

IBM Spectrum Protect Plus  
Versión 10.1.6

*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 571](#).

**Tercera edición (26 de junio de 2020)**

Esta edición se aplica a la versión 10, release 1, modificación 6 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.

© Copyright International Business Machines Corporation 2017, 2020.

---

# Contenido

<b>Acerca de esta publicación.....</b>	<b>ix</b>
A quién va dirigida esta publicación.....	ix
Publicaciones .....	ix
<b>Novedades de la Versión 10.1.6.....</b>	<b>xi</b>
<b>Cómo implicarse en el desarrollo del producto.....</b>	<b>xiii</b>
Programa de usuario patrocinador.....	xiii
Programa beta.....	xiii
<b>Capítulo 1. Visión general del producto.....</b>	<b>1</b>
Storyboard de despliegue.....	1
Componentes del producto.....	6
Panel de instrumentos del producto.....	8
Alertas.....	10
Control de acceso basado en roles.....	11
Replicar datos de almacenamiento de copia de seguridad.....	11
Copiar instantáneas en almacenamiento de copias de seguridad secundario.....	12
IBM Spectrum Protect Plus on IBM Cloud.....	14
IBM Spectrum Protect Plus on AWS.....	15
Integración con IBM Spectrum Protect.....	16
Adición de IBM Spectrum Protect Plus al Centro de operaciones.....	17
Introducción del URL del Centro de operaciones.....	19
Acceso al Centro de operaciones.....	20
<b>Capítulo 2. Instalación de IBM Spectrum Protect Plus.....</b>	<b>23</b>
Hoja de ruta de despliegue del producto.....	23
Requisitos del sistema .....	23
Requisitos de los componentes .....	23
Requisitos de hipervisor y de instancia en la nube .....	41
Requisitos de indexación y restauración de archivos.....	44
Requisitos de Sistema de archivos.....	51
Requisitos de Soporte de copia de seguridad de Kubernetes.....	56
Requisitos de Db2.....	62
Requisitos de Microsoft Exchange Server.....	68
Requisitos de MongoDB.....	74
Requisitos de Office 365.....	80
Requisitos de Oracle.....	85
Requisitos de Microsoft SQL Server.....	93
Obtención del paquete de instalación de IBM Spectrum Protect Plus.....	102
Instalación de IBM Spectrum Protect Plus como un dispositivo virtual VMware.....	103
Instalación de IBM Spectrum Protect Plus como un dispositivo virtual Hyper-V.....	105
Asignación de una dirección IP estática.....	107
Carga de la clave de producto.....	107
Edición de puertos de cortafuegos.....	108
Instalación de los programas de utilidad de iniciador iSCSI.....	110
<b>Capítulo 3. Instalación de servidores vSnap.....</b>	<b>111</b>
Instalación de un servidor vSnap.....	111
Instalación de un servidor vSnap físico.....	111

Instalación de un servidor virtual vSnap en un entorno VMware.....	112
Instalación de un servidor virtual vSnap en un entorno Hyper-V.....	114
Desinstalación de un servidor vSnap.....	115
<b>Capítulo 4. Gestión de servidores vSnap.....</b>	<b>117</b>
Registro de un servidor vSnap.....	117
Edición de valores para un servidor vSnap.....	118
Configuración de las opciones de almacenamiento de copias de seguridad.....	120
¿Cómo puedo eliminar y volver a crear una agrupación de almacenamiento de vSnap?.....	126
Inicialización del servidor vSnap.....	128
Finalización de una inicialización simple.....	129
Finalización de una inicialización avanzada.....	129
Expansión de una agrupación de almacenamiento de vSnap.....	130
Cambio de la tasa de rendimiento.....	130
Sustitución de un servidor vSnap que falla.....	131
Referencia de administración del servidor vSnap .....	131
Gestión de usuarios.....	132
Gestión de almacenamiento.....	133
Gestión de red.....	136
Herramientas y cabeceras de kernel.....	137
Resolución de problemas de servidores vSnap.....	138
Sincronización de la contraseña de vSnap.....	138
¿Por qué el servidor vSnap sigue fuera de línea?.....	138
¿Cómo puedo reparar un servidor vSnap fallido en mi entorno de IBM Spectrum Protect Plus?...	138
¿Cómo reparo un vSnap de origen que ha fallado en un entorno de IBM Spectrum Protect Plus?	139
¿Cómo reparo un vSnap de destino que ha fallado en un entorno de IBM Spectrum Protect Plus? .....	143
¿Cómo puedo reparar un vSnap de rol dual que ha fallado en un entorno de IBM Spectrum Protect Plus?.....	147
<b>Capítulo 5. Instalación de Soporte de copia de seguridad de Kubernetes.....</b>	<b>153</b>
Requisitos previos.....	153
Instalación y despliegue de imágenes en Kubernetes.....	156
Desinstalación de Soporte de copia de seguridad de Kubernetes.....	162
<b>Capítulo 6. Empezar con un inicio rápido.....</b>	<b>165</b>
Iniciar IBM Spectrum Protect Plus.....	167
Sitios de gestión.....	168
Crear políticas de copia de seguridad.....	169
Crear una cuenta de usuario para el administrador de aplicaciones.....	172
Añadir recursos para proteger.....	174
Añadir recursos a una definición de trabajo.....	176
Iniciar un trabajo de copia de seguridad.....	178
Ejecutar un informe.....	179
<b>Capítulo 7. Actualización de componentes de IBM Spectrum Protect Plus.....</b>	<b>181</b>
Gestión de actualizaciones.....	181
Actualización de servidores vSnap.....	184
Actualización del sistema operativo para un servidor vSnap físico.....	185
Actualización del sistema operativo para un servidor vSnap virtual.....	185
Actualización de un servidor vSnap.....	186
Actualización del dispositivo virtual de IBM Spectrum Protect Plus.....	187
Pasos adicionales para actualizar máquinas virtuales en entornos de Hyper-V Replica.....	188
Actualización de proxies VADP.....	189
Aplicación de actualizaciones de disponibilidad anticipada.....	190
<b>Capítulo 8. Configuración del entorno del sistema.....</b>	<b>191</b>

Gestión del almacenamiento de copia de seguridad secundario.....	191
Gestión del almacenamiento en la nube.....	191
Gestión del almacenamiento del servidor de repositorio.....	198
Gestión de sitios.....	213
Adición de un sitio.....	213
Edición de un sitio.....	214
Supresión de un sitio.....	215
Gestión de servidores LDAP y SMTP.....	216
Adición de un servidor LDAP.....	216
Adición de un servidor SMTP.....	217
Edición de valores de un servidor LDAP o SMTP.....	218
Supresión de un servidor LDAP o SMTP.....	219
Inicio de sesión en la consola de administración.....	219
Gestión de claves y certificados.....	220
Adición de una clave de acceso.....	220
Supresión de una clave de acceso.....	220
Adición de un certificado.....	221
Supresión de un certificado.....	221
Adición de una clave SSH.....	221
Supresión de una clave SSH.....	223
Carga de un certificado SSL desde la consola de administración.....	223
Establecimiento del huso horario.....	224
Inicio de sesión en el dispositivo virtual.....	225
Acceso al dispositivo virtual en VMware.....	225
Acceso al dispositivo virtual en Hyper-V.....	226
Cómo probar la conectividad de red.....	226
Ejecución de la herramienta de servicio desde una línea de mandatos.....	226
Ejecución remota de la herramienta de servicio.....	227
Adición de discos virtuales.....	228
Adición de un disco al dispositivo virtual.....	228
Adición de capacidad de almacenamiento de un nuevo disco al volumen de dispositivo.....	229
Configuración de las preferencias globales.....	232
Eliminación del entorno de demostración.....	238

## **Capítulo 9. Gestión de políticas de SLA para operaciones de seguridad..... 241**

Resumen de protección.....	241
Creación de una política de SLA para hipervisores, bases de datos y sistemas de archivos.....	244
Creación de una política de SLA para instancias de Amazon EC2.....	248
Creación de una política de SLA para clústeres Kubernetes.....	250
Edición de una política de SLA.....	255
Supresión de una política de SLA.....	255

## **Capítulo 10. Protección de sistemas virtualizados..... 257**

VMware.....	257
Adición de una instancia de vCenter Server.....	257
Copia de seguridad de datos de VMware.....	262
Gestión de proxies de copias de seguridad VADP.....	267
Restauración de datos de VMware.....	273
Hyper-V.....	284
Adición de un servidor Hyper-V.....	284
Copia de seguridad de datos de Hyper-V.....	286
Restauración de datos de Hyper-V.....	290
Amazon EC2.....	297
Creación de un usuario de IAM de AWS.....	298
Adición de una cuenta de Amazon EC2.....	299
Copia de seguridad de datos de Amazon EC2.....	300
Restauración de datos de Amazon EC2.....	302

Restauración de archivos.....	305
<b>Capítulo 11. Protección de sistemas de archivos.....</b>	<b>309</b>
Windows sistemas de archivos.....	309
Requisitos previos para sistemas de archivos.....	309
Adición de un sistema de archivos.....	310
Copia de seguridad de datos del sistema de archivos.....	314
Restauración de datos de sistema de archivos .....	321
<b>Capítulo 12. Protección de contenedores.....</b>	<b>329</b>
Visión general.....	329
Tipos de copia de seguridad y restauración.....	330
Políticas de SLA.....	331
Roles de usuario.....	332
Características de seguridad.....	333
Protección de clústeres Kubernetes utilizando la interfaz de usuario.....	334
Registro de un clúster Kubernetes.....	335
Definición de trabajos de copia de seguridad del acuerdo de nivel de servicio.....	338
Restauración de datos de contenedor.....	341
Caducidad de las sesiones de trabajo de Kubernetes.....	344
Visualización de trabajos y ejecución de informes.....	345
Protección de contenedores utilizando mandatos.....	348
Solicitudes de Soporte de copia de seguridad de Kubernetes.....	348
Copia de seguridad de contenedores utilizando la línea de mandatos.....	350
Restauración de datos de contenedor utilizando la línea de mandatos.....	360
Gestión de trabajos de copia de seguridad y restauración de contenedor.....	363
<b>Capítulo 13. Protección de sistemas de gestión en nube.....</b>	<b>369</b>
Microsoft Office 365.....	369
Registro con Azure Active Directory .....	369
Registro del arrendatario de Office 365 con IBM Spectrum Protect Plus.....	370
Registros de procesos detallados.....	371
Copia de seguridad de datos de Office 365.....	372
Restauración de datos de Office 365.....	373
<b>Capítulo 14. Protección de bases de datos.....</b>	<b>375</b>
Db2.....	375
Requisitos previos para Db2.....	375
Adición de un servidor de aplicaciones de Db2.....	378
Copia de seguridad de datos de Db2.....	382
Restauración de datos de Db2 .....	389
Exchange Server.....	403
Requisitos previos.....	403
Privilegios .....	403
Adición de un servidor de aplicaciones de Exchange.....	405
Copia de seguridad de bases de datos de Exchange.....	407
Estrategia de copia de seguridad incremental para siempre.....	410
Restauración de bases de datos de Exchange.....	411
Acceso a archivos de base de datos de Exchange con la modalidad de acceso instantáneo.....	443
MongoDB.....	446
Requisitos previos para MongoDB.....	446
Adición de un servidor de aplicaciones de MongoDB.....	449
Copia de seguridad de datos de MongoDB.....	454
Restauración de datos de MongoDB .....	458
Oracle.....	476
Adición de un servidor de aplicaciones Oracle.....	476
Copia de seguridad de datos de Oracle.....	478

Restauración de datos de Oracle.....	481
SQL Server.....	488
Adición de un servidor de aplicaciones SQL Server.....	489
Copia de seguridad de datos de SQL Server.....	491
Restauración de datos de SQL Server.....	496
<b>Capítulo 15. Protección de IBM Spectrum Protect Plus.....</b>	<b>505</b>
Copia de seguridad de la aplicación.....	505
Restauración de la aplicación.....	505
Gestión de puntos de restauración.....	506
Caducidad de las sesiones de trabajo.....	507
Supresión de metadatos de recursos del catálogo.....	507
<b>Capítulo 16. Gestión de trabajos y operaciones.....</b>	<b>509</b>
Tipos de trabajo.....	509
Creación de trabajos y planificaciones de trabajos.....	510
Inicio de trabajos bajo demanda.....	512
Visualización de trabajos.....	512
Visualización del progreso del trabajo de copia de seguridad en el nivel de recurso.....	513
Visualización de los registros de trabajo.....	514
Visualización de trabajos simultáneos.....	515
Cómo poner en pausa y reanudar trabajos.....	515
Edición de trabajos y planificaciones de trabajos.....	515
Cancelación de trabajos.....	516
Supresión de trabajos.....	516
Volver a ejecutar trabajos de copia de seguridad parcialmente completados.....	517
Ejecución de un trabajo de copia de seguridad ad hoc.....	517
Configuración de scripts para las operaciones de copia de seguridad y restauración.....	518
Carga de un script.....	519
Adición de un script a un servidor.....	519
<b>Capítulo 17. Gestión de informes y registros.....</b>	<b>521</b>
Tipos de informes.....	521
Informes de utilización de almacenamiento de copia de seguridad.....	521
Informes de protección.....	522
Informes del sistema.....	525
Ejecución de informes de entorno de máquinas virtuales.....	527
Acciones de informes.....	528
Ejecución de un informe.....	528
Creación de un informe personalizado.....	529
Planificación de un informe.....	530
Recopilación y revisión de registros de auditoría para acciones.....	531
<b>Capítulo 18. Gestión del acceso de usuarios.....</b>	<b>533</b>
Gestión de grupos de recursos de usuario.....	534
Creación de un grupo de recursos.....	534
Edición de un grupo de recursos.....	537
Supresión de un grupo de recursos.....	537
Gestión de roles.....	537
Creación de un rol.....	539
Edición de un rol.....	541
Supresión de un rol.....	542
Gestión de cuentas de usuario.....	542
Creación de una cuenta de usuario para un usuario individual.....	542
Creación de una cuenta de usuario para un grupo LDAP.....	543
Edición de las credenciales de la cuenta de usuario.....	543
Supresión de una cuenta de usuario.....	544

Gestión de identidades.....	544
Adición de una identidad.....	544
Edición de una identidad.....	545
Supresión de una identidad.....	545
<b>Capítulo 19. Visión general de la licencia.....</b>	<b>547</b>
Etiquetas SLM (Software License Metric).....	547
Integración con IBM License Metric Tool (ILMT).....	548
<b>Capítulo 20. Resolución de problemas.....</b>	<b>549</b>
Recopilación de archivos de registro para la resolución de problemas.....	549
¿Cómo puedo disponer en niveles los datos en el almacenamiento en la nube o en cintas? .....	549
Resolución de problemas de Soporte de copia de seguridad de Kubernetes.....	550
Recopilación de los archivos de registro de Soporte de copia de seguridad de Kubernetes.....	550
Establecimiento del nivel de rastreo de los archivos de registro.....	551
Visualización de registros de rastreo para Soporte de copia de seguridad de Kubernetes.....	552
Consulta rápida.....	554
Resolución de problemas de copias de seguridad y restauraciones.....	558
<b>Capítulo 21. Mensajes del producto.....</b>	<b>565</b>
Prefijos de mensajes.....	565
<b>Apéndice A. Directrices de búsqueda.....</b>	<b>567</b>
<b>Apéndice B. Accesibilidad.....</b>	<b>569</b>
<b>Avisos.....</b>	<b>571</b>
<b>Glosario.....</b>	<b>575</b>
<b>Índice.....</b>	<b>577</b>



## 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 23](#).

## 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 10.1.6

---

IBM Spectrum Protect Plus Versión 10.1.6 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](#).

Si se han realizado cambios en la documentación, se indican mediante una barra vertical (|) en el margen.



# 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 conseguido adoptar y utilizar el código inicial correctamente.

## **Información de contacto e inscripción**

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 de IBM Spectrum Protect para el almacenamiento de datos a largo plazo.

## Storyboard de despliegue para IBM Spectrum Protect Plus

Este storyboard puede ayudarle a recorrer las tareas necesarias para desplegar el producto. El término *storyboard de despliegue* está diseñado para ayudarle a desplegar correctamente IBM Spectrum Protect Plus en un entorno de producción. El storyboard enumera cada una de las tareas de la secuencia necesaria y proporciona enlaces a instrucciones de tareas, vídeos y directrices en el Blueprints de IBM Spectrum Protect Plus. El storyboard describe el resultado esperado de las tareas para que pueda verificar el progreso cuando despliega el producto.

Antes de empezar, revise los requisitos del sistema para su entorno. Para obtener más información, consulte [“Requisitos del sistema”](#) en la página 23.

Los pasos de la [Tabla 1](#) se basan en la información de [Blueprints](#) y en el funcionamiento de la *herramienta Sizer*. Se proporcionan enlaces de vídeo en la [Tabla 2](#) para ayudarle con estas tareas.

Tabla 1. Storyboard de despliegue		
Historia	Procedimiento	Resultados esperados
Prepare el dimensionamiento de los requisitos de capacidad descargando la hoja de cálculo de Blueprints y de la herramienta Sizer.	<p>Para obtener directrices de dimensionamiento, consulte los capítulos 1-3 de Blueprints de IBM Spectrum Protect Plus.</p> <p>Para obtener ayuda con el uso de la hoja de cálculo de dimensionamiento, consulte los enlaces de vídeo en la <a href="#">Tabla 2</a>.</p> <p>Descargue la <i>herramienta Sizer</i>, que es una hoja de cálculo de dimensionamiento, desde la página siguiente y complete los pasos siguientes: <a href="#">Blueprints</a>.</p>	Tiene la hoja de cálculo de la herramienta Sizer y la información que necesita para cambiar el tamaño de los requisitos de capacidad de IBM Spectrum Protect Plus.

