300
Puede ejecutar, guardar o planificar informes en IBM Spectrum Protect Plus.

"Tipos de informes" en la página 295
Puede personalizar los informes predefinidos para supervisar la utilización del almacenamiento de copia de seguridad y otros aspectos del entorno del sistema.

Informes de protección

IBM Spectrum Protect Plus proporciona informes que muestran el estado de protección de los recursos. Mediante la visualización de los informes y la adopción de cualquier acción necesaria, puede ayudar a garantizar que los datos estén protegidos mediante parámetros de objetivos de puntos de recuperación definidos por el usuario.

Para ver los informes de protección, realice los pasos siguientes:

1. En el panel de navegación, pulse **Informes y registros** > **Informes**.
2. Expanda **Protección** en el panel **Informes**.

Están disponibles los siguientes informes:

Informe de máquinas virtuales protegidas y no protegidas

Ejecute el informe de máquinas virtuales protegidas y no protegidas para ver el estado de protección de las máquinas virtuales. El informe muestra el número total de máquinas virtuales añadidos al inventario de IBM Spectrum Protect Plus antes de que se inicien los trabajos de copia de seguridad.

Utilice las opciones de informe para filtrar por tipo de hipervisor y para seleccionar hipervisores específicos que se visualizarán.

Para excluir las máquinas virtuales no protegidas en el informe, seleccione **Ocultar máquinas virtuales no protegidas**.

Para excluir máquinas virtuales de las que no se han realizado copias de seguridad en el almacenamiento de copias de seguridad secundario, seleccione **Mostrar solo las VM con copias de seguridad descargadas**.

La **Vista de resumen** muestra una visión general del estado de protección de la máquina virtual, incluyendo el número de máquinas virtuales no protegidas y protegidas y la capacidad gestionada de las máquinas virtuales protegidas. La capacidad gestionada es la capacidad utilizada de una máquina virtual. La **Vista de detalle** proporciona más información sobre las máquinas virtuales protegidas y no protegidas, incluidos nombres y ubicación.

Informe de bases de datos protegidas y no protegidas

Ejecute el informe de bases de datos protegidas y no protegidas para ver el estado de protección de las bases de datos. El informe muestra el número total de bases de datos que se han añadido al inventario de IBM Spectrum Protect Plus antes de que se inicien los trabajos de copia de seguridad.

Utilice las opciones de informe para filtrar por el tipo de aplicación, el servidor de aplicaciones y el tipo de servidor de aplicaciones que desea visualizar.

Para excluir bases de datos que están protegidas mediante trabajos de copia de seguridad basados en hipervisor, seleccione **Ocultar bases de datos protegidas como parte de la copia de seguridad del hipervisor**.

Para excluir bases de datos no protegidas en el informe, seleccione **Ocultar bases de datos no protegidas**.

La **vista de resumen** muestra una visión general del estado de protección del servidor de aplicaciones, incluido el número de bases de datos no protegidas y protegidas, así como la capacidad front-end de las bases de datos protegidas. La capacidad front-end es la capacidad utilizada de una base de datos. La **Vista de detalle** proporciona más información sobre las bases de datos protegidas y no protegidas, incluidos sus nombres y ubicación.

Informe de historial de copias de seguridad VM

Ejecute el informe de historial de copias de seguridad para revisar el historial de protección de máquinas virtuales específicas. Para ejecutar el informe, se debe especificar como mínimo una máquina virtual en la opción **Máquinas virtuales**. Puede seleccionar varios nombres de máquinas virtuales.

Utilice las opciones de informe para filtrar por trabajos fallidos o satisfactorios y la hora de la última copia de seguridad. El informe se puede filtrar más por políticas de acuerdo de nivel de servicio (SLA) específicas. En la **Vista de detalle**, pulse el icono más situado junto a un trabajo asociado para ver detalles del trabajo, por ejemplo, la razón por la que un trabajo ha fallado o el tamaño de una copia de seguridad satisfactoria.

Informe de historial de copias de seguridad de bases de datos

Ejecute el informe de historial de copias de seguridad para revisar el historial de protección de bases de datos específicas. Para ejecutar el informe, se debe especificar como mínimo una base de datos en la opción **Bases de datos**. Puede seleccionar varias bases de datos.

Utilice las opciones de informe para filtrar por trabajos fallidos o satisfactorios y la hora de la última copia de seguridad. El informe se puede filtrar más por políticas de SLA específicas. En la **Vista de detalle**, pulse el icono más situado junto a un trabajo asociado para ver detalles adicionales del trabajo, como por ejemplo la razón por la que un trabajo ha fallado o el tamaño de una copia de seguridad satisfactoria.

Informe de conformidad con RPO de las VM en políticas de SLA

El informe de conformidad con RPO de las VM en políticas de SLA muestra máquinas virtuales en relación con objetivos de puntos de recuperación (RPO) tal como se han definido en políticas de SLA. El informe muestra la información siguiente:

- Máquinas virtuales conformes
- Máquinas virtuales que no son conformes
- Máquinas virtuales en las que la última sesión de trabajo de copia de seguridad ha fallado

Utilice las opciones de informe para filtrar por tipo de hipervisor y para seleccionar hipervisores específicos que se visualizarán. El informe puede filtrar más por máquinas virtuales que son conformes o no con los objetivos de punto de recuperación (RPO) definidos.

Informe de conformidad con RPO de las bases de datos en políticas de SLA

El informe de conformidad con RPO de las bases de datos en políticas de SLA muestra bases de datos en relación con objetivos de puntos de recuperación tal como se ha definido en las políticas de SLA. El informe muestra la información siguiente:

- Bases de datos conformes
- Bases de datos que son conformes
- Bases de datos en las que ha fallado la última sesión de trabajo de copia de seguridad

Utilice las opciones de informe para filtrar por tipo de aplicación y para seleccionar los servidores de aplicaciones específicos que se deben visualizar. El informe puede filtrar más por bases de datos que son conformes o no con los objetivos de punto de recuperación (RPO) definidos o por tipo de

protección, incluidos datos de los que se ha realizado una copia de seguridad en vSnap o mediante la réplica.

Conceptos relacionados

"Tipos de informes" en la página 295
Puede personalizar los informes predefinidos para supervisar la utilización del almacenamiento de copia de seguridad y otros aspectos del entorno del sistema.

Informes del sistema

IBM Spectrum Protect Plus proporciona informes del sistema que muestran una vista en profundidad del estado de la configuración, incluida la información del sistema de almacenamiento, los trabajos y el estado del trabajo.

Para ver los informes del sistema, realice los pasos siguientes:

1. En el panel de navegación, pulse **Informes y registros** > **Informes**.
2. Expanda **Sistema** en el panel **Informes**.

Están disponibles los siguientes informes:

Informe de configuración
Revise la configuración de los servidores de aplicaciones, los hipervisores y el almacenamiento de copia de seguridad que está disponible. Utilice las opciones de informe para filtrar los tipos de configuración que se van a visualizar. En el informe se muestra el nombre del recurso, el tipo de recurso, el sitio asociado y el estado de conexión SSL.

Informe de trabajos
Revise los trabajos disponibles en la configuración. Ejecute este informe para ver los trabajos por tipo, su duración media y el porcentaje de ejecución satisfactorio. Utilice las opciones de informe para filtrar los tipos de trabajo que se visualizarán y para visualizar los trabajos que se han ejecutado correctamente durante un periodo de tiempo. La **Vista de resumen** lista los trabajos por tipo, junto con el número de veces que se ha ejecutado, ha completado o ha fallado una sesión de trabajo. Las sesiones de trabajo listadas como Otro son trabajos que han terminado de forma anómala, se han ejecutado parcialmente, se ejecutan en la actualidad, se han omitido o se han detenido. En la **Vista de detalle**, pulse el icono más situado junto a un trabajo asociado para ver detalles adicionales del trabajo como, por ejemplo, máquinas virtuales que están protegidas por un trabajo de copia de seguridad, el tiempo de ejecución promedio y el siguiente tiempo de ejecución planificado si el trabajo está planificado.

Informe de licencia
Revise la configuración del entorno de IBM Spectrum Protect Plus en relación con las funciones con licencia. Se muestran las secciones y los campos siguientes en este informe:

Protección de máquinas virtuales
El campo **Número total de máquinas virtuales** muestra el número total de máquinas virtuales protegidas a través de trabajos de copia de seguridad de hipervisor, más el número de máquinas virtuales que alojan bases de datos de aplicación protegidas a través de trabajos de copia de seguridad de aplicaciones (no hay trabajos de copia de seguridad de hipervisor). El campo **Capacidad front-end** muestra el tamaño utilizado de estas máquinas virtuales.