Tabla 1. Storyboard de despliegue (continuación)

Historia	Procedimiento	Resultados esperados
Cambie el tamaño de la capacidad que es necesaria para el almacenamiento primario de su entorno.	<p>Utilice la herramienta Sizer para cambiar el tamaño del almacenamiento primario.</p> <ol style="list-style-type: none"> <li>1. Abra la hoja de cálculo de la <i>herramienta Sizer</i> descargada y habilite las macros. Guarde una copia de la hoja de cálculo en la unidad local para el almacenamiento primario.</li> <li>2. Complete la hoja <b>Iniciar aquí</b> especificando sus opciones para las opciones globales del almacenamiento primario.</li> <li>3. Abra la pestaña VMware y especifique datos para la capacidad de vCenter que incluye el cambio de velocidad diario y el crecimiento anual.</li> <li>4. Abra la pestaña HyperV y especifique datos para la capacidad de HyperV.</li> <li>5. En cada aplicación que tiene previsto utilizar, abra una ficha de aplicación y especifique datos para sus necesidades de capacidad.</li> <li>6. Cuando se hayan especificado todos los datos, haga clic en la pestaña <b>Resultados del dimensionamiento</b> para revisar los datos calculados.</li> <li>7. Establezca el tamaño del servidor vSnap preferido. Para especificar automáticamente el valor para el tamaño de la agrupación de almacenamiento de vSnap, haga clic en Automático.</li> <li>8. Especifique el porcentaje de reserva del servidor vSnap que necesita. Esta reserva es el porcentaje del almacenamiento del servidor vSnap que está reservado para el uso, las operaciones de restauración y para cualquier reutilización.</li> <li>9. Abra IBM Spectrum Protect Plus y vaya a <b>Configuración del sistema &gt; Preferencias globales</b>. Especifique los porcentajes de preferencias globales tal como se muestra en la <i>herramienta Sizer</i>. Utilice estos porcentajes para establecer las siguientes opciones: <ul style="list-style-type: none"> <li>• <b>Error de espacio libre en destino (porcentaje)</b></li> <li>• <b>Aviso de espacio libre en destino (porcentaje)</b></li> </ul> </li> <li>10. Revise los resultados del Sizer para su almacenamiento primario. Guarde el Sizer, pero déjelo abierto para introducir valores que son necesarios para el almacenamiento secundario.</li> </ol>	<p>La hoja de cálculo de la herramienta Sizer le ayuda a calcular la información de dimensionamiento para el almacenamiento primario.</p> <p>Ha guardado una copia de la hoja de cálculo de dimensionamiento de Sizer. Si cambian los requisitos de capacidad, puede actualizar la hoja de cálculo según corresponda.</p> <p>También tiene detalles sobre el número y el tamaño necesarios de los servidores vSnap y, de forma opcional, el número de proxies de VMware vStorage API for Data Protection (VADP).</p> <p>Tiene detalles sobre una vista de crecimiento de ocho años basada en la entrada en la hoja de cálculo. Establezca las preferencias globales para desencadenar advertencias y errores desde vSnap cuando alcanza un umbral especificado en función del uso de porcentaje.</p>



Tabla 1. Storyboard de despliegue (continuación)

Historia	Procedimiento	Resultados esperados
<p>Cambie el tamaño de la capacidad que es necesaria para el almacenamiento secundario de su entorno.</p>	<p>Utilice la herramienta Sizer para cambiar el tamaño del almacenamiento secundario siguiendo estos pasos. Consulte el capítulo 5 de Blueprints.</p> <ol style="list-style-type: none"> <li>1. Descargue la hoja de cálculo de dimensionamiento desde la página de Blueprints y habilite las macros. Guarde una copia de la hoja de cálculo Sizer en la unidad local para el almacenamiento primario.</li> <li>2. Si hay algún valor, restablezca la hoja de cálculo de la herramienta Sizer pulsando <b>Hacer clic en restablecer</b>.</li> <li>3. Complete la hoja <b>Iniciar aquí</b> especificando sus opciones para las opciones globales del almacenamiento secundario.</li> <li>4. Vaya a la pestaña <b>Resultados</b> de la hoja de cálculo <i>Herramienta de Sizer</i> del almacenamiento primario que ha guardado previamente. Copie los resultados que se listan en la tabla Carga de trabajo de réplica y especifique los valores en la tabla Carga de trabajo de entrada de réplica opcional en la pestaña <b>Iniciar aquí</b> de la hoja de cálculo Herramienta Sizer de almacenamiento secundario.</li> <li>5. Si tiene previsto proteger los datos de aplicación, complete las pestañas de aplicación. Por ejemplo, puede especificar opciones para copiar datos en políticas de almacenamiento de objetos y de réplica.</li> <li>6. Revise los resultados de dimensionamiento de su almacenamiento secundario. Guarde y cierre las hojas de cálculo de la herramienta Sizer.</li> </ol>	<p>Tiene el dimensionamiento para la capacidad del almacenamiento secundario para el entorno de IBM Spectrum Protect Plus.</p> <p>Ha guardado una copia de Sizer para el almacenamiento secundario en el entorno. Si cambia algo, puede alterar el Sizer y realizar los cambios necesarios.</p> <p>También tiene detalles sobre la cantidad de servidor vSnap para cada año, la cantidad de proxy VADP y el tamaño de cada servidor vSnap.</p> <p>Tiene detalles de una vista de crecimiento de ocho años basada en sus entradas en el Sizer. Establezca las preferencias globales para desencadenar advertencias y errores desde vSnap cuando alcanza un porcentaje de uso.</p>
<p>Instale o actualice IBM Spectrum Protect Plus utilizando la imagen ISO para la versión que necesite. Si actualiza el entorno del sistema, se instala un nuevo kernel y se requiere un reinicio.</p>	<p>Instale IBM Spectrum Protect Plus, siga las instrucciones en <a href="#">“Instalación de IBM Spectrum Protect Plus como un dispositivo virtual VMware”</a> en la página 103 o <a href="#">“Instalación de IBM Spectrum Protect Plus como un dispositivo virtual Hyper-V”</a> en la página 105.</p>	<p>IBM Spectrum Protect Plus está instalado.</p>

Tabla 1. Storyboard de despliegue (continuación)		
Historia	Procedimiento	Resultados esperados
Instale o actualice el servidor vSnap utilizando la imagen ISO para la versión que necesite. Si utiliza la deduplicación de datos, el reinicio del servidor vSnap puede tardar hasta 15 minutos.	Instale el servidor vSnap, siga las instrucciones de <a href="#">“Instalación de un servidor vSnap físico”</a> en la página 111. Si está instalando un servidor vSnap virtual, siga las instrucciones de <a href="#">“Instalación de un servidor virtual vSnap en un entorno Hyper-V”</a> en la página 114.	El servidor vSnap está instalado. Para verificar que el servidor vSnap está instalado, ejecute el mandato <code>vsnap show</code> .
Compile el servidor vSnap con la capacidad que ha derivado del dimensionamiento utilizando Blueprints y la <i>Herramienta de dimensionamiento</i> .	<ol style="list-style-type: none"> <li>1. Cree volúmenes y correlacione dispositivos vSnap.</li> <li>2. Correlacione volúmenes con el clúster de máquina virtual.</li> <li>3. Consulte los pasos para configurar un servidor vSnap físico o virtual en Blueprints, <a href="#">Blueprints</a>.</li> </ol>	Se ha compilado el servidor vSnap.
Añada espacio de registro.	<p>Cree un compilador de múltiples dispositivos de Linux® con tres particiones para almacenar la memoria caché de almacenamiento del servidor vSnap, la caché en la nube y los archivos de registro. Para la memoria caché en la nube, la capacidad se establece en 128 GB de forma predeterminada. Si tiene previsto copiar datos en la nube, debe aumentar la capacidad. Para que los servidores vSnap físicos copien datos en el almacenamiento en la nube, debe crear el sistema de archivos <code>/opt/vsnap-data</code> con la capacidad necesaria.</p> <p>Para obtener más información sobre este paso, consulte <a href="#">Configuración de un servidor vSnap físico utilizando el software de almacenamiento proporcionado por RAID y Capítulo 7. Configuración del almacenamiento de objetos en la nube en Blueprints</a>.</p>	Ha establecido el espacio de registro para los servidores vSnap físicos o virtuales.
Registre el servidor vSnap.	Registre el servidor vSnap. Para obtener más información y los pasos, consulte <a href="#">“Registro de un servidor vSnap como proveedor de almacenamiento de copias de seguridad”</a> en la página 117.	El servidor vSnap se ha registrado y se ha añadido a IBM Spectrum Protect Plus.
Inicialice el servidor de aplicaciones.	Después de instalar o actualizar IBM Spectrum Protect Plus y de añadir servidores vSnap, debe inicializar los servidores los servidores vSnap. Para obtener información y pasos, consulte <a href="#">“Finalización de una inicialización simple”</a> en la página 129.	En función de su elección, el servidor vSnap se inicializa con o sin cifrado.
Configure el servidor vSnap.	Para configurar opciones de almacenamiento del servidor vSnap como la adición de socios de replicación, consulte <a href="#">“Configuración de las opciones de almacenamiento de copias de seguridad”</a> en la página 120.	Si ha configurado la característica de réplica de datos, se configuran los socios de replicación.

Tabla 1. Storyboard de despliegue (continuación)		
Historia	Procedimiento	Resultados esperados
(Opcional) Configure el servidor vSnap como un proxy VADP.	Si utiliza un proxy VADP para optimizar el movimiento de datos hacia y desde el servidor vSnap, debe registrar el servidor vSnap como un proxy VADP. Para obtener más instrucciones, consulte <a href="#">“Registro de un proxy VADP en un servidor vSnap”</a> en la página 270.	El servidor vSnap se configura como un proxy VADP.
Configure el entorno de VMware que incluye la creación de un vCenter y el registro de un hipervisor.	Para proteger los datos de VMware, primero debe configurar un vCenter Server. Para obtener instrucciones, consulte <a href="#">“Copia de seguridad y restauración de datos de VMware”</a> en la página 257. Asegúrese de que los privilegios de vCenter Server necesarios están habilitados. Para obtener más información sobre los privilegios necesarios, consulte <a href="#">“Privilegios de máquinas virtuales”</a> en la página 259.	Se configura un vCenter con los permisos necesarios para que pueda comenzar a proteger datos de VMware.
Añadir usuarios.	Añada los usuarios que serán necesarios para utilizar IBM Spectrum Protect Plus. Para obtener más información, consulte <a href="#">“Creación de una cuenta de usuario para un usuario individual”</a> en la página 542 utilizando el formulario Añadir usuario en la página.	Se añaden los usuarios y se les otorga permiso para operar IBM Spectrum Protect Plus.
Cree una política de acuerdo de nivel de servicio (SLA).	Configure una política o políticas de SLA para las cargas de trabajo de IBM Spectrum Protect Plus. Para obtener más información sobre las políticas de SLA, consulte <a href="#">Capítulo 9, “Gestión de políticas de SLA para operaciones de seguridad”</a> , en la página 241.	Las políticas de SLA para las cargas de trabajo de IBM Spectrum Protect Plus están configuradas y el usuario está preparado para ejecutar trabajos de copia de seguridad.
Actualice las preferencias globales.	Los administradores pueden editar las preferencias globales para todas las operaciones como deduplicación o cifrado. Para obtener más información sobre las preferencias globales, consulte <a href="#">“Configuración de las preferencias globales”</a> en la página 232.	Si se establecen preferencias globales, se aplican a todo el entorno de IBM Spectrum Protect Plus.

## Recursos y biblioteca de vídeos

Los blueprints se deben utilizar para dimensionar el entorno de IBM Spectrum Protect Plus. Los vídeos que se listan en la siguiente tabla [Tabla](#) pueden ayudarle con ese proceso.

Tabla 2. Blueprints y dimensionamiento	
Tarea o tema	Enlace de vídeo
Introducción a la herramienta Sizer	<a href="#">IBM Spectrum Protect Plus Sizer and Blueprints: 1. Sizer introduction - Demo</a>
Visión general de la hoja de trabajo Sizer	<a href="#">IBM Spectrum Protect Plus Sizer &amp; Blueprints: 2. Sizer Worksheet Overview – Demo</a>
Valores globales de Sizer	<a href="#">IBM Spectrum Protect Plus Sizer &amp; Blueprints: 3. Sizer Global Values – Demo</a>
Adición de un hipervisor	<a href="#">IBM Spectrum Protect Plus Sizer &amp; Blueprints: 4. Adding a Hypervisor workload to the sizer – Demo</a>
Adición de una aplicación	<a href="#">IBM Spectrum Protect Plus Sizer &amp; Blueprints: 5. Adding Application workload to the sizer– Demo</a>

Tabla 2. Blueprints y dimensionamiento (continuación)

Tarea o tema	Enlace de vídeo
Evaluación de los resultados	<a href="#">IBM Spectrum Protect Plus Sizer &amp; Blueprints: 6. Evaluating the sizer's results – Demo</a>
Adición de almacenamiento secundario	<a href="#">IBM Spectrum Protect Plus Sizer &amp; Blueprints: 7. Adding a secondary site to sizer – Demo</a>
Escenarios de <i>Qué pasa si</i>	<a href="#">IBM Spectrum Protect Plus Sizer &amp; Blueprints: 8. What if sizing scenarios – Demo</a>
Novedades de Blueprints	<a href="#">IBM Spectrum Protect Plus Sizer &amp; Blueprints: 9. What's new in 10.1.5 sizer – Presentation</a>
Uso de los resultados de Sizer para el despliegue	<a href="#">IBM Spectrum Protect Plus Sizer &amp; Blueprint: 10. Tying the blueprints, sizer and install together - Demo</a>

## 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 servicio 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 de VMware vStorage API for Data Protection (VADP). 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 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 8](#).

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

Elemento	Descripción
Icono de IBM Spectrum Protect 	Este icono abre IBM Spectrum Protect Operations Center para proporcionar protección de datos ampliada. Este icono está activo solo cuando se especifica el URL en el campo de preferencia <b>IBM Spectrum Protect Operations Center URL</b> en la <a href="#">página Preferencias globales</a> . Para obtener información sobre esta preferencia, consulte <a href="#">“Configuración de las preferencias globales”</a> en la <a href="#">página 232</a> .
Icono de alertas 	Este icono abre la ventana <b>Alertas</b> . Para obtener más información sobre las alertas, consulte <a href="#">“Alertas”</a> en la <a href="#">página 10</a> .
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.

**Restricción:** El producto de IBM Spectrum Protect Plus no sigue el orden de clasificación de ICU para menús, por lo tanto, la ordenación de los menús aparecerá en el orden de punto de código. Por ejemplo, algunos idiomas clasifican las letras de forma distinta al orden de punto de código. Por lo tanto, el orden de clasificación de caracteres y palabras tal y como aparece en los menús al utilizar esos idiomas no aparecerá en el orden esperado.

**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.

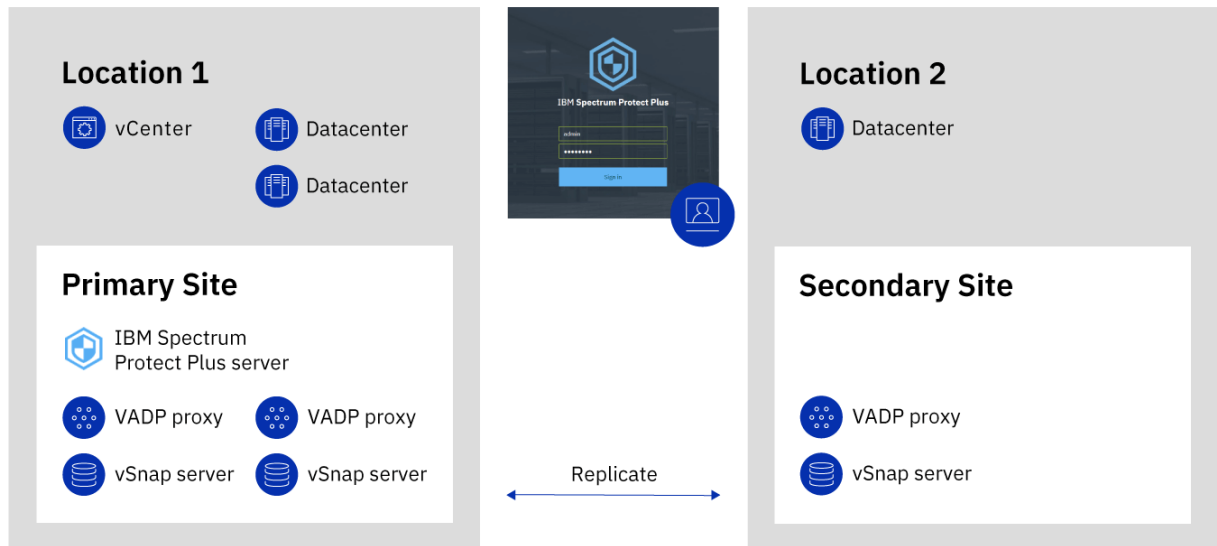


Figura 1. Despliegue de IBM Spectrum Protect Plus en dos ubicaciones geográficas

## 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:

$$100 \times \text{trabajos satisfactorios} / \text{Trabajos totales} = \text{Tasa de correctos}$$

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 ahorro de espacio que se logra además de 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 copia bloqueada

Se visualiza cuando la instantánea de almacenamiento copiada más recientemente está bloqueada. Aumente la retención de las copias o la política de frecuencia de copias.

#### 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.

#### Deduplicación inhabilitada en el almacenamiento

Se visualiza cuando la deduplicación se inhabilita y muestra la IP del servidor de almacenamiento. Esto tiene lugar cuando la opción de la tabla de deduplicación (DDT) de inhabilitación automática de vSnap está habilitada y se supera el umbral de porcentaje o tamaño definido.



## 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 solo 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 18, “Gestión del acceso de usuarios”](#), en la [página 533](#).

## 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 9, “Gestión de políticas de SLA para operaciones de seguridad”](#), en la [página 241](#).

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:

- En entornos que contienen más de un servidor vSnap, todos los servidores vSnap deben tener una asociación establecida.
- 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.

## Copiar instantáneas en almacenamiento de copias 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 copiar instantáneas desde un servidor vSnap en un almacenamiento de copias de seguridad secundario.

**Cambio de terminología:** En releases anteriores, el proceso de copia de datos de IBM Spectrum Protect Plus a un almacenamiento de copias de seguridad secundario se conocía como *descarga* de datos. A partir de IBM Spectrum Protect Plus versión 10.1.5, el proceso se conoce como *copia* de datos.

Los siguientes destinos de almacenamiento de copias de seguridad secundarias están disponibles para operaciones de copia:

- 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 de 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 estándar

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

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

La copia de instantáneas en el almacenamiento de objetos estándar 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 en cintas o de archivado en la nube.

### Almacenamiento en cintas o de archivado en la nube

El almacenamiento en cintas significa que los datos se almacenan en un soporte de cinta física o en una biblioteca de cintas virtual (VTL). El almacenamiento en cintas es una opción cuando copia datos de instantánea en un Servidor de IBM Spectrum Protect.

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 copia datos de instantánea en cintas o en un sistema de almacenamiento en la nube, se crea una copia completa de los datos.

La copia de instantáneas en un almacenamiento de archivado de objetos en la nube o en cintas proporciona ventajas adicionales de coste y seguridad. 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. Sin embargo, como la copia 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.

Cuando se copian datos en cintas de IBM Spectrum Protect Plus a Servidor de IBM Spectrum Protect, no es buena idea utilizar la función de organización por niveles de IBM Spectrum Protect. Si está archivando datos en cintas, debe utilizar una agrupación de almacenamiento en memoria caché fría. Para obtener más información sobre la disposición en niveles, consulte [“¿Cómo puedo disponer en niveles los datos en el almacenamiento en la nube o en cintas?”](#) en la página 549. Para obtener

distintos escenarios y más información sobre cómo configurar el almacenamiento, consulte [“Configuración para copiar o archivar datos en IBM Spectrum Protect” en la página 198.](#)

Para obtener información sobre cómo se copian los datos de instantánea en el almacenamiento de objetos estándar y el almacenamiento de objetos de archivado para cada sistema de almacenamiento en la nube, consulte [“Requisitos de almacenamiento en la nube” en la página 38.](#)

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

Para copiar instantáneas en el almacenamiento secundario, son necesarias las acciones siguientes:

<b>Acción</b>	<b>Procedimiento</b>
Para copiar instantáneas en un servidor de repositorio <ul style="list-style-type: none"><li>• Configure IBM Spectrum Protect Plus como un cliente objeto en el entorno del Servidor de IBM Spectrum Protect.</li><li>• Añada el almacenamiento a IBM Spectrum Protect Plus.</li></ul>	Consulte <a href="#">“Configuración para copiar o archivar datos en IBM Spectrum Protect” en la página 198</a> y <a href="#">“Registro de un servidor de repositorio como proveedor de almacenamiento de copias de seguridad” en la página 210.</a>
Para copiar instantáneas en el almacenamiento en la nube, añada el almacenamiento a IBM Spectrum Protect Plus.	Siga las instrucciones para el tipo de almacenamiento seleccionado: <ul style="list-style-type: none"><li>• <a href="#">“Adición del almacenamiento de objetos de Amazon S3” en la página 192</a></li><li>• <a href="#">“Adición de IBM Cloud Object Storage como proveedor de almacenamiento de copias de seguridad” en la página 193</a></li><li>• <a href="#">“Adición del almacenamiento en la nube de Microsoft Azure como proveedor de almacenamiento de copias de seguridad” en la página 195</a></li><li>• <a href="#">“Registro de un servidor de repositorio como proveedor de almacenamiento de copias de seguridad” en la página 210</a></li></ul>
Crear una política de copia de seguridad que incluya el almacenamiento.	Consulte <a href="#">“Crear políticas de copia de seguridad” en la página 169.</a>

### **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 copian del servidor vSnap en el sitio secundario al almacenamiento en la nube para una protección de datos a largo plazo.