Protección física de la máquina
El campo **Número total de servidores físicos** muestra el número total de servidores de aplicaciones físicos que alojan bases de datos que están protegidas a través de trabajos de copia de seguridad de aplicaciones. El campo **Capacidad front-end** muestra el tamaño utilizado de estos servidores de aplicaciones físicos.

Utilización de almacenamiento de copia de seguridad (vSnap)
El campo **Número total de servidores vSnap** muestra el número de servidores vSnap que están configurados en IBM Spectrum Protect Plus como destino de la copia de seguridad. El campo **Capacidad de destino** muestra la capacidad total utilizada de los servidores vSnap, excluidos los volúmenes de destino de réplica.

Conceptos relacionados

"Tipos de informes" en la página 295
Puede personalizar los informes predefinidos para supervisar la utilización del almacenamiento de copia de seguridad y otros aspectos del entorno del sistema.

Informes de entorno de máquinas virtuales

IBM Spectrum Protect Plus proporciona informes de entorno de máquinas virtuales para visualizar la utilización de almacenamiento y el estado de las máquinas virtuales y de los almacenes de datos.

Para ver los informes de entorno de máquinas virtuales, complete los pasos siguientes:

1. En el panel de navegación, pulse **Informes y registros** > **Informes**.
2. Expanda **Entorno de máquinas virtuales** en el panel **Informes** .

Están disponibles los siguientes informes:

Informes de almacenes de datos de máquinas virtuales

Revise la utilización de almacenamiento de los almacenes de datos, incluido el espacio libre total, el espacio de suministro y las capacidades. Ejecute este informe para ver los almacenes de datos, el número de máquinas virtuales en los almacenes de datos y el porcentaje de espacio disponible. Utilice las opciones de informe para filtrar por tipo de hipervisor y para seleccionar hipervisores específicos para mostrar. El **Filtro de vista de detalle** controla los almacenes de datos que se deben visualizar en la **Vista de detalle** en función del porcentaje de espacio utilizado. Utilice el filtro **Mostrar solo almacenes de datos huérfanos** para ver almacenes de datos que no tienen asignadas máquinas virtuales o máquinas virtuales que tienen un estado inaccesible. El motivo para que un almacén de datos esté en un estado huérfano se muestra en el campo **Almacén de datos** en la **Vista de detalle**.

Informes de LUNs de máquinas virtuales

Revise la utilización de almacenamiento de números de unidades lógicas (LUNs) de las máquinas virtuales. Ejecute este informe para ver los LUN, los almacenes de datos asociados, las capacidades y los proveedores de almacenamiento. Utilice las opciones de informe para filtrar por tipo de hipervisor y para seleccionar hipervisores específicos que se visualizarán. Utilice el filtro **Mostrar solo almacenes de datos huérfanos** para ver almacenes de datos que no tienen asignadas máquinas virtuales o máquinas virtuales que tienen un estado inaccesible.

Informe de extensión de instantáneas de máquinas virtuales

Este informe muestra la edad, el nombre y el número de instantáneas que se utilizan para proteger los recursos del hipervisor. Utilice las opciones de informe para filtrar por tipo de hipervisor y para seleccionar hipervisores específicos que se visualizarán. Utilice el filtro **Hora de creación del filtro** para visualizar instantáneas de periodos específicos de tiempo.

Informe de extensión de máquinas virtuales

Revise el estado de las máquinas virtuales, incluidas las máquinas virtuales que están apagadas, encendidas o suspendidas. Ejecute este informe para ver las máquinas virtuales no utilizadas, la fecha y la hora en las que se han apagado y las plantillas de máquina virtual. Utilice las opciones de informe para filtrar por tipo de hipervisor y para seleccionar hipervisores específicos que se visualizarán. El informe se puede filtrar más por el estado de alimentación a lo largo del tiempo, incluidos los días desde el último apagado y los días desde la última suspensión. La sección **Vista rápida** muestra un diagrama circular de espacio libre y utilizado en las máquinas virtuales en función del estado de alimentación. Utilice el filtro **Hipervisor** para visualizar máquinas virtuales en todos los hosts o en un host específico. La información en la **Vista de detalle** se clasifica por estado de alimentación. Se proporciona una tabla aparte para las plantillas de máquina virtual.

Informe de almacenamiento de máquinas virtuales

Revise las máquinas virtuales y los almacenes de datos asociados en este informe. Vea los almacenes de datos asociados y el espacio suministrado de los almacenes de datos. Utilice las opciones de informe para filtrar por tipo de hipervisor y para seleccionar hipervisores específicos que se

visualizarán. La **Vista de detalle** muestra almacenes de datos asociados y la cantidad de espacio en el almacén de datos que se asigna a archivos de disco virtuales.

Conceptos relacionados

"Tipos de informes" en la página 295
Puede personalizar los informes predefinidos para supervisar la utilización del almacenamiento de copia de seguridad y otros aspectos del entorno del sistema.

Acciones de informes

Puede ejecutar, guardar o planificar informes en IBM Spectrum Protect Plus.

Ejecución de un informe

Puede ejecutar informes de IBM Spectrum Protect Plus con parámetros predeterminados o ejecutar informes personalizados con parámetros personalizados.

Procedimiento

Para ejecutar un informe, lleve a cabo los pasos siguientes:

1. En el panel de navegación, pulse **Informes y registros** > **Informes**.
2. Expanda un tipo de informe y seleccione un informe que desee ejecutar.
3. Ejecute el informe con parámetros personalizados o parámetros predeterminados:
   - Para ejecutar el informe con parámetros personalizados, establezca los parámetros en la sección **Opciones** y pulse **Ejecutar**. Los parámetros son exclusivos de cada informe.
   - Para ejecutar el informe con parámetros predeterminados, pulse **Ejecutar**.

Qué hacer a continuación

Revise el informe en el panel **Informes**.

Conceptos relacionados

"Gestión de informes y registros" en la página 295
IBM Spectrum Protect Plus proporciona un número de informes predefinidos que puede personalizar para cumplir los requisitos de creación de informes. También se proporciona un registro de las acciones que los usuarios completan en IBM Spectrum Protect Plus.

Creación de un informe personalizado

Puede modificar informes predefinidos con parámetros personalizados en IBM Spectrum Protect Plus y guardar los informes personalizados.

Procedimiento

Para crear un informe, realice los pasos siguientes:

1. En el panel de navegación, pulse **Informes y registros** > **Informes**.
2. Seleccione un informe predefinido.
3. Establezca los parámetros personalizados.
4. Defina el informe para que se ejecute en una de las circunstancias siguientes:
   - Ejecute bajo demanda
   - Cree una planificación para ejecutar el informe tal como está define en los parámetros de la planificación.
5. Guarde el informe con un nombre personalizado.

Qué hacer a continuación

Ejecute el informe y revise el informe en el panel **Informes**.

Conceptos relacionados

"Gestión de informes y registros" en la página 295
IBM Spectrum Protect Plus proporciona un número de informes predefinidos que puede personalizar para cumplir los requisitos de creación de informes. También se proporciona un registro de las acciones que los usuarios completan en IBM Spectrum Protect Plus.

Planificación de un informe

Puede planificar informes personalizados en IBM Spectrum Protect Plus para que se ejecuten en momentos específicos.

Procedimiento

Para planificar un informe, realice los pasos siguientes:

1. En el panel de navegación, pulse **Informes y registros** > **Informes**.
2. Seleccione un tipo de informe.
3. Seleccione el informe que desea planificar.
4. Edite los parámetros de informe de la sección **Opciones**,
5. Especifique valores en los campos **Nombre** y **Descripción** para el informe.
6. Establezca los parámetros del informe.
7. En la sección **Planificar informe**, pulse **Definir planificación**.
8. Defina un activador para el informe.
9. Especifique una dirección para recibir el informe planificado en el campo de correo electrónico y, a continuación, pulse **Añadir un destinatario**.
10. Pulse **Guardar**.

Qué hacer a continuación

Después de que se ejecute el informe, el destinatario puede revisar el informe, que se entrega por correo electrónico.

Conceptos relacionados

"Gestión de informes y registros" en la página 295
IBM Spectrum Protect Plus proporciona un número de informes predefinidos que puede personalizar para cumplir los requisitos de creación de informes. También se proporciona un registro de las acciones que los usuarios completan en IBM Spectrum Protect Plus.

Recopilación de registros de auditoría para acciones

Puede recopilar registros de auditoría y buscar las acciones que se han realizado en IBM Spectrum Protect Plus.

Procedimiento

Para recopilar registros de auditoría:

1. En el panel de navegación, pulse **Informes y registros** > **Registros de auditoría**.
2. Revise un registro de las acciones que se han realizado en IBM Spectrum Protect Plus. La información incluye a los usuarios que han realizado las acciones y las descripciones de las acciones.
3. Para buscar las acciones de un usuario específico en IBM Spectrum Protect Plus, escriba el nombre de usuario en el campo de búsqueda de usuario.
4. Opcional: Expanda la sección **Filtros** para filtrar un poco más los registros visualizados. Escriba descripciones específicas para las acciones y un rango de fechas en el que se haya realizado la acción.

5. Pulse el icono de búsqueda .
6. Para descargar el registro de auditoría como un archivo `.csv`, pulse **Descargar** y, a continuación, seleccione una ubicación para guardar el archivo.

Conceptos relacionados

“Gestión de cuentas de usuario” en la página 311

Antes de que un usuario pueda iniciar la sesión en IBM Spectrum Protect Plus y utilizar las funciones disponibles, se debe crear una cuenta de usuario en IBM Spectrum Protect Plus.

Capítulo 13. Gestión del acceso de usuarios

Al utilizar el control de acceso basado en roles, puede establecer los recursos y permisos disponibles en las cuentas de usuario de IBM Spectrum Protect Plus.

Puede adaptar IBM Spectrum Protect Plus para usuarios individuales, otorgándoles acceso a las características y a los recursos que necesitan.

Una vez que los recursos están disponibles para IBM Spectrum Protect Plus, se pueden añadir a un grupo de recursos junto con elementos de IBM Spectrum Protect Plus de alto nivel como, por ejemplo, un hipervisor y pantallas individuales.

A continuación, los roles se configuran para definir las acciones que puede realizar el usuario asociado con el grupo de recursos. A continuación, estas acciones se asocian con una o más cuentas de usuario.

Utilice las secciones siguientes del panel **Cuentas** para configurar el acceso basado en roles:

Grupos de recursos
: Un grupo de recursos define los recursos que están disponibles para un usuario. Cada recurso que se añade a IBM Spectrum Protect Plus se puede incluir en un grupo de recursos, junto con funciones y pantallas de IBM Spectrum Protect Plus individuales. Mediante la definición de grupos de recursos, puede ajustar la experiencia del usuario. Por ejemplo, un grupo de recursos podría incluir un hipervisor individual, con acceso sólo a la funcionalidad de copia de seguridad y creación de informes. Cuando el grupo de recursos está asociado a un rol y a un usuario, el usuario solo verá las pantallas asociadas con la copia de seguridad y la creación de informes para el hipervisor asignado.

Roles
: Los roles definen las acciones que se pueden realizar en los recursos que están definidos en un grupo de recursos. Mientras que un grupo de recursos define los recursos que se van a poner a disposición de una cuenta de usuario, un rol establece los permisos para interactuar con los recursos definidos en el grupo de recursos. Por ejemplo, si se crea un grupo de recursos que incluye trabajos de copia de seguridad y restauración, el rol determina la forma en que un usuario puede interactuar con los trabajos.

  Los permisos se pueden establecer para permitir a un usuario crear, ver y ejecutar los trabajos de copia de seguridad y restauración que están definidos en un grupo de recursos, pero no suprimirlos. De forma similar, se pueden establecer permisos para crear cuentas de administrador, lo que permite a un usuario crear y editar otras cuentas, configurar sitios y recursos e interactuar con todas las funciones de IBM Spectrum Protect Plus disponibles.

Cuentas de usuario
: Una cuenta de usuario asocia un grupo de recursos con un rol. Para permitir que un usuario inicie la sesión en IBM Spectrum Protect Plus y utilice sus funciones, debe añadir primero el usuario como usuario individual (al que se hace referencia como usuario nativo) o como parte de un grupo importado de usuarios de LDAP y, a continuación, asignar grupos de recursos y roles a la cuenta de usuario. La cuenta tendrá acceso a los recursos y a las características que están definidos en el grupo de recursos, así como a los permisos para interactuar con los recursos y las características que se definen en el rol.

Gestión de grupos de recursos de usuario

Un grupo de recursos define los recursos que están disponibles para un usuario. Cada recurso añadido a IBM Spectrum Protect Plus se puede incluir en un grupo de recursos, junto con funciones y pantallas de IBM Spectrum Protect Plus individuales.

Creación de un grupo de recursos

Cree un grupo de recursos para definir los recursos que están disponibles para un usuario.

Antes de empezar

No puede asignar más de una aplicación por máquina como servidor de aplicaciones a un grupo de recursos. Por ejemplo, si SQL y Exchange ocupan la misma máquina y ambos están registrados en SPP, solo uno de ellos puede añadirse como servidor de aplicaciones a un determinado grupo de recursos.

Procedimiento

Para crear un grupo de recursos, siga estos pasos:

1. En el panel de navegación, pulse **Cuentas** > **Grupo de recursos**.
2. Pulse **Crear grupo de recursos**. Se visualiza el panel **Crear grupo de recursos**.
3. Escriba un nombre para el grupo de recursos.
4. En el menú **Me gustaría crear un grupo de recursos**, seleccione una de las opciones siguientes:

Opción	Acciones
Nuevo	a. Seleccione un tipo de recurso en el menú **Elegir un tipo de recurso**. b. Seleccione los subtipos de recursos y, a continuación, pulse **Añadir recursos**. Los recursos se añaden a la vista **Recursos seleccionados**.
Desde plantilla	a. Seleccione un grupo de recursos en la lista **¿Qué grupo de recursos desea utilizar como plantilla?**. Los recursos de la plantilla seleccionada se añaden a la vista **Recursos seleccionados**. b. Puede añadir recursos utilizando la lista **Elegir un tipo de recurso** y las listas asociadas. Para ver los tipos de recursos disponibles y su uso, consulte “Tipos de recursos ” en la página 304.

   Si desea suprimir recursos del grupo, pulse el icono de suprimir que está asociado a un recurso o pulse **Suprimir todo** para suprimir todos los recursos.
5. Cuando haya terminado de añadir recursos, pulse **Crear grupo de recursos**.

Resultados

El grupo de recursos se muestra en la tabla de grupos de recursos y se puede asociar con cuentas de usuario nuevas y existentes.

Qué hacer a continuación

Después de añadir el grupo de recursos, realice la acción siguiente:

Acción	Cómo
Cree roles para definir las acciones que puede realizar la cuenta de usuario que está asociada con el grupo de recursos. Los roles se utilizan para definir permisos para interactuar con los recursos que se definen en el grupo de recursos.	Consulte “Creación de un rol” en la página 308.

Tipos de recursos

Los tipos de permisos se seleccionan cuando se crean grupos de recursos y se determinan los recursos que están disponibles para un usuario asignado a un grupo.

Están disponibles los tipos y subtipos de recursos siguientes:

Tipo de recurso	Subtipo	Descripción
Cuentas	• Rol • Usuario • Identidad	Se utiliza para otorgar acceso a roles y usuarios a través del panel **Cuentas**.
Aplicación	• Db2 • Oracle • SQL - Clúster autónomo/ migración tras error • SQL siempre activado	Sirve para otorgar acceso para ver bases de datos de aplicaciones individuales en un servidor de aplicaciones en IBM Spectrum Protect Plus.
Servidor de aplicaciones	• Db2 • SQL • Oracle	Se utiliza para otorgar acceso a servidores de aplicaciones en IBM Spectrum Protect Plus sin tener acceso a bases de datos individuales.
Hipervisor	• VMware • Hyper-V	Se utiliza para otorgar acceso a recursos del hipervisor.
Trabajo	Ninguno	Se utiliza para otorgar acceso a trabajos de inventario, copia de seguridad y restauración. El grupo de recursos de trabajo es obligatorio para todas las operaciones de copia de seguridad y restauración, incluida la asignación de políticas de SLA a los recursos.
Informe	• Utilización del almacenamiento de copias de seguridad • Protección • Sistema • Entorno de VE	Se utiliza para otorgar acceso a los tipos de informe y a los informes individuales.
Pantalla	Ninguno	Se utiliza para otorgar o denegar el acceso a las pantallas de la interfaz de IBM Spectrum Protect Plus. Si determinadas pantallas no están incluidas en un grupo de recursos para un usuario, el usuario no podrá acceder a la funcionalidad proporcionada en la pantalla, independientemente de los permisos otorgados al usuario.
Política de SLA	Ninguno	Se utiliza para otorgar acceso a políticas SLA para operaciones de copia de seguridad.