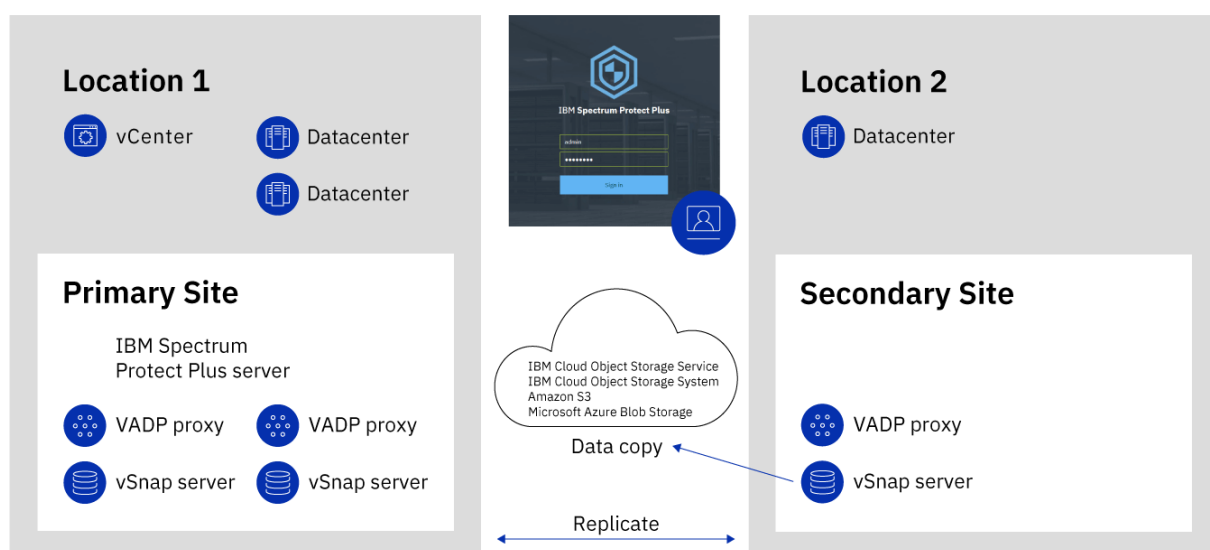


Figura 2. Despliegue de IBM Spectrum Protect Plus en dos ubicaciones geográficas con copia en el almacenamiento en la nube

La siguiente figura muestra el mismo despliegue que la anterior.

Sin embargo, en este despliegue, las instantáneas se copian desde el servidor vSnap en el sitio secundario a IBM Spectrum Protect para la protección de datos a largo plazo.

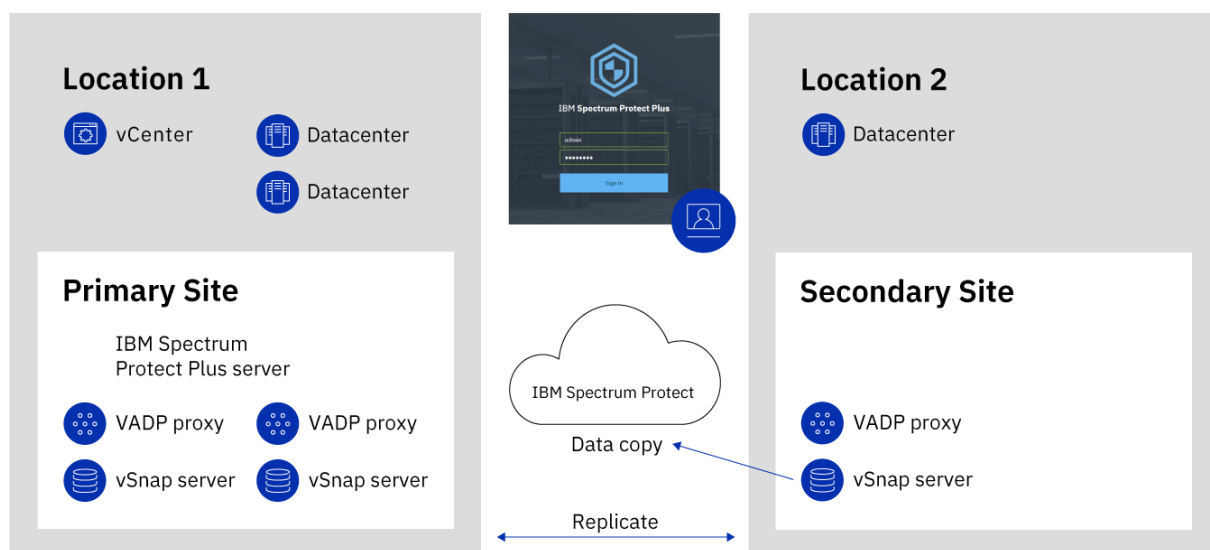


Figura 3. Despliegue de IBM Spectrum Protect Plus en dos ubicaciones geográficas con copia en IBM Spectrum Protect

## 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 de protección de datos para usuarios que desean proteger las bases de datos que se están ejecutando en AWS. Además, los usuarios pueden proteger máquinas virtuales gestionadas por VMware Cloud (VMC) en AWS mientras el servidor IBM Spectrum Protect Plus esté instalado en VMC y el servidor vSnap esté instalado en una Virtual Private Cloud (VPC) de AWS.

Puede desplegar IBM Spectrum Protect Plus on AWS en una de las siguientes configuraciones. El soporte para VMC en AWS solo está disponible en un entorno híbrido. Para obtener más información sobre el soporte de VMC en AWS, consulte [IBM Spectrum Protect Plus para VMware Cloud on AWS](#).

**Entorno todo en la nube**

En esta configuración, tanto el servidor de IBM Spectrum Protect Plus como el servidor vSnap se despliegan en AWS en un VPC existente o nuevo. No se necesita ni un servidor IBM Spectrum Protect Plus local ni una infraestructura de VMware o Microsoft Hyper-V.

Esta opción puede beneficiar a nuevos usuarios de IBM Spectrum Protect Plus que desean proteger bases de datos en AWS y no tienen IBM Spectrum Protect Plus en ejecución en un entorno local.

## Entorno híbrido

En esta configuración, solo el servidor vSnap se despliega en AWS en un VPC existente o nuevo. El servidor de IBM Spectrum Protect Plus está instalado y se mantiene en entornos locales o en otra ubicación. Esta opción puede beneficiar a los usuarios de IBM Spectrum Protect Plus existentes que desean continuar protegiendo las cargas de trabajo que están en ejecución en entornos locales y entornos de nube.

Además de las operaciones de copia de seguridad y recuperación, también puede utilizar un entorno híbrido para replicar y reutilizar datos entre las ubicaciones locales y AWS para la protección de datos adicional. Por ejemplo, puede que desee utilizar datos que están protegidos en su sitio local en AWS for DevOps, con fines de control de calidad, realización de pruebas y de recuperación tras desastre.

## Despliegue de IBM Spectrum Protect Plus en AWS

Página IBM Spectrum Protect Plus en AWS Marketplace proporciona las plantillas de AWS CloudFormation que son necesarias para desplegar el servidor IBM Spectrum Protect Plus y 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.

## Integración con IBM Spectrum Protect

Puede supervisar el entorno de IBM Spectrum Protect Plus desde IBM Spectrum Protect Operations Center. Por comodidad, también puede acceder a Centro de operaciones directamente desde IBM Spectrum Protect Plus.

### Supervise IBM Spectrum Protect Plus desde Centro de operaciones


Centro de operaciones incluye un panel de instrumentos para IBM Spectrum Protect Plus que proporciona la siguiente información:

- Un resumen de las actividades de trabajo para un periodo de tiempo seleccionado. Puede ver los porcentajes de copia de seguridad, restauración y otros trabajos que se han realizado correctamente y los que han fallado. A partir de esta información de resumen, puede ir a información más detallada para cada tipo de trabajo.
- Un resumen de la capacidad y disponibilidad de los servidores vSnap. Puede ver la capacidad de disco total que está disponible para el servidor de IBM Spectrum Protect Plus a través de todos los servidores vSnap. También puede ver la capacidad disponible para cada servidor vSnap.
- Un resumen de las políticas de acuerdo de nivel de servicio (SLA) que se resumen en el servidor de IBM Spectrum Protect Plus. Puede ver el número de políticas que tienen trabajos de copia de seguridad asociados. También puede ver el porcentaje de recursos que están protegidos por trabajos de copia de seguridad y el número de recursos que no están protegidos. A partir de esta información de resumen, puede ir a información más detallada sobre la política.

Para habilitar esta característica, el administrador del sistema debe añadir el servidor de IBM Spectrum Protect Plus a Centro de operaciones.

### Acceda a Centro de operaciones desde la GUI de IBM Spectrum Protect Plus

Para acceder a Centro de operaciones desde IBM Spectrum Protect Plus, el administrador del sistema debe añadir el URL de Centro de operaciones de la página **Preferencias globales** de la GUI de IBM Spectrum Protect Plus.

A continuación, puede acceder a Centro de operaciones desde el icono de IBM Spectrum Protect  en la barra de menús.

# Adición de IBM Spectrum Protect Plus a Centro de operaciones

Cuando añade un servidor de IBM Spectrum Protect Plus a Centro de operaciones, establece una conexión entre el servidor y Centro de operaciones. Después de establecer esta conexión, puede utilizar Centro de operaciones para supervisar el entorno de IBM Spectrum Protect Plus.


## Antes de empezar

Asegúrese de que tiene el URL para Centro de operaciones y las credenciales para iniciar sesión.

## Procedimiento

Para añadir un servidor de IBM Spectrum Protect Plus a Centro de operaciones, complete los pasos siguientes:

1. En la barra de menús de Centro de operaciones, haga clic en **Visiones generales > Protect Plus** y realice una de las siguientes acciones para abrir el asistente **Añadir servidor**:

Configuración actual	Acción
No hay servidores de IBM Spectrum Protect Plus conectados a Centro de operaciones.	Un mensaje indica que no hay configurados servidores de IBM Spectrum Protect Plus. Pulse <b>+Añadir servidor</b> .
Hay uno o varios servidores de IBM Spectrum Protect Plus conectados a Centro de operaciones.	Se muestra el panel de control de IBM Spectrum Protect Plus. En la lista de servidores del panel de control de supervisión, seleccione <b>+Añadir servidor</b> . 

2. Para añadir el servidor de IBM Spectrum Protect Plus , siga las instrucciones del asistente.

En la página **Autorización** del asistente, se le solicita que especifique las credenciales de usuario para acceder y supervisar el servidor de IBM Spectrum Protect Plus. Si tiene una cuenta de IBM Spectrum Protect Plus cuyas credenciales coinciden con las credenciales de Centro de operaciones, puede utilizar esa cuenta. Si no tiene credenciales que coincidan, debe crear una cuenta.

### Utilizar credenciales del Centro de operaciones

Seleccione esta opción para utilizar una cuenta de usuario de IBM Spectrum Protect Plus que coincida con el nombre de usuario y contraseña de la cuenta de administrador que ha utilizado para iniciar sesión en Centro de operaciones.

### Crear una cuenta de usuario de supervisión

Seleccione esta opción para que el asistente cree una cuenta de usuario de IBM Spectrum Protect Plus.

Para habilitar Centro de operaciones para acceder a IBM Spectrum Protect Plus y crear la cuenta, proporcione credenciales para una cuenta de usuario de IBM Spectrum Protect Plus asignada al rol SYSADMIN. Especifique las credenciales en los campos **Nombre de usuario** y **Contraseña** como se muestra en la siguiente figura.

# Add Server

Authorization

Identify or create a user account on the IBM Spectrum Protect Plus server for monitoring. [Learn more](#)

☐ Use Operations Center credentials (User account with the same credentials must already be defined on server)

☒ Create a monitoring administrator

Specify IBM Spectrum Protect Plus login credentials for a user account that can create custom user roles and user accounts. This user account is used only during configuration. During configuration, a new user role and account for monitoring are created.

User name

Password

Back

Add Server

Cancel

Figura 4. Introducción de credenciales del IBM Spectrum Protect Plus

Las credenciales que se han especificado aquí no se guardan. Centro de operaciones inicia sesión en el servidor de IBM Spectrum Protect Plus utilizando estas credenciales de cuenta y crea la cuenta de usuario OC\_MONITOR\_*número*, donde *número* es un número aleatorio para la identificación. Centro de operaciones se conectará al entorno IBM Spectrum Protect Plus utilizando la cuenta nueva.

3. Pulse **Añadir servidor**.

Si la operación se ha realizado correctamente, los resultados se muestran como aparecen en la siguiente figura:



## Add Server

✓ Succeeded

10:19 PM Adding IBM Spectrum Protect Plus server...  
Connecting to the IBM Spectrum Protect Plus server.  
Creating monitor role.  
Creating monitor user.  
Saving server.  
Establishing session.

✓  
✓  
✓  
✓  
✓

Close

Figura 5. IBM Spectrum Protect Plus se ha añadido correctamente

## Introducción del URL de Centro de operaciones

Para acceder a Centro de operaciones desde IBM Spectrum Protect Plus, especifique el URL para Centro de operaciones en las preferencias globales de IBM Spectrum Protect Plus.

### Acerca de esta tarea

Debe tener credenciales de administrador de IBM Spectrum Protect Plus para configurar las preferencias globales.

Cuando se especifica esta preferencia, el icono de IBM Spectrum Protect  está activo en la barra de menús de IBM Spectrum Protect Plus.

### Procedimiento

Para especificar el URL para Centro de operaciones, complete los pasos siguientes:

1. En el panel de navegación, pulse **Configuración del sistema > Preferencias globales**.
2. Especifique el URL para Centro de operaciones En el campo **IBM Spectrum Protect Operations Center URL**.

# Global Preferences

Register system preferences for your IBM Spectrum Protect Plus environment.

## Integration with other storage products

IBM Spectrum Protect Operations Center



<https://tapsrv09.storage.tucson.il>



URL

Figura 6. Introducción del URL de Centro de operaciones

- Para activar el icono de IBM Spectrum Protect en la barra de menús de IBM Spectrum Protect Plus, cierre sesión en IBM Spectrum Protect Plus e iníciela de nuevo.

## Acceso a Centro de operaciones

Inicie Centro de operaciones para supervisar el entorno de IBM Spectrum Protect Plus.


### Antes de empezar

Asegúrese de que ha realizado las tareas siguientes:

- “Adición de IBM Spectrum Protect Plus a Centro de operaciones” en la [página 17](#)
- “Introducción del URL de Centro de operaciones” en la [página 19](#)

### Procedimiento

Para acceder a Centro de operaciones y supervisar el entorno de IBM Spectrum Protect Plus, complete los pasos siguientes:

1. En la barra de menús de IBM Spectrum Protect Plus, haga clic en el icono de IBM Spectrum Protect .
2. Inicie la sesión en el Centro de operaciones.
3. En la barra de menús de Centro de operaciones, haga clic en **Descripciones generales > Protect Plus**.

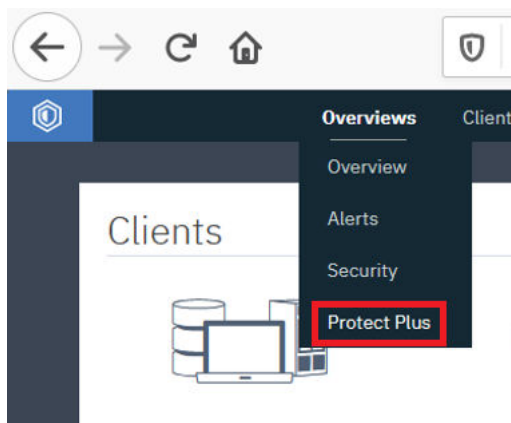


Figura 7. Selección de IBM Spectrum Protect Plus en Centro de operaciones

4. Vea el estado del entorno de IBM Spectrum Protect Plus en el panel de control de supervisión de IBM Spectrum Protect Plus tal como se muestra en la siguiente figura de ejemplo:

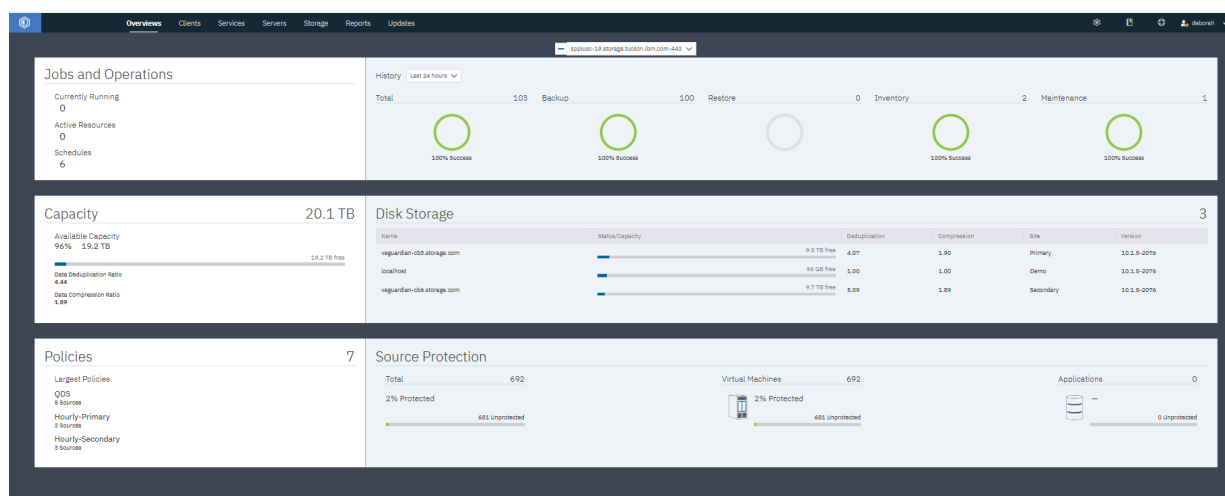


Figura 8. Visualización del panel de control de IBM Spectrum Protect Plus



## 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 <a href="#">“Requisitos del sistema”</a> en la <a href="#">página 23</a> .
Determine cómo dimensionar, compilar y colocar los componentes en el entorno de IBM Spectrum Protect Plus.	Consulte el <a href="#">Blueprints de IBM Spectrum Protect Plus</a> .
Instale IBM Spectrum Protect Plus.	Consulte <a href="#">Capítulo 2, “Instalación de IBM Spectrum Protect Plus”</a> , en la <a href="#">página 23</a> .
Si son necesarios servidores vSnap adicionales para dar soporte al entorno, instálelos y configúrelos.	Consulte <a href="#">Capítulo 3, “Instalación de servidores vSnap”</a> , en la <a href="#">página 111</a> .
Si se necesitan proxies de VMware vStorage API for Data Protection (VADP) adicionales para dar soporte al entorno, cree y configure los proxies.	Consulte <a href="#">“Gestión de proxies de copias de seguridad VADP”</a> en la <a href="#">página 267</a> .
Complete los pasos básicos para configurar y empezar a utilizar IBM Spectrum Protect Plus.	Consulte <a href="#">Capítulo 6, “Empezar con un inicio rápido”</a> , en la <a href="#">página 165</a> .