Tipo de recurso	Subtipo	Descripción
Sistema	Identidad	Se utiliza para otorgar acceso a las credenciales necesarias para acceder a los recursos. La funcionalidad de la identidad está disponible a través del panel **Sistema** > **Identidad**.
Configuración del sistema	Disco	Se utiliza para otorgar acceso a servidores de almacenamiento de copias de seguridad de vSnap.
Configuración del sistema	LDAP	Se utiliza para otorgar acceso a servidores LDAP para el registro de usuarios.
Configuración del sistema	Registros	Se utiliza para otorgar acceso a la visualización y a la descarga de registros de auditoría y del sistema.
Configuración del sistema	Script	Se utiliza para otorgar acceso a los scripts anteriores y posteriores cargados.
Configuración del sistema	Servidor de script	Se utiliza para otorgar acceso a servidores de scripts, donde los scripts se ejecutan durante un trabajo de copia de seguridad o de restauración.
Configuración del sistema	Sitio	Se utiliza para otorgar acceso a sitios, que se asignan a servidores de almacenamiento de copia de seguridad de vSnap.
Configuración del sistema	SMTP	Se utiliza para otorgar acceso a servidores SMTP para notificaciones de trabajo.
Configuración del sistema	Proxy VADP	Se utiliza para otorgar acceso a servidores proxy VADP.

Edición de un grupo de recursos

Puede editar un grupo de recursos para cambiar los recursos y las características que se han asignado al grupo. Los valores de grupo de recursos actualizados entran en vigor cuando las cuentas de usuario que están asociadas con el grupo de recursos inician la sesión en IBM Spectrum Protect Plus.

Antes de empezar

Tenga en cuenta las consideraciones siguientes antes de editar un grupo de recursos:

- Si ha iniciado sesión cuando se modifican los permisos o los derechos de acceso para la cuenta de usuario, debe cerrar la sesión e iniciarla de nuevo para que los permisos actualizados entren en vigor.
- Puede editar cualquier grupo de recursos que no se haya designado como **No se puede modificar**.

No puede asignar más de una aplicación por máquina como servidor de aplicaciones a un grupo de recursos. Por ejemplo, si SQL y Exchange ocupan la misma máquina y ambos están registrados en SPP, solo uno de ellos puede añadirse como servidor de aplicaciones a un determinado grupo de recursos.

Procedimiento

Para editar un grupo de recursos, complete los pasos siguientes:

1. En el panel de navegación, pulse **Cuentas** > **Grupo de recursos**.
2. Seleccione un grupo de recursos y pulse el icono de opciones ••• del grupo de recursos. Pulse **Modificar recursos**.
3. Revise el nombre del grupo de recursos, los recursos o ambos.
4. Pulse **Actualizar grupo de recursos**.

Supresión de un grupo de recursos

Puede suprimir cualquier grupo de recursos que no esté designado como **No se puede modificar**.

Procedimiento

Para suprimir un grupo de recursos, siga estos pasos:

1. En el panel de navegación, pulse **Cuentas** > **Grupo de recursos**.
2. Seleccione un grupo de recursos y pulse el icono de opciones ••• del grupo de recursos. Pulse **Suprimir grupo de recursos**.
3. Pulse **Si**.

Gestión de roles

Los roles definen las acciones que se pueden completar para los recursos que están definidos en un grupo de recursos. Mientras que un grupo de recursos define los recursos que están disponibles para una cuenta, un rol establece los permisos para interactuar con los recursos.

Por ejemplo, si se crea un grupo de recursos que incluye trabajos de copia de seguridad y restauración, el rol determina la forma en que un usuario puede interactuar con los trabajos. Los permisos se pueden establecer para permitir a un usuario crear, ver y ejecutar los trabajos de copia de seguridad y restauración que están definidos en un grupo de recursos, pero no suprimirlos.

De forma similar, se pueden establecer permisos para crear cuentas de administrador, lo que permite a un usuario crear y editar otras cuentas, configurar sitios y recursos e interactuar con todas las funciones de IBM Spectrum Protect Plus disponibles.

La funcionalidad de un rol depende de un grupo de recursos configurado correctamente. Al seleccionar un rol predefinido o configurar un rol personalizado, debe asegurarse de que el acceso a las operaciones, las pantallas y los recursos de IBM Spectrum Protect Plus esté en consonancia con el uso propuesto del rol.

Están disponibles los roles de cuenta de usuario siguientes:

Administrador de aplicaciones

El rol de administrador de aplicaciones permite a los usuarios completar las acciones siguientes:

- Registrar y modificar recursos de base de datos de aplicaciones que delega un administrador.
- Asociar bases de datos de aplicaciones con políticas de SLA asignadas.
- Completar operaciones de copia de seguridad y restauración.
- Ejecutar y planificar informes a los que el usuario tiene acceso.

Un administrador debe otorgar el acceso a los recursos a través del panel **Cuentas** > **Grupos de recursos**.

Solo copia de seguridad

El rol de solo copia de seguridad permite a los usuarios completar las acciones siguientes:

- Ejecutar, editar y supervisar operaciones de copia de seguridad
- Ver, crear y editar políticas de SLA a las que el usuario tiene acceso

Un administrador debe otorgar acceso a recursos, incluidos trabajos de copia de seguridad específicos pulsando **Cuentas** > **Grupos de recursos**.

Restaurar únicamente
El rol de restaurar únicamente permite a los usuarios completar las acciones siguientes:

- Restauraciones instantáneas a nivel de volumen y VSS completo.
- Ver, crear y editar políticas de SLA a las que el usuario tiene acceso.

Un administrador debe otorgar acceso a recursos, incluidos trabajos de restauración específicos pulsando **Cuentas** > **Grupos de recursos**.

Autoservicio
El rol de autoservicio permite a los usuarios supervisar las operaciones de copia de seguridad y restauración existentes que delega un administrador.

Un administrador debe otorgar acceso a recursos, incluidos trabajos específicos a través del panel **Cuentas** > **Grupos de recursos**.

SYSADMIN
El rol SYSADMIN es el rol de administrador. Este rol proporciona acceso a todos los recursos y privilegios.

Los usuarios con este rol pueden añadir usuarios y llevar a cabo las acciones siguientes para todos los usuarios que no sean el usuario `admin`:

- Modificar y suprimir cuentas de usuario
- Cambiar contraseñas de usuario
- Asignar roles de usuario

Un administrador también puede acceder a la consola de administración seleccionando **IBM Spectrum Protect Plus** en la lista **Tipo de autenticación** en la ventana de inicio de sesión de la consola y especificando las credenciales de administrador.

Desde la consola de administración, el administrador puede aplicar actualizaciones de software, reiniciar el dispositivo de IBM Spectrum Protect Plus y establecer el huso horario local.

Para obtener más información sobre el uso de la consola de administración, consulte "Inicio de sesión en la consola de administración" en la página 284.

VM Admin
El rol de VM Admin permite a los usuarios completar las acciones siguientes:

- Registrar y modificar recursos de hipervisor a los que el usuario tiene acceso.
- Asociar hipervisores con políticas de SLA.
- Completar operaciones de copia de seguridad y restauración.
- Ejecutar y planificar informes a los que el usuario tiene acceso.

Un administrador debe otorgar el acceso a los recursos a través del panel **Cuentas** > **Grupos de recursos**.

Creación de un rol

Cree roles para definir las acciones que el usuario de una cuenta que está asociada a un grupo de recursos puede realizar. Los roles se utilizan para definir permisos para interactuar con los recursos que se definen en el grupo de recursos.

Procedimiento

Para crear un rol de usuario, complete los pasos siguientes:

1. En el panel de navegación, pulse **Cuentas** > **Rol**.
2. Pulse **Crear rol**. Se visualiza el panel **Crear rol**.
3. En la lista **Me gustaría crear un rol**, seleccione una de las opciones siguientes:

Opción	Acciones
Nuevo	Seleccione los permisos que desea aplicar al rol. De forma predeterminada, ninguno de los permisos está preseleccionado.
Desde plantilla	a. Seleccione un rol en el menú **¿Qué rol deseo utilizar como plantilla?**. Los permisos que están asociados al rol de plantilla se seleccionan de forma predeterminada. b. Seleccione permisos adicionales para aplicar al rol y suprima los permisos que no sean necesarios. Para ver los permisos disponibles y su uso, consulte "Tipos de permisos " en la página 309.

4. Escriba un nombre para el rol y, a continuación, pulse **Crear rol**.

Resultados
El nuevo rol se visualiza en la tabla de roles y se puede aplicar a las cuentas de usuario nuevas y existentes.

Tipos de permisos
Los tipos de permisos se seleccionan cuando se crean cuentas de usuario y se determinan los permisos que están disponibles para el usuario.

Están disponibles los permisos siguientes:

Nombre	Permisos	Descripción
Aplicación	Ver	Sirve para ver bases de datos de aplicaciones individuales en un servidor de aplicaciones en IBM Spectrum Protect Plus.
Servidor de aplicaciones	Registrar, ver, editar, anular registro	Sirve para interactuar con los servidores de aplicaciones tales como servidores QL u Oracle, sin acceso a bases de datos individuales.
Certificado	Crear, ver, editar, suprimir	Sirve para interactuar con certificados SSL para acceder a servidores de nube.
Nube	Registrar, ver, editar, anular registro	Sirve para interactuar con servidores de nube que están definidos como almacenamiento de copias de seguridad para traspasos de datos.
Hipervisor	Registrar, ver, editar, anular registro, opciones	Sirve para interactuar con máquinas virtuales de hipervisor, tales como máquinas virtuales VMware o Hyper-V.
Identidad y claves	Crear, ver, editar, suprimir	Sirve para interactuar con las credenciales necesarias para acceder a los recursos. La funcionalidad de identidad está disponible mediante el panel Cuentas > Identidades.

Nombre	Permisos	Descripción
LDAP	Registrar, ver, editar, anular registro	Sirve para interactuar con los servidores LDAP para el registro de usuarios.
Registro	Ver	Sirve para ver registros de auditoría y del sistema.
Trabajo	Crear, ver, editar, ejecutar, suprimir	Sirve para interactuar con trabajos de inventario, copia de seguridad y restauración. **Nota:** Si el usuario tiene permiso para **ejecutar** un trabajo, también puede **Retener**, **Liberar** y **Realizar acciones de restauración personalizadas** para el trabajo
Proxy VADP	Registrar, ver, editar, anular registro	Sirve para interactuar con VADP
Informe	Crear, ver, editar, suprimir	Sirve para interactuar con informes.
Grupo de recursos	Crear, ver, editar, suprimir	Sirve para interactuar con grupos de recursos, que definen recursos de IBM Spectrum Protect Plus que están a disposición de un usuario.
Rol	Crear, ver, editar, suprimir	Sirve para interactuar con los roles, que definen las acciones que se pueden realizar sobre los recursos definidos en un grupo de recursos.
Script	Cargar, ver, sustituir, suprimir	Se utiliza para interactuar con scripts anteriores y posteriores que se añaden a IBM Spectrum Protect Plus y se ejecutan antes o después de un trabajo.
Sitio	Crear, ver, editar, suprimir	Sirve para interactuar con sitios, que están asignados a servidores de almacenamiento de copias de seguridad de vSnap.
SMTP	Registrar, ver, editar, anular registro	Sirve para interactuar con los servidores SMTP para las notificaciones de trabajo.
Almacenamiento de copias de seguridad	Registrar, ver, editar, anular registro	Sirve para interactuar con servidores de almacenamiento de copias de seguridad de vSnap.
Política de SLA	Crear, ver, editar, suprimir	Sirve para interactuar con las políticas de SLA, que permiten a los usuarios crear plantillas personalizadas para trabajos de copia de seguridad.

Nombre	Permisos	Descripción
Usuario	Crear, ver, editar, suprimir	Sirve para interactuar con usuarios, que asocian un grupo de recursos con un rol y proporciona acceso a la interfaz de usuario de IBM Spectrum Protect Plus.

Edición de un rol

Puede editar un rol para cambiar los recursos y permisos que se asignan al rol. Los valores de rol actualizados entran en vigor cuando las cuentas de usuario que están asociadas con el rol inician sesión en IBM Spectrum Protect Plus.

Antes de empezar

Tenga en cuenta las siguiente consideraciones antes de editar un rol:

- Si ha iniciado sesión cuando se modifican los permisos o los derechos de acceso para la cuenta de usuario, debe cerrar la sesión e iniciarla de nuevo para que los permisos actualizados entren en vigor.
- Puede editar cualquier rol que no se haya designado como **No se puede modificar**.

Procedimiento

Para editar un rol de usuario, complete los pasos siguientes

1. En el panel de navegación, pulse **Cuentas** > **Rol**.
2. Seleccione un rol y pulse el icono de opciones ••• del rol. Pulse **Modificar rol**.
3. Revise el nombre de rol, los permisos o ambos.
4. Pulse **Actualizar rol**.

Supresión de un rol

Puede suprimir un rol que no esté designado como **No se puede modificar**.

Procedimiento

Para suprimir un rol, siga estos pasos:

1. En el panel de navegación, pulse **Cuentas** > **Rol**.
2. Seleccione un rol y pulse el icono de opciones ••• del rol. Pulse **Suprimir rol**.
3. Pulse **Si**.

Gestión de cuentas de usuario

Antes de que un usuario pueda iniciar la sesión en IBM Spectrum Protect Plus y utilizar las funciones disponibles, se debe crear una cuenta de usuario en IBM Spectrum Protect Plus.

Creación de una cuenta de usuario para un usuario individual

Añada una cuenta para un usuario individual en IBM Spectrum Protect Plus. Si está actualizando desde una versión de IBM Spectrum Protect Plus anterior a la versión 10.1.1, los permisos asignados a los usuarios de la versión anterior se deben reasignar en IBM Spectrum Protect Plus.

Antes de empezar

Si desea utilizar roles y grupos de recursos personalizados, créelos antes de crear un usuario. Consulte “Creación de un grupo de recursos” en la página 303 y “Creación de un rol” en la página 308.

Procedimiento

Para crear una cuenta para un usuario individual, complete los pasos siguientes:

1. En el panel de navegación, pulse **Cuentas** > **Usuario**.
2. Pulse **Añadir usuario**. Se muestra el panel **Añadir usuario**.
3. Pulse **Seleccionar el tipo de usuario o grupo que desea añadir** > **Usuario nuevo individual**.
4. Escriba un nombre y una contraseña para el usuario.
5. En la sección **Asignar rol**, seleccione uno o varios roles para el usuario
6. En la sección **Grupos de permisos**, revise los permisos y los recursos que están disponibles para el usuario y, a continuación, pulse **Continuar**.
7. En la sección **Añadir usuarios - Asignar recursos**, asigne uno o varios grupos de recursos al usuario y, a continuación, pulse **Añadir recursos**.

   Los grupos de recursos se añaden a la sección **Recursos seleccionados**.
8. Pulse **Crear usuario**.

Resultados

La cuenta de usuario se muestra en la tabla de usuarios. Seleccione un usuario de la tabla para ver los roles, los permisos y los grupos de recursos disponibles.

Creación de una cuenta de usuario para un grupo LDAP

Añada una cuenta de usuario para un grupo de LDAP a IBM Spectrum Protect Plus.

Antes de empezar

Revise los procedimientos siguientes antes de crear una cuenta de usuario para un grupo LDAP:

- Registre un proveedor de LDAP en IBM Spectrum Protect Plus. Consulte “Adición de un servidor LDAP” en la página 280.
- Si desea utilizar roles y grupos de recursos personalizados, créelos antes de crear un usuario. Consulte “Creación de un grupo de recursos” en la página 303 y “Creación de un rol” en la página 308.

Procedimiento

Complete los pasos siguientes para crear una cuenta de usuario para un grupo LDAP:

1. En el panel de navegación, pulse **Cuentas** > **Usuario**.
2. Pulse **Añadir usuario**. Se muestra el panel **Añadir usuario**.
3. Pulse **Seleccionar el tipo de usuario o grupo que desea añadir** > **Grupo LDAP**.
4. Seleccione un grupo de LDAP.
5. En la sección **Asignar rol**, seleccione uno o varios roles para el usuario
6. En la sección **Grupos de permisos**, revise los permisos y los recursos que están disponibles para el usuario y, a continuación, pulse **Continuar**.
7. En la sección **Añadir usuarios - Asignar recursos**, asigne uno o varios grupos de recursos al usuario y, a continuación, pulse **Añadir recursos**.

   Los grupos de recursos se añaden a la sección **Recursos seleccionados**.
8. Pulse **Crear usuario**.

Resultados

La cuenta de usuario se muestra en la tabla de usuarios. Seleccione un usuario de la tabla para ver los roles, los permisos y los grupos de recursos disponibles.

Edición de una cuenta de usuario

Puede editar el nombre de usuario, la contraseña, los grupos de recursos asociados y los roles de una cuenta de usuario, salvo los usuarios a los que se les asigna el rol SUPERUSER. Si un usuario es un miembro del rol SUPERUSER, solo puede cambiar la contraseña del usuario.

Antes de empezar

Si ha iniciado sesión cuando se modifican los permisos o los derechos de acceso para la cuenta de usuario, debe cerrar la sesión e iniciarla de nuevo para que los permisos actualizados entren en vigor.

Procedimiento

Complete los pasos siguientes para editar las credenciales de una cuenta de usuario:

1. En el panel de navegación, pulse **Cuentas** > **Usuario**.
2. Seleccione uno o varios usuarios. Si selecciona varios usuarios con roles diferentes, solo puede modificar sus recursos y no sus roles.
3. Pulse el icono de opciones ••• para ver las opciones disponibles. Las opciones que se muestran dependen del usuario o los usuarios seleccionados.