### 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 obtener los requisitos más actuales, que pueden incluir actualizaciones, consulte [Nota técnica 304861](#).

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 obtener los requisitos más actuales, que pueden incluir actualizaciones, consulte [Nota técnica 304861](#).

El soporte de IBM Spectrum Protect Plus para plataformas de terceros, aplicaciones, servicios y hardware depende de los proveedores de 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 que el proveedor.

## 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 cumple uno de los requisitos siguientes:

- 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 los niveles de parche (a partir de IBM Spectrum Protect Plus V10.1.2)
- vSphere 7.0, incluidas todas las actualizaciones y los niveles de parche (a partir de IBM Spectrum Protect Plus V10.1.6)
- Microsoft® Hyper-V 2016
- Microsoft Hyper-V 2019 (a partir de IBM Spectrum Protect Plus V10.1.3)

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

- Servidor de 8 núcleos de 64 bits
- 48 GB de memoria
- 548 GB de almacenamiento de disco para la máquina virtual (MV)

Utilice un servidor NTP (Network Time Protocol) para sincronizar el huso horario en los recursos de IBM Spectrum Protect Plus en el entorno, como el dispositivo virtual 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, las operaciones de inventario, los trabajos de copia de seguridad o los trabajos de restauración de archivos. Para obtener más información sobre la identificación y resolución de la derivación del temporizador, consulte el siguiente artículo de la base de conocimientos de VMware:: [Tiempo en derivaciones de máquina virtual debido a la derivación del temporizador de hardware](#)

## 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 y validado con los navegadores web siguientes:

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

Si la resolución de la pantalla es inferior a 1024 x 768, es posible que algunos elementos no se ajusten a la ventana. Habilite las ventanas emergentes en el navegador para acceder al sistema de ayuda y a algunas operaciones de IBM Spectrum Protect Plus.

## Puertos de dispositivo virtual

IBM Spectrum Protect Plus y los servicios asociados utilizan los puertos siguientes.

*Tabla 3. Puertos de comunicación cuando el destino es un dispositivo virtual de IBM Spectrum Protect Plus*

<b>Puerto</b>	<b>Protocolo</b>	<b>Iniciador</b>	<b>Objetivo</b>	<b>Descripción</b>
22	Protocolo de control de transmisiones (TCP)	Servidor vSnap	Dispositivo virtual de IBM Spectrum Protect Plus	Proporciona acceso a las tareas de resolución de problemas y mantenimiento en el dispositivo virtual de IBM Spectrum Protect Plus utilizando el protocolo SSH.  También se utiliza para la réplica de datos en el dispositivo virtual de IBM Spectrum Protect Plus utilizando el protocolo SSH.
443	TCP	interfaz de usuario de IBM Spectrum Protect Plus	Dispositivo virtual de IBM Spectrum Protect Plus	Proporciona acceso web utilizando HTTPS. Este puerto es el punto de entrada principal para las conexiones de cliente, que utilizan el protocolo SSL. Este puerto también se utiliza para las consultas de API REST (Application Programming Interface Representational State Transfer).
5671	TCP y Advanced Message Queuing Protocol (AMQP)	Host del proxy de VMware vStorage API for Data Protection (proxy VADP)	Dispositivo virtual de IBM Spectrum Protect Plus	Se utiliza para gestionar mensajes producidos y utilizados por el proxy VADP y los trabajadores de gestión de trabajos de VMware. Este puerto es una infraestructura de mensajes RabbitMQ, que también facilita la gestión de registro de trabajo.

*Tabla 3. Puertos de comunicación cuando el destino es un dispositivo virtual de IBM Spectrum Protect Plus (continuación)*

<b>Puerto</b>	<b>Protocolo</b>	<b>Iniciador</b>	<b>Objetivo</b>	<b>Descripción</b>
8090	TCP	Consola de administración	Dispositivo virtual de IBM Spectrum Protect Plus	Proporciona acceso para la administración de sistema. Esta infraestructura ampliable da soporte a plug-ins que ejecutan operaciones como, por ejemplo, actualizaciones de sistema y de red.
111	TCP	Hipervisores, proxy VADP o agentes que utilizan el cliente de NFS (Network File System)	Dispositivo virtual de IBM Spectrum Protect Plus: servidor vSnap incorporado	Permite que los clientes descubran los puertos que los clientes de Open Network Computing (ONC) requieren para comunicarse con servidores ONC.
2049	TCP	Hipervisores, proxy VADP o agentes que utilizan el cliente de NFS (Network File System)	Dispositivo virtual de IBM Spectrum Protect Plus: servidor vSnap incorporado	Se utiliza para transferir la compartición de archivos NFS utilizando el servidor vSnap.
3260	TCP	Hipervisores, proxy VADP o agentes que utilizan el cliente de iSCSI (Internet Small Computer System Interface)	Dispositivo virtual de IBM Spectrum Protect Plus: servidor vSnap incorporado	Se utiliza para la transferencia de datos de iSCSI utilizando el servidor vSnap.
20048	TCP	Hipervisores, proxy VADP o agentes que utilizan el cliente de NFS (Network File System)	Dispositivo virtual de IBM Spectrum Protect Plus: servidor vSnap incorporado	Se utiliza para la transferencia de datos de NFS utilizando el servidor vSnap.

#### **Actualizaciones de puerto:**

- Puerto 9090: en versiones anteriores, el puerto 9090 se utilizaba para la ayuda en línea. A partir de V10.1.4, este puerto ya no es necesario para la ayuda en línea. No es necesaria ninguna acción adicional.
- Puerto 8761: en versiones anteriores, el puerto 8761 se utilizaba para descubrir automáticamente proxies VADP y para las operaciones de copia de seguridad de la máquina virtual (MV) de IBM Spectrum Protect Plus. A partir de IBM Spectrum Protect Plus V10.1.6, la arquitectura del proxy VADP se modifica y ya no es necesario que el puerto 8761 esté abierto. Cuando se actualiza IBM Spectrum Protect Plus a V10.1.6, también se actualizan los proxies VADP asociados en el entorno.



*Tabla 4. Puertos de comunicación cuando el iniciador es un dispositivo virtual de IBM Spectrum Protect Plus*

<b>Puerto</b>	<b>Protocolo</b>	<b>Iniciador</b>	<b>Objetivo</b>	<b>Descripción</b>
22	TCP	Dispositivo virtual de IBM Spectrum Protect Plus	Servidor vSnap o host de proxy VADP	Proporciona acceso a tareas de resolución de problemas y de mantenimiento en servidores vSnap remotos y el proxy VADP utilizando el protocolo SSH. También se utiliza para la réplica de datos de vSnap desde el dispositivo virtual de IBM Spectrum Protect Plus utilizando el protocolo SSH.
25	TCP	Dispositivo virtual de IBM Spectrum Protect Plus	Servidor de correo electrónico al que se puede acceder mediante el protocolo simple de transferencia de correo (SMTP)	Proporciona acceso a un servicio de correo electrónico.
389	TCP	Dispositivo virtual de IBM Spectrum Protect Plus	Servidor LDAP (Lightweight Directory Access Protocol)	Proporciona acceso a servicios de Active Directory.
443	TCP	Dispositivo virtual de IBM Spectrum Protect Plus	Hipervisor: host de VMware Elastic Sky X Integrated (ESXi) y vCenter	Proporciona acceso a ESXi y vCenter para gestionar operaciones.
636	TCP	Dispositivo virtual de IBM Spectrum Protect Plus	servidor LDAP	Proporciona acceso a servicios de Active Directory utilizando el protocolo SSL.

*Tabla 4. Puertos de comunicación cuando el iniciador es un dispositivo virtual de IBM Spectrum Protect Plus (continuación)*

<b>Puerto</b>	<b>Protocolo</b>	<b>Iniciador</b>	<b>Objetivo</b>	<b>Descripción</b>
902	TCP	Dispositivo virtual de IBM Spectrum Protect Plus	Hipervisor: host de VMware ESXi	Se utiliza para el protocolo NFC (Network File Copy), que proporciona un servicio de Protocolo de transferencia de archivos (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	Dispositivo virtual de IBM Spectrum Protect Plus	Hipervisor: Hyper-V o agentes que utilizan el iniciador iSCSI	Proporciona acceso al servicio Microsoft Windows Remote Management (WinRM) para servidores basados en Windows.
5986	TCP	Dispositivo virtual de IBM Spectrum Protect Plus	Hipervisor: Hyper-V o agentes que utilizan el iniciador iSCSI	Proporciona acceso al servicio Microsoft Windows Remote Management (WinRM) para servidores basados en Windows.
8098	TCP	Dispositivo virtual de IBM Spectrum Protect Plus	Host de proxy VADP	Da soporte a las comunicaciones de API REST entre el dispositivo virtual de IBM Spectrum Protect Plus y el proxy VADP utilizando el protocolo de (TLS).

*Tabla 4. Puertos de comunicación cuando el iniciador es un dispositivo virtual de IBM Spectrum Protect Plus (continuación)*

Puerto	Protocolo	Iniciador	Objetivo	Descripción
8900	TCP	Dispositivo IBM Spectrum Protect Plus	Servidor vSnap	Da soporte a las comunicaciones de la API REST entre el dispositivo virtual de IBM Spectrum Protect Plus y el servidor vSnap utilizando el protocolo TLS.

#### Diagrama de vías de acceso de comunicación de IBM Spectrum Protect Plus

El diagrama siguiente es una visión general de las vías de acceso de comunicación que gestiona IBM Spectrum Protect Plus. Este diagrama puede proporcionar asistencia para la resolución de problemas y la configuración de red para escenarios de despliegue.

- Los recursos etiquetados en el fondo gris representan los servicios principales del dispositivo virtual de IBM Spectrum Protect Plus .
- Los colores de los distintos módulos representan diferentes tipos de servicios según lo definido por la clave.
- El área etiquetada **Cortafuegos** representa el cortafuegos de red.
- Los servicios que aparecen en el área **Cortafuegos** son indicativos de los puertos que están abiertos en el cortafuegos.
- Las flechas con guión representan la comunicación entre los recursos y los servicios.
- Las flechas fluyen hacia el puerto de escucha.
- El puerto de escucha indica los números de puerto que deben estar abiertos.

Por ejemplo:

- El servicio vSnap se representa como externo al dispositivo virtual de IBM Spectrum Protect Plus. El servicio vSnap está escuchando en el puerto 8900 y en otros puertos.
- Un componente en el dispositivo virtual establece una vía de acceso de comunicación con una conexión al servicio vSnap en el puerto 8900.



<sup>3</sup> Los agentes siguientes utilizan un cliente de NFS: VMware, Oracle, IBM Db2, MongoDB, Kubernetes y Microsoft Office 365.

<sup>4</sup> Un puerto SSH conecta el servidor de IBM Spectrum Protect Plus al agente de soporte de copia de seguridad de Kubernetes. Si no selecciona un puerto, los servicios NodePort seleccionan un número de puerto aleatorio en el rango predeterminado. Si especifica un valor para este puerto, utilice un número de puerto dentro del rango de NodePort establecido por el administrador de Kubernetes que todavía no está en uso.

## **Requisitos del servidor vSnap**

### **Instalación 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 cuando se despliega inicialmente el dispositivo virtual de IBM Spectrum Protect Plus. El servidor vSnap de `localhost` es adecuado para fines de demostración o de prueba. Para su uso en un entorno de producción, es necesario instalar uno o más servidores vSnap externos.

Asigne memoria basándose en la capacidad de copia de seguridad para una deduplicación de datos más eficiente. Para obtener más información sobre cómo crear una solución de IBM Spectrum Protect Plus, consulte [Blueprints de IBM Spectrum Protect Plus](#).

### **Despliegue inicial del servidor vSnap**

Para el despliegue inicial, asegúrese de que la máquina virtual o el servidor físico de Linux® cumplen los requisitos mínimos siguientes:

- – Servidor 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 `/opt/vsnap-data`

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

Opcionalmente, utilice una unidad de estado sólido (SSD) para mejorar el rendimiento de copia de seguridad y restauración:

- Para mejorar el rendimiento de copia de seguridad, configure la agrupación de almacenamiento para utilizar uno o más dispositivos de registro de los que se ha hecho copia de seguridad en 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 de almacenamiento para utilizar uno o más dispositivos de registro de los que se ha hecho copia de seguridad en una SSD.

### **Instalación de máquina virtual del servidor vSnap**

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

- 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 los niveles de parche (a partir de IBM Spectrum Protect Plus V10.1.2)
- vSphere 7.0, incluidas todas las actualizaciones y los niveles de parche (a partir de IBM Spectrum Protect Plus V10.1.6)
- Microsoft Hyper-V 2016
- Microsoft Hyper-V 2019 (a partir de IBM Spectrum Protect Plus V10.1.3)

## Instalación física del servidor vSnap

A partir de V10.1.3, IBM Spectrum Protect Plus proporciona nuevas funciones que requieren que se soporten los niveles de kernel en Red Hat Enterprise Linux (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 instalaciones de vSnap físicas.

Se da soporte a los siguientes sistemas operativos Linux para instalaciones del servidor vSnap físico de IBM Spectrum Protect Plus V10.1.6:

- CentOS 7.1804 (7.5) (x86\_64) (a partir de IBM Spectrum Protect Plus V10.1.2)
- CentOS 7.1810 (7.6) (x86\_64) (a partir de IBM Spectrum Protect Plus V10.1.3 parche 1)
- CentOS 7.1908 (7.7) (x86\_64) (a partir de IBM Spectrum Protect Plus V10.1.5 parche 1)
- RHEL 7.5 (x86\_64) (a partir de IBM Spectrum Protect Plus V10.1.2)
- RHEL 7.6 (x86\_64) (a partir de IBM Spectrum Protect Plus V10.1.3 parche 1)
- RHEL 7.7 (x86\_64) (a partir de IBM Spectrum Protect Plus V10.1.5 parche 1)

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

- CentOS 7.3.1611 (x86\_64)
- CentOS 7.4.1708 (x86\_64)
- RHEL 7.3 (x86\_64)
- RHEL 7.4 (x86\_64)

## Puertos del servidor vSnap

Los servidores vSnap utilizan los puertos siguientes.

Tabla 5. Puertos de comunicación cuando el destino es un servidor vSnap				
Puerto	Protocolo	Iniciador	Objetivo	Descripción
22	TCP	Dispositivos virtuales, hipervisores o agentes de IBM Spectrum Protect Plus que utilizan el cliente de NFS	Servidor vSnap	Proporciona acceso a tareas de resolución de problemas y mantenimiento en servidores vSnap utilizando el protocolo SSH.
111	TCP	Hipervisores, proxy VADP o agentes que utilizan el cliente de NFS (Network File System)	Servidor vSnap	Permite que los clientes de Open Network Computing (ONC) descubran puertos para las comunicaciones con servidores ONC.

*Tabla 5. Puertos de comunicación cuando el destino es un servidor vSnap (continuación)*

<b>Puerto</b>	<b>Protocolo</b>	<b>Iniciador</b>	<b>Objetivo</b>	<b>Descripción</b>
445	TCP	Agentes de aplicación que utilizan el protocolo Server Message Block (SMB) o el protocolo Common Internet File System (CIFS)	Servidor vSnap	Proporciona un puerto de destino utilizado por el servidor vSnap a través del protocolo SMB o CIFS para montar recursos compartidos del sistema de archivos para operaciones de copia de seguridad del registro de transacciones y de recuperación.
2049	TCP	Hipervisores, proxy VADP o agentes que utilizan el cliente de NFS (Network File System)	Servidor vSnap	Se utiliza para la compartición de archivos NFS por parte del servidor vSnap.
3260	TCP	Hipervisores, proxy VADP o agentes que utilizan el cliente de iSCSI	Servidor vSnap	Se utiliza para la transferencia de datos iSCSI por medio de servidores vSnap.
8900	TCP	Dispositivo virtual de IBM Spectrum Protect Plus	Servidor vSnap	Da soporte a las comunicaciones de la API REST entre el dispositivo virtual de IBM Spectrum Protect Plus y el servidor vSnap utilizando el protocolo TLS.
20048	TCP	Hipervisores, proxy VADP o agentes que utilizan el cliente de NFS (Network File System)	Servidor vSnap	Monta sistemas de archivos vSnap en clientes tales como proxy VADP, servidores de aplicaciones y almacenes de datos de virtualización. Este puerto también se utiliza para la transferencia de datos NFS a servidores vSnap.

**Información de seguridad importante:** procese solicitudes para los puertos de datos de vSnap (NFS, SMB e iSCSI) solo cuando la solicitud proviene de un nodo de la red interna. Las solicitudes que provienen de nodos de red (no privada) externos deben bloquearse. Para asegurarse de que se siguen las prácticas de seguridad adecuadas, trabaje con el administrador de seguridad de red.

**Actualización de puertos:** En versiones anteriores, los agentes de aplicación que utilizan SMBv1 utilizaban los puertos 137, 138 y 139 del servidor vSnap. A partir de IBM Spectrum Protect Plus V10.1.6, no se utiliza el protocolo SMBv1. Todos los agentes utilizan SMBv2 o posterior, lo que no requiere los puertos 137, 138 o 139.

## Requisitos del proxy VADP

### Instalación del proxy VADP

En IBM Spectrum Protect Plus, la ejecución de trabajos de copia de seguridad de MV mediante VADP requiere recursos de sistema significativos. Al crear proxies de trabajo de copia de seguridad VADP, permite la compartición 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 procesamiento se desplaza desde el dispositivo virtual de IBM Spectrum Protect Plus a los proxies.

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 con una versión de kernel mínima de v2.6.32 en los entornos de Linux siguientes:

- CentOS 6.5 y niveles de mantenimiento y modificación posteriores (a partir de IBM Spectrum Protect Plus V10.1.1 parche 1)
- CentOS 7.0 y niveles de mantenimiento y modificación posteriores (a partir de IBM Spectrum Protect Plus V10.1.1 parche 1)
- RHEL 6.4 y niveles de mantenimiento y modificación posteriores (a partir de IBM Spectrum Protect Plus V10.1.1)
- RHEL 7 y niveles de mantenimiento y modificación posteriores (a partir de IBM Spectrum Protect Plus V10.1.1)
- SUSE Linux Enterprise Server (SLES) 12 y niveles de mantenimiento y modificación posteriores (a partir de IBM Spectrum Protect Plus V10.1.1)

Para obtener más información sobre cómo crear una solución de IBM Spectrum Protect Plus, consulte [Blueprints de IBM Spectrum Protect Plus](#)

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

- Procesador de 4 núcleos de 64 bits
- Se necesitan 8 GB de memoria de acceso aleatorio (RAM), se prefieren 16 GB
- 60 GB de espacio libre en disco

Debido al aumento de utilización del procesador y de la simultaneidad en el servidor proxy VADP, debe aumentarse la memoria asignada en el servidor proxy.