   Modificar valores
   Edite el nombre de usuario y la contraseña, los roles asociados y los grupos de recursos.

   Modificar recursos
   Edite los grupos de recursos asociados.
4. Modifique los valores del usuario y, a continuación, pulse **Actualizar usuario** o **Asignar recursos**.

Supresión de una cuenta de usuario

Puede suprimir cualquier cuenta de usuario, salvo los usuarios a quienes se les asigna el rol SUPERUSER.

Procedimiento

Para suprimir una cuenta de usuario, complete los pasos siguientes:

1. En el panel de navegación, pulse **Cuentas** > **Usuario**.
2. Seleccione un usuario.
3. Pulse el icono de opciones ••• y, a continuación, pulse **Suprimir usuario**.

Gestión de identidades

Algunas características de IBM Spectrum Protect Plus requieren credenciales para acceder a los recursos. Por ejemplo, IBM Spectrum Protect Plus se conecta a servidores de Oracle como usuario del sistema operativo local que se especifica durante el registro para completar tareas como la catalogación, la protección de datos y la restauración de datos.

Los nombres de usuario y las contraseñas de los recursos se pueden añadir y editar a través del panel **Identidad**. A continuación, cuando se utiliza una característica en IBM Spectrum Protect Plus que requiere credenciales para acceder a un recurso, seleccione **Utilizar usuario existente** y seleccione una identidad en el menú desplegable.

Adición de una identidad

Añada una identidad para proporcionar las credenciales de usuario.

Procedimiento

Para añadir una identidad, realice los pasos siguientes:

1. En el panel de navegación, pulse **Cuentas** > **Identidad**.

2. Pulse **Añadir identidad**.
3. Complete los campos en el panel **Propiedades de identidad**:

   Nombre

   Especifique un nombre significativo para ayudar a identificar la identidad.

   Nombre de usuario

   Especifique el nombre de usuario que está asociado a un recurso como, por ejemplo, un servidor SQL u Oracle.

   Contraseña

   Especifique la contraseña que está asociada a un recurso.
4. Pulse **Guardar**.

   La identidad se visualiza en la tabla de identidades y se puede seleccionar cuando se utiliza una característica que requiere credenciales para acceder a un recurso a través de la opción **Utilizar usuario existente**.

Edición de una identidad

Puede revisar una identidad para cambiar el nombre de usuario y la contraseña que se utilizan para acceder a un recurso asociado.

Procedimiento

Para editar una identidad, realice los pasos siguientes:

1. En el panel de navegación, pulse **Cuentas** > **Identidad**.
2. Pulse el icono de edición que está asociado a una identidad.

   Se muestra el panel **Identificar propiedades**.
3. Revise el nombre de identidad, el nombre de usuario y la contraseña.
4. Pulse **Guardar**.

   La identidad revisada se muestra en la tabla de identidades y se puede seleccionar cuando se utiliza una característica que requiere credenciales para acceder a un recurso a través de la opción **Utilizar usuario existente**.

Supresión de una identidad

Puede suprimir una identidad cuando esté obsoleta. Si una identidad está asociada a un servidor de aplicaciones registrado, debe eliminarse del servidor de aplicaciones para que se pueda suprimir. Para eliminar la asociación, vaya a la página **Copia de seguridad** > **Gestionar servidores de aplicaciones** asociada con el tipo de servidor de aplicaciones y, a continuación, edite los valores del servidor de aplicaciones.

Procedimiento

Para suprimir una identidad, complete los pasos siguientes:

1. En el panel de navegación, pulse **Cuentas** > **Identidad**.
2. Pulse el icono de suprimir que está asociado a una identidad.
3. Pulse **Sí** para suprimir la identidad.

Capítulo 14. Licencia

De forma predeterminada en IBM Spectrum Protect Plus la auditoría de la licencia está habilitada para determinar si el uso actual está dentro de los niveles de titularidad de la licencia y para impedir posibles incumplimientos en la misma.

IBM Spectrum Protect Plus genera registros de auditoría de titularidad como archivos IBM® Software License Metric Tag (`.slmtag`). A continuación, IBM® License Metric Tool (ILMT) se utiliza para convertir el archivo y generar License Consumption Reports. Utilice la información de esta sección para interpretar los archivos `.slmtag`.

Etiquetas SLM (Software License Metric)

IBM Spectrum Protect Plus genera registros de auditoría de titularidad como archivos IBM® Software License Metric Tag (`.slmtag`). A continuación, IBM® License Metric Tool (ILMT) se utiliza para convertir el archivo y generar License Consumption Reports. Utilice la información proporcionada para interpretar los archivos `.slmtag`.

Los archivos `.slmtag` pueden almacenar información de hasta un tamaño máximo de archivo de 1 MB, tras el cual se archiva el archivo y se crea un nuevo archivo de registro. Se conserva un máximo de 10 archivos de registro.

Requisitos de actualización: Si va a actualizar a IBM Spectrum Protect Plus 10.1.3 desde un release anterior, debe ejecutar el trabajo de mantenimiento para generar los archivos `.slmtag`. Para actualizaciones futuras, debe ejecutar el trabajo de mantenimiento para actualizar los archivos `.slmtag` existentes.

Formato de registro

Los archivos `.slmtag` se almacenan en formato XML y los nuevos registros de métrica se añaden al final del archivo.

A continuación se muestra un ejemplo de archivo `.slmtag`:

```
<SchemaVersion>2.1.1</SchemaVersion>
<SoftwareIdentity>
   <SoftwareIdentity name>"IBM Spectrum Protect Plus"</Name>
   <InstanceId>/opt/virgo</InstanceId>
</SoftwareIdentity>
<Metric logTime ="2018-11-05T16:05:09+00:00">
   <Type>HYPERVISOR_SERVER_COUNT</Type>
   <SubType>HYPERVISOR_SERVER_COUNT</SubType>
   <Value>0</Value>
   <Period>
    <StartTime>2018-11-05T16:05:09+00:00</StartTime>
    <EndTime>2018-11-05T16:05:09+00:00</EndTime>
   </Period>
</Metric>
<Metric logTime="2018-11-05T16:05:09+00:00">
   <Type>APPLICATION_INSTANCE_COUNT</Type>
   <SubType>APPLICATION_INSTANCE_COUNT</SubType>
   <Value>0</Value>
   <Period>
    <StartTime>2018-11-05T16:05:09+00:00</StartTime>
    <EndTime>2018-11-05T16:05:09+00:00</EndTime>
   </Period>
</Metric>
```

donde el elemento `Value` muestra el número de hosts en todos los grupos de recursos con paquetes desplegados para un grupo de instancias, en el momento especificado en el elemento `EndTime`.

El archivo crece a lo largo del tiempo y se puede editar para eliminar elementos de medida más antiguos. Asegúrese de mantener los elementos lo suficientemente granes para la exploración de ILMT; la frecuencia de exploración la determina el administrador de ILMT, pero en general debe ser suficiente para mantener los elementos durante un mes.

Ubicación de registro

El archivo `.slmtag` se encuentra en el directorio /data/slmtag.

Conceptos relacionados

"Tipos de trabajo" en la página 257
Los trabajos se utilizan para ejecutar operaciones de copia de seguridad, restauración, mantenimiento e inventario en IBM Spectrum Protect Plus.

Tareas relacionadas

"Inicio de trabajos" en la página 258
Puede ejecutar cualquier trabajo bajo demanda, incluso si el trabajo se ha establecido para que se ejecute en una planificación.

Integración con IBM License Metric Tool (ILMT)

Utilice IBM License Metric Tool (ILMT) para determinar si el entorno del sistema es compatible con los requisitos de licencia.

ILMT proporciona características útiles para gestionar entornos virtualizados y medir la utilización de licencias. ILMT descubre el software que está instalado en la infraestructura, le ayuda a analizar los datos de consumo y le permite generar informes de auditoría. Cada informe le proporciona información diferente sobre la infraestructura, tal como los grupos de sistemas, instalaciones de software y el contenido del catálogo de software.

De forma predeterminada, cada informe de auditoría de ILMT presenta datos de los últimos 90 días. Existe la posibilidad de personalizar el tipo y la cantidad de información visualizada en un informe con la ayuda de filtros así como guardar los valores de personalizados para un uso posterior. También puede exportar los informes a formato .csv o .pdf y planificar los correos electrónicos de los informes de forma que los destinatarios sean notificados cuando se produzcan sucesos importantes.

Para obtener más información, consulte la documentación del producto IBM License Metric Tool.