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

Para crear proxies VADP, debe tener un ID de usuario con el rol SYSADMIN asignado. Para obtener más información sobre los roles, consulte [“Gestión de roles” en la página 537](#).



## Puertos de proxy VADP

Los proxies VADP utilizan los puertos siguientes.

Tabla 6. Puertos de comunicación cuando el destino es un host de proxy VADP				
Puerto	Protocolo	Iniciador	Objetivo	Descripción
22	TCP	Dispositivo virtual de IBM Spectrum Protect Plus	Host de proxy VADP	Proporciona acceso para tareas de resolución de problemas y de mantenimiento en hosts de proxy VADP utilizando el protocolo SSH.
8098	TCP	Dispositivo virtual de IBM Spectrum Protect Plus	Host de proxy VADP	Da soporte a las comunicaciones de la API REST entre el dispositivo virtual de IBM Spectrum Protect Plus y el proxy VADP utilizando el protocolo TLS.

Tabla 7. Puertos de comunicación cuando el iniciador es un host de proxy VADP				
Puerto	Protocolo	Iniciador	Objetivo	Descripción
111	TCP	Host de proxy VADP	Servidor vSnap	Permite que los clientes de Open Network Computing (ONC) descubran puertos para las comunicaciones con servidores ONC.
443	TCP	Host de proxy VADP	Hipervisor: host de VMware ESXi y vCenter	Proporciona acceso a ESXi y vCenter para gestionar operaciones.

*Tabla 7. Puertos de comunicación cuando el iniciador es un host de proxy VADP (continuación)*

<b>Puerto</b>	<b>Protocolo</b>	<b>Iniciador</b>	<b>Objetivo</b>	<b>Descripción</b>
902	TCP	Host de proxy VADP	Hipervisor: host de VMware ESXi	Se utiliza para el protocolo NFC (Network File Copy), que proporciona un servicio de Protocolo de transferencia de archivos (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.
2049	TCP	Host de proxy VADP	Servidor vSnap	Se utiliza para transferir la compartición de archivos NFS utilizando el servidor vSnap.
5671	TCP y AMQP	Host de proxy VADP	Dispositivo virtual de IBM Spectrum Protect Plus	Se utiliza para gestionar mensajes producidos y utilizados por el proxy VADP y los trabajadores de gestión de trabajos de VMware. Este puerto es una infraestructura de mensajes RabbitMQ, que también facilita la gestión de registro de trabajo.

Tabla 7. Puertos de comunicación cuando el iniciador es un host de proxy VADP (continuación)

Puerto	Protocolo	Iniciador	Objetivo	Descripción
20048	TCP	Host de proxy VADP	Servidor vSnap	Monta sistemas de archivos vSnap en clientes tales como proxy VADP, servidores de aplicaciones y almacenes de datos de virtualización. Este puerto también se utiliza para la transferencia de datos NFS a servidores vSnap.

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

**Actualizaciones de puerto:** en releases anteriores, el puerto 8761 se utilizaba para descubrir automáticamente proxies VADP y para las operaciones de copia de seguridad de la máquina virtual (MV) de IBM Spectrum Protect Plus. A partir de IBM Spectrum Protect Plus V10.1.6, la arquitectura del proxy VADP se modifica y ya no es necesario que el puerto 8761 esté abierto. Cuando se actualiza IBM Spectrum Protect Plus a V10.1.6, también se actualizan los proxies VADP asociados en el entorno.

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 instrucciones sobre la edición de puertos de cortafuegos, consulte [“Edición de puertos de cortafuegos”](#) en la página 108.

### Proxy VADP en el servidor vSnap

Los proxies VADP se pueden instalar en los 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. Tenga en cuenta los requisitos del sistema de ambos dispositivos y añada los requisitos de núcleo y RAM juntos para identificar los requisitos mínimos de la combinación de proxy VADP y servidor vSnap.

En un proxy VADP instalado en un servidor vSnap virtual, se deben cumplir los requisitos siguientes:

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

Todos los [“Puertos de proxy VADP”](#) en la página 35 y [“Puertos del servidor vSnap”](#) en la página 32 necesarios deben estar abiertos en la combinación proxy VADP y servidor vSnap.

### Requisitos de conectividad

- IBM Spectrum Protect Plus utiliza NFS (Network File System) para montar volúmenes de almacenamiento para operaciones de copia de seguridad y de restauración. En Linux, asegúrese de que el cliente de NFS de Linux nativo esté instalado.
- Todos los servidores, proxies, aplicaciones e hipervisores que se añaden al entorno de IBM Spectrum Protect Plus se pueden registrar utilizando un nombre del Sistema de nombres de dominio (DNS) o una dirección IP (Protocolo Internet).
- Si se utilizan nombres DNS, deben poder resolverse en la red mediante el servidor de dispositivos virtuales IBM Spectrum Protect Plus y desde el servidor vSnap. Todos los componentes de IBM Spectrum Protect Plus también deben poder resolverse mediante sus nombres de DNS.

- Si el DNS no está disponible, debe añadir el servidor al archivo `/etc/hosts` en el dispositivo virtual de IBM Spectrum Protect Plus utilizando la línea de mandatos.

### Requisitos de almacenamiento del servidor de repositorio

Si tiene previsto utilizar IBM Spectrum Protect como servidor de repositorio para copiar datos en el almacenamiento en la nube, asegúrese de que utiliza IBM Spectrum Protect V8.1.10.

### Requisitos de almacenamiento en la nube

#### Área de memoria caché de disco

Para todas las funciones relacionadas con las operaciones de copia de datos y de restauración a y desde los destinos de archivado y de nube, el servidor vSnap requiere que un área de memoria caché de disco esté presente en el servidor vSnap:

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

Para obtener instrucciones sobre el dimensionamiento y la instalación de la memoria caché, consulte [Blueprints de IBM Spectrum Protect Plus](#).

#### Múltiples de acceso

Durante las operaciones de copia en el almacenamiento de objetos, IBM Spectrum Protect Plus conecta y desconecta los dispositivos de nube virtuales en los servidores vSnap. Si la configuración de múltiples rutas está habilitada en el servidor vSnap mediante **dm-multipath**, la configuración puede interferir con la operación de copia. Para evitar esta interferencia, los dispositivos de nube virtual deben excluirse de la configuración de múltiples rutas. Añada las líneas siguientes en la sección de lista negra del archivo de configuración de múltiples rutas `/etc/multipath.conf`:

```
blacklist
{
    device {
        vendor "LIO-ORG"
        product ".*"
    }
}
```

Después de realizar este cambio, vuelva a cargar la configuración de múltiples rutas utilizando el mandato siguiente:

```
sudo systemctl reload multipathd
```

#### Certificados

- **Certificados autofirmados:** si el punto final de nube o el servidor de repositorio utiliza un certificado autofirmado, debe especificar el certificado en formato PEM (Privacy Enhanced Mail) cuando registre 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, debe añadir el certificado raíz o intermedio de la CA privada al almacén de certificados del sistema en cada servidor vSnap utilizando el siguiente procedimiento:
  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 nube utiliza un certificado firmado por CA, no se necesita ninguna acción especial. El servidor vSnap valida el certificado utilizando el almacén de certificados del sistema predeterminado.

## Red

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

Tabla 8. Puertos de comunicación cuando el destino es un punto final de servidor de nube o servidor de repositorio				
Puerto	Protocolo	Iniciador	Objetivo	Descripción
443	TCP	Servidor vSnap	Puntos finales del servidor de nube	Permite que el servidor vSnap se comuniquen con los puntos finales de Amazon Simple Storage Service (S3), Microsoft Azure o IBM Cloud Object Storage.
9000	TCP	Servidor vSnap	Puntos finales de servidor de repositorio	Permite que el servidor vSnap se comuniquen con los puntos finales de IBM Spectrum Protect (servidor de repositorio).

Los cortafuegos o proxies de red que inspeccionan la SSL o que realizan una inspección profunda de paquetes de tráfico entre los servidores vSnap y los puntos finales de nube pueden interferir con la validación de certificados SSL en servidores vSnap. Esta interferencia también puede provocar errores en el trabajo de copia en la nube. Para impedir esta interferencia, los servidores vSnap deben estar exentos de la interceptación SSL y de la inspección en la configuración del cortafuegos o de proxy.

## Proveedor de 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 siempre incremental 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

- **Almacenamiento de objetos estándar:** cuando se registra el proveedor de nube en IBM Spectrum Protect Plus, debe especificarse 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.

- **Almacenamiento de objetos de archivado:** cuando se registra el proveedor de nube en IBM Spectrum Protect Plus, debe especificarse 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 carga directamente archivos de datos en el nivel de 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 almacenamiento de objetos de IBM Cloud**

- **Almacenamiento de objetos estándar:** cuando el proveedor de nube está registrado en IBM Spectrum Protect Plus, se debe especificar un grupo existente. Si el grupo especificado tiene una política WORM (Grabar una vez leer varias) 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. El grupo debe tener habilitado el valor Índice de nombres.
- **Almacenamiento de objetos de archivado:** cuando el proveedor de nube está registrado en IBM Spectrum Protect Plus, debe especificarse 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. El grupo debe tener habilitado el valor Índice de nombres.

• **Requisitos de Microsoft Azure**

- **Almacenamiento de objetos estándar:** cuando el proveedor de nube está registrado en IBM Spectrum Protect Plus, debe especificarse un contenedor existente en una cuenta de almacenamiento en caliente o en frío.
- **Almacenamiento de objetos de archivado:** cuando el proveedor de nube está registrado en IBM Spectrum Protect Plus, debe especificarse un contenedor existente en una cuenta de almacenamiento en caliente o en frío. 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)**

- **Almacenamiento de objetos estándar:** cuando el proveedor de nube está registrado 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.
- **Almacenamiento de objetos de archivado:** cuando el proveedor de nube está registrado 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 en 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 en cintas de IBM Spectrum Protect para fines de recuperación tras desastre.

Tabla 9. Requisitos de copia y copia archivada para proveedores de nube		
Operación	Proveedor	Requisitos
Copia	Amazon S3	Se debe especificar un grupo existente de uno de los niveles de almacenamiento soportados.

Tabla 9. Requisitos de copia y copia archivada para proveedores de nube (continuación)		
Operación	Proveedor	Requisitos
Copia	IBM Cloud Object Storage	Se debe especificar un grupo existente. El grupo debe tener habilitado el valor Índice de nombres.
Copia	Microsoft Azure	Debe especificarse un contenedor existente desde un nivel de almacenamiento en frío o en caliente.
Copia	IBM Spectrum Protect	IBM Spectrum Protect Plus crea su propio grupo exclusivo.
Copia archivada	Amazon S3	El servidor vSnap debe poder comunicarse con los puntos finales de IBM Spectrum Protect (servidor de repositorio).
Copia archivada	IBM Cloud Object Storage	Se debe especificar un grupo existente del nivel de archivado. El grupo debe tener habilitado el valor Índice de nombres.
Copia archivada	Microsoft Azure	Se debe especificar un contenedor existente del nivel de almacenamiento dinámico y del nivel de archivado.
Copia archivada	IBM Spectrum Protect	IBM Spectrum Protect Plus crea su propio grupo exclusivo que se copiará en cinta de IBM Spectrum Protect.

## Requisitos de copia de seguridad y restauración de hipervisor (Microsoft Hyper-V y VMware) e instancia en la nube (Amazon EC2)

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 obtener los requisitos más actuales, que pueden incluir actualizaciones, consulte [Nota técnica 304861](#).

### 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
- Hyper-V Server 2019 (a partir de IBM Spectrum Protect Plus V10.1.4) o Microsoft Hyper-V on Windows Server 2019 (a partir de IBM Spectrum Protect Plus V10.1.3)

IBM Spectrum Protect Plus protege máquinas virtuales (MV) que pueden utilizar la característica Hyper-V Replica. En función del entorno de Hyper-V, es posible que se deba actualizar alguna política de acuerdo de nivel de servicio (SLA) al actualizar el entorno del sistema a IBM Spectrum Protect Plus V10.1.6. Para obtener más información sobre los requisitos para actualizar máquinas virtuales en entornos de Hyper-V, “Pasos adicionales para actualizar máquinas virtuales en entornos de Hyper-V Replica” en la página 188,

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 de los datos de Hyper-V, como se describe en [“Copia de seguridad y restauración de datos de Hyper-V”](#) en la [página 284](#).

Antes de configurar servidores Hyper-V, revise los requisitos para cada paso de configuración:

- Registrando los proveedores de los que desea hacer copia de seguridad.

Los servidores Hyper-V se pueden registrar utilizando un nombre del Sistema de nombres de dominio (DNS) o una dirección de Protocolo Internet Protocol (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 deben poder resolverse mediante DNS. Si el DNS no está disponible, debe añadir el servidor al archivo `/etc/hosts` en el dispositivo virtual 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.

- Configuración de políticas de SLA.

Si una máquina virtual está asociada con varias políticas de SLA, asegúrese de que las políticas no están planificadas 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 una máquina virtual está protegida por una política de SLA, las copias de seguridad de la máquina virtual se retienen en función de los parámetros de retención de la política de SLA, incluso si se elimina la máquina virtual.

- Asegúrese de que los servicios de integración de Hyper-V más recientes están instalados:

- En entornos de Microsoft Windows, consulte [Sistemas operativos de invitado soportados de Windows para Hyper-V en Windows Server](#)
- En entornos de Linux®, consulte [Máquinas virtuales soportadas de Linux y FreeBSD para Hyper-V en Windows](#)

Antes de realizar una copia de seguridad o restaurar datos de Hyper-V, realice las acciones siguientes:

- Asegúrese de que el servicio del iniciador iSCSI de Microsoft se está ejecutando en todos los servidores Hyper-V, incluidos los nodos de clúster. En la ventana **Servicios**, establezca el tipo de inicio para que 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.

- Asegúrese de que los roles y grupos de recursos adecuados se asignan a los usuarios que iniciarán las operaciones de copia de seguridad y restauración. Otorgue a los usuarios acceso a roles y grupos de recursos utilizando el panel **Cuentas**. Añada el usuario al grupo de administradores locales en el servidor Hyper-V.
- Si tiene previsto restaurar una máquina virtual utilizando la modalidad de clonación y utilizando la configuración de IP original, asegúrese de que las credenciales se establezcan mediante el nombre de usuario de SO de invitado y las opciones de contraseña de SO de invitado en la definición de trabajo de copia de seguridad.

#### Restricciones

- En los datos de Hyper-V, las operaciones de copia de seguridad y de restauración solo se soportan para discos duros virtuales (VHDX). Para obtener más información, consulte [Problemas conocidos y limitaciones: IBM Spectrum Protect Plus V10.1.6.x](#)
- Al restaurar los archivos de restauración de un archivo de IBM Spectrum Protect, los archivos se migran inicialmente desde el almacenamiento en cintas a una agrupación de transferencia. Dependiendo del tamaño de los archivos que se van a restaurar, este proceso puede tardar varias horas.



## Requisitos de VMware

Se da soporte a las siguientes versiones de VMware vSphere :

- 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 los niveles de parche (a partir de IBM Spectrum Protect Plus V10.1.2)
- vSphere 7.0, incluidas todas las actualizaciones y los niveles de parche (a partir de IBM Spectrum Protect Plus V10.1.6)

Asegúrese de que esté instalada la versión más reciente de Herramientas de VMware en máquinas virtuales de VMware.

IBM Spectrum Protect Plus da soporte a etiquetas de máquina virtual de VMware.

La copia de seguridad y restauración de la máquina virtual restaurada se soporta con vSphere 6.5 y posterior.

Es posible que un volumen NFS (Network File System) esté montado en varios centros de datos que pertenezcan al mismo vCenter. Si el volumen NFS se monta en más de un centro de datos, vCenter trata el mismo volumen como dos almacenes de datos diferentes. IBM Spectrum Protect Plus lo trata como un único almacén de datos y combina todas las máquinas virtuales y los discos de máquina virtual (VMDK) que residen en el almacén de datos de todos los centros de datos en los que está montado el almacén de datos. Cualquier selección de SLA en este almacén de datos hará que se realicen copias de datos de todas las máquinas virtuales de los diferentes centros de datos o que se restauren en IBM Spectrum Protect Plus.

IBM Spectrum Protect Plus V10.1.5 y posterior protege las máquinas virtuales gestionadas por VMware Cloud (VMC) en un Software-Defined Data Center (SDDC) de Amazon Web Services (AWS). Para obtener más información, consulte [IBM Spectrum Protect Plus for VMware Cloud on AWS](#)

Para proteger los datos de VMware, primero añada instancias de vCenter Server a IBM Spectrum Protect Plus y, a continuación, cree trabajos para hacer copias de seguridad y restauración de los datos, como se describe en [“Copia de seguridad y restauración de datos de VMware”](#) en la página 257.

- Cuando se añade una instancia de vCenter Server a IBM Spectrum Protect Plus, se captura un inventario de la instancia. El inventario es necesario para que los usuarios puedan completar trabajos de copia de seguridad y restauración y ejecutar informes.
- Debe configurarse al menos una política de SLA para los datos de VMware.
- 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 roles y grupos de recursos utilizando el panel Cuentas.
- Si una máquina virtual está asociada con varias políticas de SLA, asegúrese de que las políticas no están planificadas 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.
- Asegúrese de que los destinos para los trabajos de restauración se registran en IBM Spectrum Protect Plus. Este requisito se aplica a los trabajos de restauración que restauran los datos a los hosts o clústeres nuevos.
- Si tiene previsto restaurar una máquina virtual utilizando la modalidad de clonación y utilizando la configuración de IP original, asegúrese de que las credenciales se establezcan mediante el nombre de usuario de SO de invitado y las opciones de contraseña de SO de invitado en la definición de trabajo de copia de seguridad.

Restricciones

- Las plantillas de máquina virtual restauradas no se pueden encender después de la recuperación de una máquina virtual.
- Las claves de Secure Shell (SSH) no son un mecanismo de autorización válido para plataformas Windows.
- Asegúrese de que la versión más reciente de Herramientas de VMware esté instalada en el entorno.
- 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 la máquina virtual.

## Requisitos de Amazon EC2

A partir de IBM Spectrum Protect Plus V10.1.6, se añade soporte o copia de seguridad y restauración de datos en instancias de Amazon EC2.

Para proteger los datos de Amazon EC2, primero añada una cuenta de EC2 a IBM Spectrum Protect Plus y, a continuación, cree trabajos para las operaciones de copia de seguridad y restauración para las instancias de EC2 asociadas con dicha cuenta, tal como se describe en [“Copia de seguridad y restauración de datos de Amazon EC2”](#) en la página 297.

Antes de realizar una copia de seguridad o restaurar los datos de Amazon EC2, revise los requisitos siguientes:

- Para añadir una cuenta de EC2 a IBM Spectrum Protect Plus, se necesitan claves de acceso. Las claves de acceso son credenciales a largo plazo para un usuario de gestión de identidad y acceso (IAM) o el usuario root de la cuenta AWS.
- Cuando se añade una cuenta de Amazon EC2 a IBM Spectrum Protect Plus, se captura un inventario de las instancias asociadas con la cuenta. Después, puede ejecutar trabajos de copia de seguridad y restauración y generar informes para las instancias.
- Asegúrese de que se han configurado una o más políticas de SLA para las instancias de EC2.
- Asegúrese de que los roles y los grupos de recursos de IBM Spectrum Protect Plus estén asignados al usuario que configurará los trabajos de copia de seguridad y de restauración.
- Si una cuenta está asociada con varias políticas de SLA, asegúrese de que las políticas no están planificadas 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.
- Asegúrese de que los destinos que tiene previsto utilizar para trabajos de restauración estén registrados en IBM Spectrum Protect Plus.