Capítulo 15. Resolución de problemas

Hay procedimientos de resolución de problemas disponibles para el diagnóstico y la resolución de problemas.

Para obtener una lista de los problemas conocidos y las limitaciones para cada release de IBM Spectrum Protect Plus, consulte Nota técnica 2014120.

Recopilación de archivos de registro para la resolución de problemas

Para resolver problemas en la aplicación de IBM Spectrum Protect Plus, puede descargar un archivado de archivos de registro generados por IBM Spectrum Protect Plus.

Procedimiento

Para recopilar archivos de registro para la resolución de problemas, complete los pasos siguientes:

1. Pulse el menú de usuario y, a continuación, pulse **Descargar registros del sistema**.

   Es posible que el proceso de descarga tarde algún tiempo en completarse.
2. Abra o guarde el archivo zip del registro de archivos, que contiene archivos de registro individuales para distintos componentes de IBM Spectrum Protect Plus.

   Para obtener información sobre los archivos de registro, consulte las secciones de copia de seguridad de protección de aplicaciones o protección de hipervisores.

Qué hacer a continuación

Para la resolución de problemas, complete los pasos siguientes:

1. Analice los archivos de registro y emprenda las acciones adecuadas para resolver el problema.
2. Si no puede resolver el problema, envíe los archivos de registro a IBM Software Support para solicitar ayuda.

Capítulo 16. Mensajes del producto

Los componentes de IBM Spectrum Protect Plus envían mensajes con prefijos que permiten identificar el componente del que provienen. Utilice la opción de búsqueda para buscar un determinado mensaje utilizando su identificador exclusivo.

Los mensajes constan de los siguientes elementos:

- Un prefijo de cinco letras.
- Un número para identificar el mensaje.
- Un mensaje de texto que se muestra en pantalla y está escrito en el registro de mensajes.

Consejo: Utilice la funcionalidad de búsqueda del navegador con Ctrl+F para encontrar el código de mensaje que está buscando.

El siguiente ejemplo contiene el prefijo del agente de Db2. Si pulsa Más, se mostrarán detalles adicionales que explican el motivo del mensaje.

```
Warning
Apr 16, 2019
9:14:37 AM
GTGGH0098
[myserver1.myplace.irl.ibm.com]
Database AC7 will not be backed up as it is ineligible for the backup operation. More
```

Prefijos de mensajes de IBM Spectrum Protect Plus

Los mensajes tienen prefijos diferentes para ayudarle a identificar el componente que emite el mensaje.

La tabla siguiente identifica el prefijo que está asociado con cada componente.

Tabla 24. Prefijos de mensaje por componente

Prefijo	**Componente**
CTGGA	IBM Spectrum Protect Plus
CTGGE	IBM Spectrum Protect Plus for Microsoft SQL Server
CTGGF	IBM Spectrum Protect Plus para Oracle
CTGGG	IBM Spectrum Protect Plus for Microsoft Exchange Server
CTGGH	IBM Spectrum Protect Plus para IBM Db2
CTGGI	IBM Spectrum Protect Plus para MongoDB

Para ver una lista de los mensajes, consulte el IBM Knowledge Centre aquí.

Apéndice A. Directrices de búsqueda

Utilice filtros para buscar una entidad como, por ejemplo, un archivo o un punto de restauración.

Puede especificar una serie de caracteres para buscar objetos con un nombre que coincida exactamente con la serie de caracteres. Por ejemplo, la búsqueda del término `string.txt` devuelve la coincidencia exacta, `string.txt`.

Las entradas de búsqueda de expresiones regulares también están soportadas. Para obtener más información, consulte Buscar texto con expresiones regulares.

También puede incluir los siguientes caracteres especiales en la búsqueda. Debe utilizar un carácter de escape de barra inclinada invertida (\) antes de cualquier carácter especial:

```
+ - & | ! ( ) { } [ ] ^ " ~ * ? : \
```

Por ejemplo, para buscar el archivo `string[2].txt`, entre `string\[2\].txt`.

Búsqueda con comodines

Puede colocar comodines en el principio, en el medio o en el final de una serie y combinarlos dentro de una serie.

Hacer coincidir una serie de caracteres con un asterisco

Los ejemplos siguientes muestran un texto de búsqueda con un asterisco:

- `seri*` busca términos como serie, series o serial
- `seri*e` busca términos como serie, sericeo o sericea
- `*serie` busca palabras como serie o multiserie

Puede utilizar varios comodines de asterisco en una sola serie de texto, pero varios comodines pueden ralentizar considerablemente una búsqueda grande.

Hacer coincidir un único carácter con un signo de interrogación:

Los ejemplos siguientes muestran el texto de búsqueda con un signo de interrogación:

- `cadena?` busca términos como cadenas, cadena1, cadena2
- `ca??na` busca términos como cadena, carena
- `???cadena` busca términos como encadena, subcadena

Apéndice B. Características de accesibilidad de la familia de productos IBM Spectrum Protect

Las características de accesibilidad ayudan a los usuarios con discapacidades como, por ejemplo, con movilidad restringida o con visión limitada, de manera que puedan usar el contenido de las tecnologías de la información satisfactoriamente.

Visión general

La familia de productos de IBM Spectrum Protect incluye las siguientes características más importantes de accesibilidad:

- Operación sólo con teclado
- Operaciones que utilizan un lector de pantalla

La familia de productos IBM Spectrum Protect utiliza el último estándar de W3C, WAI-ARIA 1.0 (www.w3.org/TR/wai-aria/), para asegurar el cumplimiento de la US Section 508 (www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/section-508-standards) y las Web Content Accessibility Guidelines (WCAG) 2.0 (www.w3.org/TR/WCAG20/). Para aprovechar las características de accesibilidad, utilice el release más reciente de su lector de pantalla en combinación con el navegador web más reciente que admita este producto.

La documentación del producto en IBM Knowledge Center está habilitada para una correcta accesibilidad. Las características de accesibilidad de IBM Knowledge Center se describen en la sección de accesibilidad de la ayuda de IBM Knowledge Center (www.ibm.com/support/knowledgecenter/about/releasenotes.html?view=kc#accessibility).

Navegación mediante teclado

Este producto utiliza teclas de navegación estándar.

Información sobre las interfaces

Las interfaces de usuario no tiene contenido que parpadee de 2 a 55 veces por segundo.

Las interfaces de usuario web se basan en hojas de estilo en cascada para representar el contenido correctamente y proporcionar una funcionalidad adecuada. La aplicación proporciona una forma equivalente para que los usuarios con problemas de visión utilicen los valores de visualización del sistema, como por ejemplo la modalidad de alto contraste. Puede controlar el tamaño de font utilizando los valores del dispositivo o del navegador web.

Las interfaces web incluyen puntos de referencia de navegación WAI-ARIA que permiten navegar con rapidez a áreas funcionales en la aplicación.

Software de otros proveedores

La familia de productos de IBM Spectrum Protect incluye determinado software de proveedor que no está cubierto bajo el acuerdo de licencia de IBM. IBM no es responsable de las características de accesibilidad de estos productos. Póngase en contacto con el proveedor para obtener información sobre la accesibilidad relacionada con sus productos.

Información de accesibilidad relacionada

Además del centro de atención al cliente y de los sitios web de soporte estándar de IBM, IBM dispone de un servicio telefónico TTY que permite a clientes sordos o con dificultades auditivas acceder a los servicios de ventas y asistencia técnica:

Servicio TTY
800-IBM-3383 (800-426-3383)
(en Norteamérica)

Para obtener más información acerca del compromiso de IBM con la accesibilidad, consulte IBM Accessibility(www.ibm.com/able).

Avisos

Esta información se ha desarrollado para productos y servicios ofrecidos en Estados Unidos. Este material estarán disponibles en IBM en otros idiomas. No obstante, puede que sea necesario ser propietario de una copia del producto o la versión del producto en dicho idioma para poder acceder al mismo.

IBM no proporcionará los productos, servicios o funciones que se tratan en este documento en otros países. Póngase en contacto con su representante local de IBM para obtener más información acerca de los productos y servicios que actualmente están disponibles en su país. Cualquier referencia a un producto, programa o servicio de IBM no significa ni implica que sólo pueda utilizar este determinado producto, programa o servicio de IBM. En su lugar, puede utilizarse cualquier producto, programa o servicio equivalente funcionalmente que no infrinja los derechos de propiedad intelectual de IBM. No obstante, es responsabilidad del usuario evaluar y verificar el funcionamiento de cualquier producto, programa o servicio que no sea de IBM.

IBM puede tener patentes o solicitudes de patente pendientes que cubran el tema central tratado en este documento. La entrega de este documento no le otorga ninguna licencia sobre dichas patentes. Puede enviar las consultas sobre licencias, por escrito, a la siguiente dirección:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
EE.UU.

Para consultas sobre licencias relativas a la información del conjunto de caracteres de doble byte (DBCS), póngase en contacto con el departamento de propiedad intelectual de IBM en su país o envíe las consultas, por escrito, a:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokio 103-8510, Japón

INTERNATIONAL BUSINESS MACHINES CORPORATION PROPORCIONA ESTA PUBLICACIÓN "TAL CUAL" SIN GARANTÍA DE NINGUNA CLASE, NI EXPRESA NI IMPLÍCITA, INCLUIDAS, PERO NO LIMITADAS A LAS GARANTÍAS IMPLÍCITAS DE NO CUMPLIMIENTO, COMERCIALIZACIÓN O IDONEIDAD PARA UNA FINALIDAD DETERMINADA. Algunas jurisdicciones no permiten la renuncia a las garantías explícitas o implícitas en determinadas transacciones; por lo tanto, es posible que esta declaración no sea aplicable en su caso.

Esta información puede contener imprecisiones técnicas o errores tipográficos. La información de este documento está sometida a modificaciones periódicas, las cuales se incorporarán en nuevas ediciones de la publicación. IBM se reserva el derecho a realizar en cualquier momento y sin notificación previa, mejoras o modificaciones en los productos y programas que se describen en el presente manual.

Todas las referencias hechas en este documento a sitios web que no son de IBM se proporcionan únicamente a título informativo y no representan en modo alguno una recomendación de dichos sitios web. Los materiales proporcionados en dichos sitios web no forman parte de los materiales de este producto de IBM y la utilización de esos sitios web será responsabilidad del usuario.

IBM puede utilizar o distribuir la información que se le proporcione, en la forma que crea conveniente, sin incurrir por ello en ninguna obligación con el remitente.

Los poseedores de licencias de este programa que deseen obtener información sobre éste a efectos de permitir: (i) el intercambio de información entre programas creados de forma independiente y otros

programas (incluido éste) y (ii) el uso mutuo de la información intercambiada, deben ponerse en contacto con:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
EE.UU.

Esta información puede estar disponible, sujeta a las condiciones y los términos apropiados, incluido en ciertos casos el pago de una cuota.

El programa bajo licencia descrito en este documento y todo el material bajo licencia disponible para él mismo los proporciona IBM de acuerdo con los términos del Acuerdo de Cliente de IBM, el Acuerdo Internacional de Programa bajo Licencia de IBM o cualquier acuerdo equivalente entre las partes.

Los datos de rendimiento aquí comentados se presentan como derivados bajo condiciones de operación específicas. Los resultados reales pueden variar.

La información relativa a productos que no son de IBM se ha obtenido de los proveedores de dichos productos, de sus anuncios publicados o de otras fuentes disponibles públicamente. IBM no ha realizado pruebas de estos productos y no puede confirmar la exactitud de la información con respecto a su rendimiento, compatibilidad u otros aspectos relacionados con los productos que no sean de IBM. Las preguntas relacionadas con las funcionalidades de los productos que no son de IBM deberán dirigirse a los proveedores de estos productos.

Esta información contiene ejemplos de datos e informes utilizados en operaciones comerciales cotidianas. Para ilustrarlos de la forma más completa posible, se han utilizado nombres de personas, empresas, marcas y productos. Todos estos nombres son ficticios y cualquier parecido con nombres y direcciones de una empresa real es pura coincidencia.

Marcas registradas

el logotipo de IBM, el logotipo de IBM, e ibm.com son marcas o marcas registradas de International Business Machines Corp., registradas en muchas jurisdicciones de todo el mundo. Otros nombres de producto y servicio podrían ser marcas registradas de IBM u otras empresas. Existe una lista actualizada de marcas registradas de IBM en el sitio web "Copyright and trademark information" (Información de copyright y marcas registradas) en www.ibm.com/legal/copytrade.shtml.

Adobe es una marca registrada de Adobe Systems Incorporated en Estados Unidos, en otros países o en ambos.

Linear Tape-Open, LTO y Ultrium son marcas registradas de HP, IBM Corp. y Quantum en EE.UU. y en otros países.

Intel e Itanium son marcas registradas de Intel Corporation o sus empresas filiales en Estados Unidos y otros países.

Linux es una marca registrada de Linus Torvalds en Estados Unidos y en otros países.

Microsoft, Windows y Windows NT son marcas registradas de Microsoft Corporation en Estados Unidos y/o en otros países.

Java y todas las marcas registradas y logotipos basados en Java son marcas comerciales o marcas registradas de Oracle y/o sus afiliados.

UNIX es una marca registrada de The Open Group en Estados Unidos y en otros países.

VMware, VMware vCenter Server y VMware vSphere son marcas registradas o marcas comerciales de VMware, Inc. o de sus empresas filiales en Estados Unidos o en otras jurisdicciones.

Términos y condiciones de la documentación del producto

Los permisos para la utilización de estas publicaciones se otorgan bajo cumplimiento de los siguientes términos y condiciones.

Aplicabilidad
Estos términos y condiciones se añaden a los términos de utilización del sitio web de IBM.

Uso personal
Puede reproducir estas publicaciones para su uso personal, no comercial, siempre y cuando se conserven todos los avisos de propiedad. Queda prohibida la distribución, exposición o realización de trabajos derivados de estas publicaciones, o de cualquier parte de las mismas, sin el consentimiento expreso de IBM.

Uso comercial
Puede reproducir, distribuir y mostrar estas publicaciones únicamente dentro de su empresa, siempre que se conserven todos los avisos sobre derechos de propiedad. No es posible generar ningún documento derivado de estas publicaciones, ni reproducir, distribuir ni visualizar estas publicaciones, ni en parte ni en su totalidad, fuera de la empresa sin el consentimiento expreso de IBM.

Derechos
Exceptuando el caso en el que este permiso se entrega expresamente, no se ofrecen otros permisos, licencias ni derechos, ni de forma expresa o implicada, para las publicaciones ni ninguna información, datos, software ni otros elementos de propiedad intelectual que contengan.

IBM se reserva el derecho de retirar los permisos que se hayan proporcionado siempre que, bajo su discreción, el uso de las publicaciones sea perjudicial para sus intereses o, según determine IBM, no se estén siguiendo adecuadamente las instrucciones detalladas anteriormente.

No podrá descargar, exportar o volver a exportar esta información si no se cumplen completamente todas las leyes y regulaciones aplicables, incluidas las leyes y regulaciones de exportación de los Estados Unidos.

IBM NO GARANTIZA EL CONTENIDO DE ESTAS PUBLICACIONES. LAS PUBLICACIONES SE PROPORCIONAN "TAL CUAL", SIN GARANTÍA DE NINGUNA CLASE, NI EXPLÍCITA NI IMPLÍCITA, QUE INCLUYE, PERO NO SE LIMITA A, LAS GARANTÍAS DE MERCANTIBILIDAD, NO VULNERACIÓN Y ADECUACIÓN A UN FIN DETERMINADO.

Consideraciones sobre la política de privacidad

Los productos de IBM Software, incluido el software como soluciones de servicio, (“Ofertas de software”) pueden utilizar cookies u otras tecnologías para recopilar información de uso del producto, para ayudar a mejorar la experiencia del usuario final, para adaptar las interacciones con el usuario final o para otros fines. En muchos casos, las Ofertas de software no recopilan información de identificación personal. Algunas de nuestras ofertas de software pueden ayudarle a recopilar información de identificación

personal. Si esta oferta de software utiliza cookies para recopilar información de identificación personal, la información específica sobre la utilización de cookies de esta oferta se expone más adelante.

Esta oferta de software no utiliza cookies u otras tecnologías para recopilar información de identificación personal.

Si las configuraciones desplegadas para esta Oferta de software le ofrecen como cliente la posibilidad de recopilar información de identificación personal de los usuarios finales mediante cookies y otras tecnologías, debe buscar asesoramiento legal sobre las leyes aplicables a dicha recopilación de datos, incluidos los requisitos de aviso y consentimiento.

Para obtener más información sobre el uso de las distintas tecnologías, incluidas las cookies, para estos fines, consulte la Política de privacidad de IBM en http://www.ibm.com/privacy y la Política de privacidad de IBM en http://www.ibm.com/privacy/details en la sección "Cookies, Web Beacons and Other Technologies", e "IBM Software Products and Software-as-a-Service Privacy Statement" en http://www.ibm.com/software/info/product-privacy.

Glosario

Está disponible un glosario con términos y definiciones para la familia de productos de IBM Spectrum Protect.

Consulte el Glosario de IBM Spectrum Protect.

Índice

H

I

K

L

M

N

O

P

R

S

T

U

V

W

Impreso en EE.UU.