## 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 obtener los requisitos más actuales, que pueden incluir actualizaciones, consulte [Nota técnica 304861](#).

### General

- En operaciones de hipervisor, IBM Spectrum Protect Plus solo soporta los sistemas operativos que están disponibles en los hipervisores. Para obtener información sobre los sistemas operativos soportados, revise la documentación del hipervisor.
- IBM Spectrum Protect Plus puede proteger y restaurar máquinas virtuales (MV) con sistemas de archivos que no se listan en esta documentación, pero solo los sistemas de archivos listados previamente son elegibles para operaciones de indexación y restauración de archivos.

- Los discos de Internet Small Computer Interface (iSCSI) que se correlacionan directamente con el sistema operativo de invitado no se indexarán. Los volúmenes soportados incluyen volúmenes de disco de máquina virtual (VMDK) montados según lo especificado por 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 en el entorno. Para catalogar 1 millón de archivos, el volumen de catálogo del dispositivo virtual IBM Spectrum Protect Plus requiere 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.
- La indexación de archivos y la restauración de archivos no están soportadas en los puntos de restauración que se copiaron en los recursos de nube o servidores de repositorio.
- Un archivo se puede restaurar en una ubicación alternativa solo si se han establecido credenciales para la máquina virtual alternativa mediante la opción **Nombre de usuario de SO de invitado** y **Contraseña de SO de invitado** en la definición de trabajo de copia de seguridad.

### Requisitos de VMware

- Asegúrese de que esté instalada la versión más reciente de Herramientas de VMware en máquinas virtuales de VMware.
- En los valores de MV en Configuración avanzada, el parámetro **disk.EnableUUID** debe establecerse en true.

### Requisitos de Hyper-V

- Asegúrese de que está instalada la versión más reciente de los Servicios de integración de Hyper-V en las MV de Hyper-V.
- Las operaciones de indexación y restauración de archivos soportan discos SCSI (Interfaz para pequeños sistemas) en un entorno de Hyper-V:
  - Solo los volúmenes de los discos SCSI son aptos para la catalogación de archivos y la restauración de archivos.
  - Los discos IDE (Integrated Drive Electronics) no están soportados.

### Requisitos de Windows










Tabla 10. Matriz de cobertura para sistemas operativos soportados en Windows x64				
IBM Spectrum Protect Plus	Windows Server 2008 R2* Ediciones Standard y Datacenter	Windows Server 2012 R2 y Windows Server 2012R2 core* Ediciones Standard y Datacenter	Windows Server 2016 y Windows Server 2016 core* Ediciones Standard y Datacenter	Windows Server 2019 y Windows Server 2019 core* Ediciones Standard y Datacenter
V10.1.0				--
V10.1.1				--
V10.1.2				--

Tabla 10. Matriz de cobertura para sistemas operativos soportados en Windows x64 (continuación)

IBM Spectrum Protect Plus	Windows Server 2008 R2* Ediciones Standard y Datacenter	Windows Server 2012 R2 y Windows Server 2012R2 core* Ediciones Standard y Datacenter	Windows Server 2016 y Windows Server 2016 core* Ediciones Standard y Datacenter	Windows Server 2019 y Windows Server 2019 core* Ediciones Standard y Datacenter
V10.1.3	✓	✓	✓	✓ (solo Windows Server 2019 core)
V10.1.4	✓	✓	✓	✓
V10.1.5	✓	✓	✓	✓
V10.1.6	✓	✓	✓	✓
* Se admiten el release base y los niveles de mantenimiento posteriores.				

Tabla 11. Matriz de cobertura para sistemas de archivos soportados y tipos de almacenamiento de disco

<b>Sistemas de archivos soportados</b>	<ul style="list-style-type: none"> <li>• New Technology File System (NTFS)</li> <li>• Resilient File System (ReFS)</li> <li>• Tabla de asignación de archivos (FAT)</li> </ul>
<b>Tipos de almacenamiento de disco soportados</b>	<p>Discos básicos con las particiones siguientes:</p> <ul style="list-style-type: none"> <li>• MBR (Master Boot Record)</li> <li>• GPT (GUID Partition Table)</li> </ul> <p><b>Restricción:</b> No puede realizar copias de seguridad o restaurar archivos en discos dinámicos.</p>

### Restricciones

- Se debe habilitar el shell remoto de Windows (WinRM).
- **Importante:** IBM Spectrum Protect Plus puede proteger y restaurar máquinas virtuales con sistemas de archivos que no se listan en este documento, pero solo los sistemas de archivos listados son elegibles para la indexación y restauración de archivos.
- Cuando se indexan archivos en un entorno de Windows, se omiten los directorios siguientes en el recurso:

```

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

```

Los archivos de estos directorios no se añaden al inventario de IBM Spectrum Protect Plus y no están disponibles para la recuperación de archivos.

- La indexación de archivos y la restauración de archivos de una máquina virtual de Windows requieren que la vía de acceso binaria de Windows PowerShell esté establecida en la variable de entorno %PATH %.
- Los sistemas de archivos Windows cifrados no están soportados para la catalogación de archivos o la restauración de archivos.
- Al restaurar archivos en un entorno de Resilient File System (ReFS), no se da soporte a los trabajos de restauración de versiones más recientes de Windows Server a versiones anteriores. Por ejemplo, no puede restaurar un archivo de Windows Server 2016 a Windows Server 2012.
- La catalogación de archivos, copia de seguridad, restauraciones de un punto en el tiempo y otras operaciones que invocan el agente Windows fallarán si se especifica un administrador local no predeterminado como Nombre de usuario de SO de invitado al definir 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 LocalAccountTokenFilterPolicy en 1 en el invitado de Windows del que se está realizando 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.

### **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 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 virtual de IBM Spectrum Protect Plus debe poder resolverse desde la máquina virtual de Windows.
- La dirección el Protocolo Internet (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 que se ha seleccionado para la indexación debe dar soporte a las conexiones de salida al puerto 22, que utiliza el protocolo Secure Shell (SSH), en el dispositivo virtual de IBM Spectrum Protect Plus.
- El servicio de Microsoft Windows Remote Management (WinRM) debe estar en ejecución.
- Los cortafuegos deben configurarse para permitir que IBM Spectrum Protect Plus se conecte al servidor utilizando WinRM.
- La dirección IP de la máquina que registra debe ser accesible desde el servidor IBM Spectrum Protect Plus y desde el servidor vSnap. Ambos servidores deben tener un servicio WinRM que esté a la escucha en el puerto 5985.
- Todos los servidores, proxies, aplicaciones e hipervisores que se añaden al entorno de IBM Spectrum Protect Plus se pueden registrar utilizando un nombre del Sistema de nombres de dominio (DNS) o una dirección IP (Protocolo Internet).
- Si se utilizan nombres DNS, deben poder resolverse en la red mediante el servidor de dispositivos virtuales IBM Spectrum Protect Plus y desde el servidor vSnap. Todos los componentes de IBM Spectrum Protect Plus también deben poder resolverse mediante sus nombres de DNS.

## Requisitos de autenticación y privilegios

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

- La identidad de usuario debe tener el derecho **Iniciar sesión como servicio**, que se asigna al panel de control Herramientas administrativas en el servidor 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 Windows Challenge/Response (NTLM) y la identidad de usuario sigue el formato domain\Name 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. Deben establecerse las credenciales para la máquina virtual asociada utilizando las opciones **Nombre de usuario de SO de invitado** y **Contraseña de SO de invitado** en la definición de trabajo de copia de seguridad.
- Las credenciales de inicio de sesión en el sistema deben tener los permisos del administrador local.

## Requisitos de Kerberos

- La autenticación basada en Kerberos puede habilitarse a través de un archivo de configuración en el dispositivo virtual de IBM Spectrum Protect Plus. Este valor alterará temporalmente el protocolo NTLM predeterminado de Windows. Kerberos no da soporte al uso de cuentas de usuario locales y solo es adecuado para entornos en los que todas las máquinas virtuales están en un único 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) del centro de distribución de claves (KDC) en el dominio especificado por el nombre de dominio completo.
- La autenticación Kerberos también requiere que el desfase horario entre el controlador de dominio y el dispositivo virtual de IBM Spectrum Protect Plus sea inferior a 5 minutos. El protocolo NTLM de Windows predeterminado no depende del tiempo.

## Requisitos del objeto de política de grupo

Puede especificar el valor de Objeto de política de grupo (GPO) navegando a:

- **Configuración del sistema > Políticas > Valores de Windows > Configuración de seguridad > Políticas locales > Opciones de seguridad > Seguridad de red: Restringir NTLM: tráfico de NTLM entrante**

O bien,

- **Configuración del sistema > Políticas > Valores de Windows > Configuración de seguridad > Políticas locales > Opciones de seguridad > Seguridad de red: Restringir NTLM: tráfico de NTLM de salida**

A continuación, elija una de las opciones siguientes:

- **Permitir todo**
- **Permitir todas las cuentas**

## Requisitos de Linux

Tabla 12. Matriz de cobertura para sistemas operativos soportados en Linux® x86\_64

IBM Spectrum Protect Plus	RHEL 6.4*	RHEL 7.0*	RHEL 8.0*	CentOS 6.4*	CentOS 7.0*	CentOS 8.0*	SLES 12.0*	SLES 15.0*
V10.1.0	✓	✓	--	✓	✓	--	✓	--
V10.1.1	✓	✓	--	✓	✓	--	✓	--
V10.1.2	✓	✓	--	✓	✓	--	✓	--
V10.1.3	✓	✓	--	✓	✓	--	✓	--
V10.1.4	✓	✓	--	✓	✓	--	✓	--
V10.1.5	✓	✓	--	✓	✓	--	✓	--
V10.1.6	✓	✓	✓	✓	✓	✓	✓	✓

\* Se admiten el release base y los niveles de mantenimiento posteriores.

Tabla 13. Matriz de cobertura para sistemas de archivos soportados

<b>Sistemas de archivos soportados</b>	<ul style="list-style-type: none"> <li>• ext2</li> <li>• ext3</li> <li>• ext4</li> <li>• XFS</li> </ul>
----------------------------------------	---------------------------------------------------------------------------------------------------------

## Restricciones

- Es posible que un sistema de archivos creado en una versión de kernel más reciente no pueda montarse en un sistema con una versión de kernel anterior. En este caso, no se da soporte a la restauración de archivos desde el sistema más reciente al sistema antiguo.
- Cuando los archivos se indexan en un entorno de 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 se indexan los sistemas de archivos, se generan archivos de metadatos temporales en el directorio `/tmp` y, después, se suprimen cuando se completa la indexación. La cantidad de espacio libre necesario para los metadatos depende del número total de archivos en el sistema. Asegúrese de que hay aproximadamente 350 MB de espacio libre por 1 millón de archivos.

### Requisitos de software

- Los paquetes **bash** y **sudo** deben estar instalados. El paquete **sudo** debe ser la versión 1.7.6p2 o posterior. Ejecute **sudo -V** para comprobar la versión.

**Consejo:** Los paquetes **bash** y **sudo** necesarios se incluyen en los sistemas operativos Linux 86\_64 soportados.

- Asegúrese de que está instalada la versión soportada de Linux x86\_64.
- El paquete RPM de International Components for Unicode (libicu) correspondiente al sistema operativo debe estar instalado.
- En un entorno de Linux, asegúrese de que el paquete del programa de utilidad de Linux `util-linux-ng` o el paquete **util-linux** es actual.
- Asegúrese de que el valor **ulimit -f** de tamaño de archivo efectivo para el usuario de agente de IBM Spectrum Protect Plus y el usuario de instancia de IBM 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.
- **Usuarios de Red Hat® Enterprise Linux y CentOS 6:**

Asegúrese de que el paquete `util-linux-ng` sea actual ejecutando el mandato siguiente:

```
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 de gestor de volúmenes lógicos (LVM), asegúrese de que la versión de LVM sea 2.0.2.118 o posterior.

Ejecute el mandato **lvm version** para comprobar la versión y ejecute el mandato **yum update lvm2** para actualizar el paquete si es necesario.

- Si los datos residen en volúmenes LVM, el servicio **lvm2-lvm2d** debe estar inhabilitado, ya que puede interferir con la capacidad de IBM Spectrum Protect Plus para montar y volver a firmar el grupo de volúmenes instantáneas y clones. Para inhabilitar el servicio, complete los pasos siguientes:

1. Ejecute los mandatos siguientes:

```
systemctl stop lvm2-lvm2d
systemctl disable lvm2-lvm2d
```

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

```
use_lvm2d = 0
```

Para obtener más información, consulte [Daemon de metadatos \(lvm2d\)](#).

- Si los datos residen en sistemas de archivos XFS y la versión del paquete `xfsprogs` es entre 3.2.0 y 4.1.9, la operación de restauración de archivos puede fallar debido a un problema conocido en **xfsprogs** que causa la corrupción de un sistema de archivos de instantánea o de un clon cuando se modifica su UUID (Universally Unique Identifier). Para resolver este problema, actualice **xfsprogs** a la versión 4.2.0 o posterior. Para obtener más información, consulte [Registros de informes de error Debian](#)

### Requisitos de conectividad

- El subsistema secure file transfer protocol (SFTP) para SSH está habilitado.



- El servicio SSH se está ejecutando en el puerto 22 en el servidor de host de proxy.
- Los cortafuegos están configurados para permitir que IBM Spectrum Protect Plus se conecte al servidor de host de proxy utilizando SSH.
- IBM Spectrum Protect Plus utiliza NFS (Network File System) para montar volúmenes de almacenamiento para operaciones de copia de seguridad y de restauración. En Linux, asegúrese de que el cliente de NFS de Linux nativo esté instalado.
- Todos los servidores, proxies, aplicaciones e hipervisores que se añaden al entorno de IBM Spectrum Protect Plus se pueden registrar utilizando un nombre del Sistema de nombres de dominio (DNS) o una dirección IP (Protocolo Internet).
- Si se utilizan nombres DNS, deben poder resolverse en la red mediante el servidor de dispositivos virtuales IBM Spectrum Protect Plus y desde el servidor vSnap. Todos los componentes de IBM Spectrum Protect Plus también deben poder resolverse mediante sus nombres de DNS.
- Si el DNS no está disponible, debe añadir el servidor al archivo `/etc/hosts` en el dispositivo virtual de IBM Spectrum Protect Plus utilizando la línea de mandatos.

### Requisitos de autenticación y privilegios

IBM Spectrum Protect Plus requiere privilegios de usuario raíz utilizando **sudo** para diversas tareas tales como el descubrimiento de diseños de almacenamiento, el montaje y desmontaje de discos y la gestión de bases de datos. Las credenciales de la máquina virtual deben especificar un usuario con los privilegios de **sudo** siguientes:

- La configuración de `sudoers` debe permitir que el usuario ejecute mandatos sin una contraseña.
- Debe especificarse el valor `!requiretty`.

El método recomendado consiste en crear un usuario agente de IBM Spectrum Protect Plus dedicado con los privilegios que se muestran en la configuración de ejemplo:

- Cree el usuario emitiendo el mandato:

```
useradd -m sppagent
```

donde `sppagent` especifica el usuario agente de IBM Spectrum Protect Plus

- Establezca una contraseña utilizando el mandato:

```
passwd sppagent_password
```

- Para habilitar privilegios de superusuario para el usuario agente, establezca el valor **!requiretty**. Al final del archivo de configuración `/etc/sudoers`, añada las líneas siguientes:

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

Si el archivo `sudoers` está configurado para importar configuraciones desde otro directorio, por ejemplo `/etc/sudoers.d`, puede añadir las líneas en el archivo adecuado en dicho directorio..

### Requisitos de Sistema de archivos



Antes de registrar Microsoft Windows sistemas de archivos con IBM Spectrum Protect Plus, asegúrese de que el entorno del sistema cumple los requisitos indicados.

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 obtener los requisitos más actuales, que pueden incluir actualizaciones, consulte [Nota técnica 304861](#).

Los requisitos de copia de seguridad y restauración de IBM sistemas de archivos para IBM Spectrum Protect Plus son los siguientes.


## Configuración

### Versiones de la aplicación

IBM Spectrum Protect Plus	Microsoft Windows Resilient File System (ReFS)	Microsoft New Technology File System (NTFS)
V10.1.6		

**Restricción:** Incluso si se detectan otros sistemas de archivos de Microsoft Windows , como por ejemplo la tabla de asignación (FAT), durante el proceso de inventario, estos sistemas de archivos no se pueden añadir a trabajos o protegidos.

### Sistemas operativos

IBM Spectrum Protect Plus	Ediciones de Microsoft Windows Server 2012 R2* Standard y Datacenter	Ediciones de Microsoft Windows Server 2016* Standard y Datacenter	Ediciones de Microsoft Windows Server 2019* Standard y Datacenter
V10.1.6			
*Se admiten el release base y los niveles de mantenimiento posteriores (kernel de 64 bits).			

IBM Spectrum Protect Plus da soporte al servidor de host de proxy que se ejecuta en servidores físicos (bare metal) y en un entorno virtualizado.

### Restricciones

Se aplican las siguientes restricciones:

- IBM Spectrum Protect Plus no protege los recursos compartidos del sistema de archivos o volúmenes de clúster de Microsoft.
- Los sistemas de archivos de Microsoft FAT no están soportados.
- Los archivos de resguardo de IBM Spectrum Protect HSM for Windows no están soportados.
- Asegúrese de que la configuración del sistema de archivos no incluye puntos de montaje anidados.
- Los recursos compartidos de red no son ubicaciones alternativas válidas para los trabajos de restauración.
- Los trabajos de inventario no deben planificarse para ejecutarse al mismo tiempo que los trabajos de copia de seguridad.

### Autenticación y privilegios

#### Autenticación

Para registrar un sistema de archivos de Windows, se debe registrar un usuario de administración de IBM Spectrum Protect Plus en el host de cliente donde están ubicados los sistemas de archivos que se deben proteger.

Los servidores de archivos de Windows se pueden registrarse con el ID de usuario administrador. Es posible registrar el servidor de archivos utilizando un ID de usuario de dominio, si dicho usuario es el administrador de dominio o un usuario local con privilegios de administrador.

#### Privilegios

El ID de usuario para registrar servidores de archivos de Windows se puede configurar con una de las siguientes configuraciones de Windows:

- Inhabilite la cuenta de usuario administrador del sistema local con el componente de seguridad de Control de cuenta de usuario (UAC).
  - Abra el panel de control del sistema **Windows > Valores de control de cuenta de usuario**
  - Mueva el deslizador a **No notificar nunca**.
- Inhabilite el valor de política de seguridad de Modalidad de aprobación de administrador para un usuario que sea miembro del grupo de administradores locales.
  - con este usuario, abra la política de seguridad local del sistema **Windows**
  - desde el menú **Configuración de seguridad**, seleccione **Políticas locales > Opciones de seguridad > Control de cuenta de usuario: Ejecutar todos los administradores** en la política **Modalidad de aprobación de administrador**
  - inhabilite **Control de cuenta de usuario: Ejecutar todos los administradores**
  - Asegúrese de que el **Grupo de administradores locales** incluye la política **Iniciar sesión como servicio**.

Consulte también [Valores de la política de grupo de Control de cuenta de usuario y de la clave de registro](#)

## Requisitos previos y operaciones

### Requisitos previos

Antes de empezar a proteger los recursos, deben cumplirse los requisitos previos siguientes. Para obtener los detalles, consulte [Requisitos previos para sistemas de archivos](#).

- Antes de empezar a hacer una copia de seguridad de los datos que se almacenan en el sistema de archivos registrado, asegúrese de que tiene suficiente espacio libre de disco en el host de copia de seguridad en el repositorio de vSnap.
- Si tiene previsto restaurar datos en una ubicación alternativa, permita espacio adicional. Los archivos no se sobrescriben durante el proceso de restauración. Cuando se encuentran archivos con nombres idénticos, se conservan ambas copias.
- Si se está ejecutando el agente de sistema de archivos de IBM Spectrum Protect Plus, se crean una clave y un certificado autofirmado. Puede aumentar el acceso seguro para proteger los archivos del sistema de archivos con IBM Spectrum Protect Plus creando un certificado y gestionando su ubicación.

### Operaciones

Antes de iniciar una operación de copia de seguridad o restauración:

- Para empezar a proteger los datos en un ReFS o NTFS, debe añadir la dirección de host donde se encuentra el sistema de archivos. Puede repetir el procedimiento para añadir cada host que desee proteger con IBM Spectrum Protect Plus, tal como se describe en [Adición de un servidor de sistema de archivos](#).
- Para que un usuario de IBM Spectrum Protect Plus pueda implementar operaciones de copia de seguridad y restauración, deben asignarse roles y grupos de recursos al usuario. Otorgue a los usuarios acceso a las operaciones de copia de seguridad y restauración utilizando el panel Cuentas. Para obtener instrucciones, consulte [Gestión de acceso de usuario](#).
- Configure una política de acuerdo de nivel de servicio (SLA). Para obtener instrucciones, consulte [Definición de un trabajo de copia de seguridad de Acuerdo de nivel de servicio](#).

Revise la información siguiente sobre la creación de trabajos de copia de seguridad y restauración:

- Durante la copia de seguridad inicial, IBM Spectrum Protect Plus crea un nuevo volumen de vSnap y un recurso compartido de Common Internet File System (CIFS). Durante las copias de seguridad incrementales, se reutiliza el volumen creado previamente. El agente de sistema de archivos de IBM Spectrum Protect Plus monta el recurso compartido en el servidor donde se va a completar la copia de seguridad, como se describe en [Copia de seguridad de datos del sistema de archivos](#).
- En un trabajo de copia de seguridad, puede definir reglas de exclusión para excluir determinadas unidades, directorios o archivos. No se hace copia de seguridad de estos archivos como parte de la

política de SLA o como parte de un trabajo de copia de seguridad ad hoc. Cuando ejecuta un trabajo de restauración, las reglas de exclusión significan que las unidades, directorios o archivos especificados en las reglas de exclusión no se restauran en la nueva copia. Para obtener más información, consulte [Excluir sintaxis de reglas](#).

- Para restaurar los datos del sistema de archivos del repositorio de vSnap, defina un trabajo que restaure datos de la copia de seguridad más reciente o de una copia de seguridad anterior. Puede restaurar datos en la ubicación original o en una ubicación alternativa, que puede estar en un host de cliente diferente. También puede especificar otras opciones de recuperación, como se describe en [Restauración de datos del sistema de archivos](#).
- No se realiza el seguimiento del proceso de restauración en la página Trabajos y operaciones de IBM Spectrum Protect Plus. Utilice el navegador de Restauración a nivel de archivo de los sistemas de archivos para especificar las unidades, directorios y archivos para el trabajo. Puede definir una ubicación alternativa para la operación de restauración y supervise el trabajo de restauración hasta que se complete en el navegador.
- Asegúrese de que el objetivo del destino de IBM Spectrum Protect para el trabajo de restauración se ha registrado y configurado correctamente.
- Cuando finaliza el trabajo de restauración, debe eliminar el recurso de la pestaña Recursos activos en la ventana Trabajos y operaciones. No puede ejecutar otro trabajo de restauración hasta que se cancele el recurso activo.

## Conectividad

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

- El adaptador de red utilizado para la conexión debe configurarse como un cliente para Microsoft Networks.
- El servicio de Microsoft Windows Remote Management (WinRM) debe estar en ejecución.
- Los cortafuegos deben configurarse para permitir que IBM Spectrum Protect Plus se conecte al servidor utilizando WinRM.
- Los cortafuegos deben configurarse para permitir que el navegador de Restauración a nivel de archivo de los sistemas de archivos de IBM Spectrum Protect Plus se conecte al servicio de restauración.
- Se debe poder acceder a la dirección IP del host de cliente que registra desde el servidor IBM Spectrum Protect Plus y desde el servidor vSnap. El agente de sistema de archivos de Windows debe tener un servicio de gestión remota de Windows que esté a la escucha en el puerto 5985.
- Todos los servidores, proxies, aplicaciones e hipervisores que se añaden al entorno de IBM Spectrum Protect Plus deben registrarse utilizando un nombre de sistema de nombres de dominio (DNS) o una dirección IP (Protocolo Internet).
- Si se utilizan nombres DNS, deben poder resolverse en la red mediante el servidor de dispositivos virtuales IBM Spectrum Protect Plus y desde el servidor vSnap. Todos los componentes de IBM Spectrum Protect Plus también deben poder resolverse mediante sus nombres de DNS.

## Puertos

Los usuarios agente de IBM Spectrum Protect Plus utilizan los puertos siguientes.

Tabla 14. Puertos de comunicación cuando el destino es un agente de IBM Spectrum Protect Plus				
Puerto	Protocolo	Iniciador	Objetivo	Descripción
5985	Protocolo de control de transmisiones (TCP)	Dispositivo virtual IBM Spectrum Protect Plus <sup>1</sup>	Sistemas de archivos de Windows	Proporciona acceso al servicio de Microsoft WinRM para servidores basados en Windows

*Tabla 14. Puertos de comunicación cuando el destino es un agente de IBM Spectrum Protect Plus (continuación)*

<b>Puerto</b>	<b>Protocolo</b>	<b>Iniciador</b>	<b>Objetivo</b>	<b>Descripción</b>
5986	TCP	Dispositivo virtual IBM Spectrum Protect Plus <sup>1</sup>	Sistemas de archivos de Windows	Proporciona acceso al servicio de Microsoft WinRM para servidores basados en Windows
9085	TCP	Navegador de Restauración a nivel de archivo de los sistemas de archivos	Sistemas de archivos de Windows	El navegador de Restauración a nivel de archivo de los sistemas de archivos utilizado durante las operaciones de restauración se conecta entre esa IU y el servidor de archivos

<sup>1</sup> El dispositivo virtual IBM Spectrum Protect Plus contiene los siguientes componentes base: el servidor IBM Spectrum Protect Plus, el servidor vSnap y un proxy VADP, consulte [Componentes de producto](#).

*Tabla 15. Puertos de comunicación cuando el iniciador es un usuario agente de IBM Spectrum Protect Plus*

<b>Puerto</b>	<b>Protocolo</b>	<b>Iniciador</b>	<b>Objetivo</b>	<b>Descripción</b>
445	TCP	Sistemas de archivos de Windows	Servidor vSnap	Proporciona el puerto de destino CIFS del servidor CIFS que se utiliza para montar recursos compartidos del sistema de archivos para operaciones de copia de seguridad y restauración del archivo de transacciones

## Hardware

Tabla 16. Requisitos mínimos de hardware		
Sistema	Espacio de disco	Memoria
Hardware basado en x86_64 compatible con una de las versiones del sistema operativo Windows que se lista en la sección Software.	500 MB de espacio libre de disco que se puede utilizar para el despliegue del agente de copia de seguridad.	5 GB de RAM por millón de archivos en el sistema de archivos que se debe proteger.  <b>Nota:</b> La prueba de escalabilidad ha mostrado que el módulo utilizado para explorar el sistema de archivo para identificar los candidatos de copia de seguridad consume más memoria de lo esperado. Un APAR aborda esta limitación.

## Requisitos de Soporte de copia de seguridad de Kubernetes

Antes de desplegar Soporte de copia de seguridad de IBM Spectrum Protect Plus Kubernetes en el entorno de Kubernetes, asegúrese de que el entorno del sistema cumple los requisitos indicados.

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 obtener los requisitos más actuales, que pueden incluir actualizaciones, consulte [Nota técnica 304861](#).






Soporte de copia de seguridad de Kubernetes solo está disponible en inglés en IBM Spectrum Protect Plus versión 10.1.6.

### Configuración

#### Versiones de la aplicación

Los contenedores Docker se soportan en Soporte de copia de seguridad de Kubernetes.

#### Sistemas operativos

Tabla 17. Matriz de cobertura para sistemas operativos soportados en Linux x86_64			
IBM Spectrum Protect Plus	RHEL 7.6	RHEL 7.7	RHEL 7.8
V10.1.5			--
V10.1.6			

#### Requisitos adicionales

IBM Spectrum Protect Plus V10.1.6 da soporte al software y sistemas siguientes:

- Parches y actualizaciones de Kubernetes 1.18 y posteriores
- Parches y actualizaciones de Kubernetes 1.17 y posteriores
- Parches y actualizaciones de Kubernetes 1.16 y posteriores
- Controlador Ceph Container Storage Interface (CSI) 1.2, 2.0 y 2.1 con almacenamiento Rados Block Device (RBD)
- Helm v2.16.1 y posterior.

**Restricción:** Helm v3 no está soportado.

Si utiliza las siguientes versiones de controlador CSI para Kubernetes y Ceph, use IBM Spectrum Protect Plus V10.1.5:

- Parches y actualizaciones de Kubernetes v1.13 y posteriores
- Parches y actualizaciones de Kubernetes v1.14 y posteriores
- Parches y actualizaciones de Kubernetes v1.15 y posteriores
- Controlador Ceph CSI 1.1 con almacenamiento RBD

Para obtener información sobre los releases de Kubernetes, consulte [Control de versiones de publicación de Kubernetes](#).

Para instalar y configurar el soporte de copia de seguridad de contenedor, debe desplegar el software de Soporte de copia de seguridad de Kubernetes en un entorno de Kubernetes. Para obtener instrucciones, consulte [Capítulo 5, “Instalación de Soporte de copia de seguridad de Kubernetes”](#), en la [página 153](#).

### Restricciones

- Las operaciones de copia de seguridad para volúmenes de bloques en bruto no están soportadas.
- Para garantizar que una solicitud de restauración funciona correctamente, no suprima manualmente ninguna instantánea de los volúmenes protegidos por Soporte de copia de seguridad de Kubernetes.
- No puede restaurar una copia de seguridad de instantánea o de copia en un espacio de nombres o clúster distinto.
- No puede restaurar una copia de seguridad de instantánea o de copia en el volumen persistente original.
- Puede restaurar una copia de seguridad de instantánea o de copia solo en un volumen persistente nuevo. La reclamación de volumen persistente (PVC) para el nuevo volumen se crea automáticamente durante la operación de restauración.
- La retrotracción a una versión anterior de Soporte de copia de seguridad de Kubernetes no está soportada. En otras palabras, no puede utilizar Soporte de copia de seguridad de Kubernetes V10.1.5 para restaurar datos de los que Soporte de copia de seguridad de Kubernetes V10.1.6 hizo una copia de seguridad.
- No se admite la actualización del producto desde Soporte de copia de seguridad de Kubernetes V10.1.5.
- Debido a los cambios subyacentes en el objeto BaaSReq de Soporte de copia de seguridad de Kubernetes V10.1.6, no puede utilizar Soporte de copia de seguridad de Kubernetes V10.1.6 para restaurar datos de los que ha hecho copia de seguridad Soporte de copia de seguridad de Kubernetes V10.1.5.

### Software

#### Requisitos previos de clúster

Asegúrese de que se cumplen los siguientes requisitos previos de clúster:

- Soporte de copia de seguridad de Kubernetes protege solo el almacenamiento persistente asignado por un plug-in de almacenamiento que da soporte a CSI.
- Debe estar ejecutando un clúster Kubernetes con soporte de CSI.
- El almacenamiento persistente debe proporcionarlo el controlador CSI, que debe dar soporte a las prestaciones de instantáneas de CIS.
- El soporte de instantánea de CSI debe habilitarse en la línea de mandatos de **kubect1**.
- La herramienta de línea de mandatos de Kubernetes **kubect1** debe estar accesible en el host de instalación y en la vía de acceso local.
- Solo los volúmenes formateados se pueden montar en el transportador de datos para operaciones de copia.

- Opcional: para ayudar a optimizar la escalabilidad y el rendimiento del producto, asegúrese de que Kubernetes Metrics Server v0.3.5 o posterior está instalado y en ejecución en el clúster. Para obtener instrucciones, consulte [“Verificar si Metrics Server está en ejecución”](#) en la página 154.
- Solo para Kubernetes 1.16: las operaciones de copia de seguridad y restauración de instantánea requieren que la característica alfa **VolumeSnapshotDataSource** esté habilitada. Para habilitar la característica alfa **VolumeSnapshotDataSource**, debe parchear el planificador, el controlador y el servidor de API de Kubernetes: Para obtener instrucciones, consulte [“Habilitación de la característica VolumeSnapshotDataSource”](#) en la página 153.
- Se debe definir una clase de almacenamiento para los volúmenes persistentes que se están protegiendo.
- El registro de imágenes de destino debe ser accesible desde el clúster Kubernetes. El registro de imágenes de destino puede ser un registro de imágenes local o un registro de imágenes externo. Para obtener un registro de imágenes externo, puede configurar el secreto de extracción de imagen para proteger el entorno. Para obtener instrucciones, consulte [“Creación de un secreto de extracción de imagen para su uso con un registro externo”](#) en la página 155.
- El host que se utiliza para instalar Soporte de copia de seguridad de Kubernetes debe usar el archivo `kubeconfig` con privilegios de administración de clúster, `KUBECONFIG`, y el cliente Helm debe estar instalado.
- Para crear nuevos recursos en todo el clúster, debe iniciar sesión en el clúster de destino como usuario con privilegios `cluster-admin`.
- Asegúrese de que los secretos de Soporte de copia de seguridad de Kubernetes que incluyen los ID de usuario, las contraseñas y las claves estén cifrados en el resto del almacén de valor de clave distribuido `etcd`. Para obtener más información, consulte [Cifrado de datos secretos en reposo](#).

### Requisitos previos de Helm

- La herramienta Helm debe configurarse en el clúster de destino para que se pueda ejecutar un nuevo despliegue con la línea de mandatos **helm**. El despliegue de un paquete con Helm permite que se generen reglas de control de acceso basado en roles para todo el clúster (RBAC) y enlaces de rol.
- En el clúster Kubernetes, para instalar Helm como usuario root con la cuenta de usuario administrativo de Kubernetes, ejecute el siguiente script, que se incluye en el paquete de instalación:

```
./helm_install_k8s.sh
```

### IBM Spectrum Protect Plus requisitos previos

Los componentes externos que no son de contenedor como, por ejemplo, IBM Spectrum Protect Plus y el servidor vSnap de IBM Spectrum Protect Plus deben ser suministrados y configurados por el administrador de IBM Spectrum Protect Plus.

- Debe configurarse una cuenta administrativa para Soporte de copia de seguridad de Kubernetes en IBM Spectrum Protect Plus.

Esta cuenta administrativa puede configurarse como una cuenta de Lightweight Directory Access Protocol (LDAP) global en el centro de datos. Esta cuenta global es necesaria para acceder a todos los componentes externos con los que opera Soporte de copia de seguridad de Kubernetes.

Debe especificar este nombre de cuenta en el parámetro `BAAS_ADMIN` en el archivo de configuración de `baas_config.cfg` antes de desplegar Soporte de copia de seguridad de Kubernetes. `baas_config.cfg` está ubicado en el directorio `installer`. Para obtener instrucciones, consulte [“Instalación y despliegue de imágenes de Soporte de copia de seguridad de Kubernetes en el entorno de Kubernetes”](#) en la página 156.

- Debe desplegarse una instancia de IBM Spectrum Protect Plus y debe tener licencia como dispositivo virtual de VMware.

La conectividad de red debe existir a y desde el clúster de destino. La dirección de Protocolo Internet (IP) y el número de puerto de IBM Spectrum Protect Plus deben especificarse en el archivo `baas_config.cfg` antes de desplegar Soporte de copia de seguridad de Kubernetes. Solo se puede especificar un puerto (443) para su uso con todas las instancias de IBM Spectrum Protect Plus.



- Debe desplegarse una instancia de vSnap de IBM Spectrum Protect Plus como dispositivo virtual de VMware.
  - La conectividad de red debe existir a y desde el clúster Kubernetes de destino y la instancia de vSnap de IBM Spectrum Protect Plus.
  - La instancia de vSnap debe configurarse como un servidor vSnap externo para almacenar copias de seguridad. Para obtener instrucciones, consulte [Capítulo 3, “Instalación de servidores vSnap”](#), en la [página 111](#).
  - Si las copias de seguridad están cifradas en reposo, asegúrese de que se ha asignado suficiente capacidad para el cifrado en el servidor vSnap.

## **Autenticación y privilegios**

- Asegúrese de especificar el nombre de usuario para la cuenta administrativa de IBM Spectrum Protect Plus en el archivo de configuración `baas_config.cfg`. Para obtener más información, consulte [“Instalación y despliegue de imágenes de Soporte de copia de seguridad de Kubernetes en el entorno de Kubernetes”](#) en la [página 156](#).
- Para acceder al dispositivo asociado con el volumen persistente, el contenedor de transportador de datos debe ser un contenedor privilegiado.
- En función de su rol, los desarrolladores de aplicaciones empresariales y los administradores de copia de seguridad interactúan con distintas interfaces de usuario para proteger los datos persistentes en contenedores, tal como se describe en [“Roles de usuario”](#) en la [página 332](#).

## **Requisitos previos y operaciones**

### **Requisitos previos**

Asegúrese de que se cumplen los requisitos de [“Software”](#) en la [página 57](#), [“Conectividad”](#) en la [página 60](#), [“Autenticación y privilegios”](#) en la [página 59](#).

Soporte de copia de seguridad de Kubernetes debe estar instalado en el entorno de Kubernetes, tal como se describe en [Capítulo 5, “Instalación de Soporte de copia de seguridad de Kubernetes”](#), en la [página 153](#).

### **Operaciones**

Antes de iniciar una operación de copia de seguridad o restauración:

- Una vez que Soporte de copia de seguridad de Kubernetes está instalado, el host de aplicación para el contenedor de Soporte de copia de seguridad de Kubernetes se registra automáticamente tras el inicio del host de clúster en Kubernetes. Cuando se registra un clúster con IBM Spectrum Protect Plus, se captura automáticamente un inventario, permitiéndole completar los trabajos de copia de seguridad y restauración y ejecutar informes.
- Para proteger los volúmenes persistentes que están conectados a un clúster Kubernetes, cree políticas de acuerdo de nivel de servicio (SLA) y cree trabajos para las operaciones de copia de seguridad y restauración en la interfaz de usuario de IBM Spectrum Protect Plus. Si no tiene previsto utilizar la política de SLA predeterminada para contenedores, asegúrese de configurar una política de SLA. Para obtener instrucciones, consulte [“Creación de una política de SLA para clústeres Kubernetes”](#) en la [página 250](#).
- Asegúrese de que se asignan los roles y grupos de recursos adecuados al usuario que ejecuta el trabajo de copia de seguridad. 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. Para obtener instrucciones, consulte [Capítulo 18, “Gestión del acceso de usuarios”](#), en la [página 533](#).
- Las solicitudes de copia de seguridad se dirigen a las PVC para los volúmenes que desea proteger. Antes de planificar un trabajo de copia de seguridad, realice las acciones siguientes:
  - Asegúrese de que la PVC existe en el espacio de nombres especificado.

- Asegúrese de que la PVC esté formateado. Los PVC deben formatearse antes de que se pueda hacer una copia de seguridad de ellos. Para que una PVC tenga el formato correcto, debe estar montado y grabado. No se admiten las operaciones de copia de seguridad de volúmenes de bloque en bruto.
- Determine qué política de SLA se asigna a los PVC. Para obtener instrucciones sobre la visualización de políticas de SLA disponibles, consulte [“Políticas de SLA” en la página 331](#).
- Si una PVC está asociada con varias políticas de SLA, asegúrese de que las políticas no están planificadas 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.

Revise la información siguiente sobre la creación de trabajos de copia de seguridad y restauración:

- Puede utilizar la interfaz de usuario de IBM Spectrum Protect Plus para crear trabajos para operaciones de copia de seguridad y restauración, y para hacer caducar o supervisar trabajos de Soporte de copia de seguridad de Kubernetes y crear informes. Para obtener instrucciones, consulte [“Copia de seguridad y restauración de clústeres Kubernetes utilizando la interfaz de usuario de IBM Spectrum Protect Plus” en la página 334](#).
- Como desarrollador de aplicaciones en un entorno de Kubernetes, puede enviar solicitudes de soporte de copia de seguridad de Kubernetes utilizando la interfaz de línea de mandatos de Kubernetes para realizar copias de seguridad y restaurar datos de contenedor y para consultar el estado de las solicitudes de Soporte de copia de seguridad de Kubernetes. Para obtener instrucciones, consulte [“Protección de contenedores utilizando la línea de mandatos” en la página 348](#).

## Conectividad

Asegúrese de que se cumplen los siguientes requisitos de conectividad:

- El subsistema de protocolo de transferencia de archivos seguro (SFTP) para Secure Shell (SSH) está habilitado.
- El servicio SSH se está ejecutando en los servicios NodePort de Kubernetes .
- Los cortafuegos están configurados para permitir que IBM Spectrum Protect Plus conecte contenedores de transportador de datos utilizando SSH en el rango de puertos de NodePort del clúster Kubernetes. El servicio NodePort permite que Kubernetes determine el puerto específico en el rango de NodePort en el tiempo de ejecución.
- IBM Spectrum Protect Plus utiliza el protocolo Network File System (NFS) para montar volúmenes de almacenamiento para las operaciones de copia de seguridad y restauración. Asegúrese de que el cliente de NFS de Linux nativo está instalado en el servidor de host de proxy.
- Todos los servidores, proxies, aplicaciones e hipervisores que se añaden al entorno de IBM Spectrum Protect Plus deben registrarse utilizando un nombre de Sistema de nombres de dominio (DNS) o una dirección de Protocolo Internet (IP).
- Si se utilizan nombres de DNS, deben poder resolverse a través de la red mediante el servidor de dispositivos virtuales de IBM Spectrum Protect Plus y el servidor vSnap. Todos los componentes de IBM Spectrum Protect Plus también deben poder resolverse mediante sus nombres de DNS.
- Si el DNS no está disponible, debe añadir el servidor al archivo `/etc/hosts` en el dispositivo virtual de IBM Spectrum Protect Plus utilizando la línea de mandatos.

## Puertos

Los agentes de IBM Spectrum Protect Plus utilizan los puertos de comunicación siguientes.

*Tabla 18. Puertos de comunicación cuando el destino está en un agente de IBM Spectrum Protect Plus*

<b>Puerto</b>	<b>Protocolo</b>	<b>Iniciador</b>	<b>Objetivo</b>	<b>Descripción</b>
Asignado por el servicio de NodePort en Kubernetes	Protocolo de control de transmisiones (TCP)	Dispositivo virtual IBM Spectrum Protect Plus <sup>1</sup>	Kubernetes	Utilizado por IBM Spectrum Protect Plus para conectarse al contenedor de transportador de datos para desplegar y ejecutar agentes

<sup>1</sup>Se refiere al servidor IBM Spectrum Protect Plus, que es un componente del dispositivo virtual IBM Spectrum Protect Plus, como se describe en “Componentes del producto” en la página 6.

En las conexiones SSH entre contenedores del entorno de Kubernetes, se utiliza el puerto 22. En todas las demás conexiones, ya sea en los hosts de Kubernetes o fuera del clúster, se utiliza el puerto que ha asignado el servicio de NodePort en tiempo de ejecución.

*Tabla 19. Puertos de comunicación cuando el iniciador es el agente de IBM Spectrum Protect Plus*

<b>Puerto</b>	<b>Protocolo</b>	<b>Iniciador</b>	<b>Objetivo</b>	<b>Descripción</b>
111	TCP	Kubernetes	Servidor vSnap	Permite que los clientes descubran los puertos que los clientes de Open Network Computing (ONC) requieren para comunicarse con servidores ONC
443	TCP	Kubernetes	Servidor vSnap	Utilizado por los mandatos emitidos por IBM Spectrum Protect Plus para ejecutar operaciones de copia de seguridad, restauración, inventario y otras operaciones de configuración
2049	TCP	Kubernetes	Servidor vSnap	Se utiliza para la transferencia de datos NFS hacia y desde los servidores vSnap

Tabla 19. Puertos de comunicación cuando el iniciador es el agente de IBM Spectrum Protect Plus (continuación)

Puerto	Protocolo	Iniciador	Objetivo	Descripción
20048	TCP	Kubernetes	Servidor vSnap	Monta sistemas de archivos vSnap en clientes tales como el proxy de VMware vStorage API for Data Protection (VADP), servidores de aplicaciones y almacenes de datos de virtualización

### Conceptos relacionados

“Protección de contenedores” en la página 329

Soporte de copia de seguridad de Kubernetes es una característica de IBM Spectrum Protect Plus que amplía la protección de datos a los contenedores de los clústeres Kubernetes. Kubernetes es un sistema para la orquestación de contenedores en clústeres de hosts.

## Requisitos de Db2

Antes de registrar Db2 con IBM Spectrum Protect Plus, asegúrese de que el entorno del sistema cumple los requisitos indicados.

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 obtener los requisitos más actuales, que pueden incluir actualizaciones, consulte [Nota técnica 304861](#).

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:

### Versiones de la aplicación

Tabla 20. Matriz de cobertura para niveles de aplicación soportados por IBM Spectrum Protect Plus










IBM Spectrum Protect Plus	Db2 V10.5* Enterprise Edition	Db2 V11.1* Enterprise Edition	Db2 V11.5* Enterprise Edition
V10.1.2			--
V10.1.3			--
V10.1.4			--
V10.1.5			

Tabla 20. Matriz de cobertura para niveles de aplicación soportados por IBM Spectrum Protect Plus (continuación)

V10.1.6			
* Se admiten el release base y los niveles de mantenimiento y modificación posteriores.			

## Sistemas operativos

Tabla 21. Matriz de cobertura para sistemas operativos soportados en IBM PowerPC











IBM Spectrum Protect Plus	IBM AIX 7.1*	IBM AIX 7.2*
V10.1.2		
V10.1.3		
V10.1.4		
V10.1.5		
V10.1.6		
* Se admiten el release base y los niveles de mantenimiento y modificación posteriores.		

Tabla 22. Matriz de cobertura para niveles de aplicación soportados por IBM Spectrum Protect Plus













IBM Spectrum Protect Plus	RHEL 6.8*	RHEL 7.0*	SLES 11.0 SP4*	SLES 12.0 SP1*
V10.1.2				
V10.1.3				
V10.1.4				
V10.1.5				
V10.1.6				
* Se admiten el release base y los niveles de mantenimiento y modificación posteriores.				

Tabla 23. Matriz de cobertura para sistemas operativos soportados en Linux on Power Systems (little endian)

IBM Spectrum Protect Plus	RHEL 7.1*	SLES 12.0 SP1*
---------------------------	-----------	----------------

Tabla 23. Matriz de cobertura para sistemas operativos soportados en Linux on Power Systems (little endian) (continuación)

V10.1.4		
V10.1.5		
V10.1.6		
* Se admiten el release base y los niveles de mantenimiento y modificación posteriores.		

## Restricciones

- IBM Db2 pureScale no está soportada
- Asegúrese de que la configuración del volumen lógico de Db2 no incluya puntos de montaje anidados.
- Si tiene previsto proteger varias particiones, Db2 debe estar en modalidad de copia de seguridad paralela. La modalidad de copia de seguridad paralela se puede habilitar editando las variables de registro de Db2. Para obtener más información, consulte Requisitos previos para Db2. La variable de registro **DB2\_PARALLEL\_ACS** solo está disponible en determinados niveles de fixpack de Db2. Si la variable **DB2\_PARALLEL\_ACS** no está disponible en su versión, puede cumplir el requisito especificando **DB2\_WORKLOAD = SAP**.

## 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.  
**Consejo:** Los paquetes bash y sudo necesarios se incluyen en los sistemas operativos Linux86\_64 y LinuxPower Sytems (little endian) con soporte.
- Instale los parches y las actualizaciones de Db2 más recientes en su entorno.
- Asegúrese de que esté instalada la versión soportada de Linux x86\_64, LinuxPower Systems (little endian) o AIX. Asegúrese de que se han instalado los parches y las actualizaciones más recientes.
- Debe instalarse el paquete RPM de International Components for Unicode (libicu) correspondiente al sistema operativo.
- Asegúrese de que el valor de tamaño de archivo efectivo `ulimit -f` para el usuario agente de IBM Spectrum Protect Plus y el usuario de instancia de Db2 esté establecido 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 Db2 para finalizar la configuración.
- En un entorno Linux, dependiendo de la versión o distribución, asegúrese de que el paquete del programa de utilidad de Linux `util-linux-ng` o del paquete `util-linux` es actual.
- **Usuarios de RHEL y CentOS 6:** para asegurarse de que el paquete `util-linux-ng` o `util-linux` es actual, ejecute el mandato siguiente: `yum update package_name`.

## Autenticación y privilegios

### Autenticación

- El servidor Db2 debe estar registrado con IBM Spectrum Protect Plus utilizando el usuario de sistema operativo que existe en el servidor Db2. A continuación, se hace referencia al usuario como 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.

## Privilegios

Para utilizar una base de datos Db2, el usuario de agente de IBM Spectrum Protect Plus debe tener los siguientes permisos:

- Privilegios para ejecutar mandatos como usuario root y como usuario propietario de software de Db2 utilizando sudo. IBM Spectrum Protect Plus requiere estos privilegios para diversas tareas como, por ejemplo, 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.
  - Debe establecerse el valor `!requiretty`, como se describe en [Establecimiento de privilegios sudo para Db2](#)
- Privilegios para leer el inventario de Db2 utilizando el mandato **db2ls** en el directorio `/usr/local/bin`. IBM Spectrum Protect Plus requiere estos privilegios para descubrir y recopilar información sobre instancias y bases de datos de Db2.

## Requisitos previos y operaciones

### Requisitos previos

Antes de empezar a proteger los recursos, deben cumplirse los requisitos previos siguientes. Para obtener más detalles, consulte [Requisitos previos para Db2](#)

- El registro de archivado de Db2 se ha activado y Db2 está en modalidad recuperable.
- Hay suficiente espacio disponible 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](#)
  - Antes de realizar 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.
  - En el caso de AIX, no pueden existir más de 15 instantáneas para cada Enhanced Journaled File System (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.
  - 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.

- Los volúmenes lógicos que contienen espacios de tabla Db2 (espacios de tablas de datos y temporales), el directorio de bases de datos local y archivos de registro de Db2 que gestiona el sistema de gestión de volúmenes lógicos (LVM2) en Linux o JFS2 en AIX. 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](#).

## Operaciones

Antes de iniciar una operación de copia de seguridad o restauración:

- Debe añadir la dirección de host donde se encuentran las instancias de Db2 en IBM Spectrum Protect Plus. Puede repetir el procedimiento para añadir cada host que desee proteger. Si el entorno de Db2 es multiparticionado con varios hosts, debe añadir cada host a IBM Spectrum Protect Plus. Para obtener instrucciones, consulte [Adición de un servidor de aplicaciones de Db2](#).
- Configure una política de acuerdo de nivel de servicio (SLA). Para obtener instrucciones, consulte [Definición de un trabajo de copia de seguridad de Acuerdo de nivel de servicio](#).
- Para que un usuario de IBM Spectrum Protect Plus pueda implementar operaciones de copia de seguridad y restauración, deben asignarse roles y grupos de recursos al usuario. Otorgue a los usuarios acceso a las operaciones de copia de seguridad y restauración utilizando el panel Cuentas. Para obtener instrucciones, consulte [Gestión de 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 del registro 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 del registro habilitada, una copia de seguridad del registro de un trabajo puede truncar un registro antes de que se realice una copia de seguridad de él en el siguiente trabajo. Este recorte puede provocar que fallen los trabajos de restauración de punto en el tiempo.
- 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 planea restaurar 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 las particiones deben estar en un único 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.

Revise la información siguiente sobre la creación de trabajos de copia de seguridad y restauración:

- Defina trabajos de copia de seguridad de Db2 planificados regularmente para proteger los datos. También puede habilitar operaciones de copia de seguridad continuas para los registros de archivado de forma que pueda restaurar una copia de un punto en el tiempo con opciones de recuperación en avance si es necesario. Para obtener instrucciones, consulte [Copia de seguridad de Db2 data](#).
- 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. Decida si desea restaurar los datos a la instancia original o a una instancia alternativa en un host de cliente diferente. Para obtener instrucciones, consulte [Restauración de datos de Db2](#).

## Conectividad

Asegúrese de que se cumplen los siguientes requisitos de conectividad:



- El subsistema de protocolo de transferencia de archivos seguro (SFTP) para Secure Shell (SSH) está habilitado.
- El servicio Secure Shell (SSH) se está ejecutando en el puerto 22 en el servidor host de proxy.
- Los cortafuegos están configurados para permitir que IBM Spectrum Protect Plus se conecte al servidor de host de proxy utilizando SSH.
- IBM Spectrum Protect Plus utiliza el protocolo NFS (Network File System) para montar volúmenes de almacenamiento para operaciones de copia de seguridad y restauración.
  - En Linux, asegúrese de que el cliente de NFS de Linux nativo esté instalado en el servidor de host de proxy.
  - En AIX, asegúrese de que la comunicación NFS esté configurada con puertos reservados utilizando el mandato siguiente:  

```
nfsd -p -o nfs_use_reserved_port=1
```
- Todos los servidores, proxies, aplicaciones e hipervisores que se añaden al entorno de IBM Spectrum Protect Plus deben registrarse utilizando un nombre de sistema de nombres de dominio (DNS) o una dirección IP (Protocolo Internet).
- Si se utilizan nombres de DNS, deben poder resolverse en la red mediante el servidor de dispositivos virtuales IBM Spectrum Protect Plus y el servidor vSnap. Todos los componentes de IBM Spectrum Protect Plus también deben poder resolverse mediante sus nombres de DNS.
- Si el DNS no está disponible, debe añadir el servidor al archivo /etc/hosts en el dispositivo virtual de IBM Spectrum Protect Plus utilizando la línea de mandatos.

## Puertos

Los agentes de usuario de IBM Spectrum Protect Plus utilizan los puertos siguientes.

Tabla 24. Puertos de comunicación cuando el destino es un agente de IBM Spectrum Protect Plus				
Puerto	Protocolo	Iniciador	Objetivo	Descripción
22	Protocolo de control de transmisiones (TCP)	Dispositivo virtual IBM Spectrum Protect Plus <sup>1</sup>	Servidor de Db2	Proporciona acceso para resolver problemas y mantener servidores de host de proxy remoto que ejecutan componentes de la aplicación invitada utilizando el protocolo SSH
<sup>1</sup> El dispositivo virtual IBM Spectrum Protect Plus contiene los siguientes componentes base: el servidor IBM Spectrum Protect Plus, el servidor vSnap y un proxy VADP, como se describe en <a href="#">Componentes de producto</a> .				

*Tabla 25. Puertos de comunicación cuando el iniciador es el agente de IBM Spectrum Protect Plus*

<b>Puerto</b>	<b>Protocolo</b>	<b>Iniciador</b>	<b>Objetivo</b>	<b>Descripción</b>
111	TCP	Servidor de Db2	Servidor vSnap	Permite que los clientes descubran los puertos que los clientes de Open Network Computing (ONC) requieren para comunicarse con servidores ONC
2049	TCP	Servidor de Db2	Servidor vSnap	Se utiliza para la transferencia de datos NFS hacia y desde los servidores vSnap
20048	TCP	Servidor de Db2	Servidor vSnap	Monta sistemas de archivos vSnap en clientes tales como el proxy de VMware vStorage API for Data Protection (VADP), servidores de aplicaciones y almacenes de datos de virtualización

## Hardware

*Tabla 26. Requisitos mínimos de hardware*

<b>Sistema</b>	<b>Espacio en disco</b>
Hardware compatible soportado por el sistema operativo y el servidor de base de datos Db2	Se instalará un mínimo de 500 MB de espacio en disco para el producto que se va a instalar

## 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 obtener los requisitos más actuales, que pueden incluir actualizaciones, consulte [Nota técnica 304861](#).

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

### Configuración

#### Versiones de aplicación

Tabla 27. Matriz de cobertura para niveles de aplicación soportados por IBM Spectrum Protect Plus

IBM Spectrum Protect Plus	Microsoft Exchange Server 2013 CU16* Ediciones Standard y Enterprise	Microsoft Exchange Server 2016 CU5* Ediciones Standard y Enterprise	Microsoft Exchange Server 2019* Ediciones Standard y Enterprise
V10.1.3			
V10.1.4			
V10.1.5			
V10.1.6			
* Se admiten el release base y los niveles de mantenimiento y actualizaciones acumulativas posteriores.			

**Nota:** Se da soporte a los grupos de disponibilidad de base de datos (DAG) de Microsoft Exchange.

#### Sistemas operativos

Tabla 28. Matriz de cobertura para sistemas operativos soportados en Windows x64

IBM Spectrum Protect Plus	Microsoft Windows Server 2012 R2* Ediciones Standard y Datacenter	Microsoft Windows Server 2016* Ediciones Standard y Datacenter	Microsoft Windows Server 2019* Ediciones Standard y Datacenter
V10.1.3			
V10.1.4			
V10.1.5			
V10.1.6			
* Se admiten el release base y los niveles de mantenimiento posteriores.			

IBM Spectrum Protect Plus soporta un Microsoft Exchange Server que se ejecuta en un servidor (bare metal) físico y en un entorno virtualizado. Se da soporte a los siguientes entornos virtualizados:

- Sistema operativo de invitado VMware Elastic Sky X (ESX)
- Sistema operativo de invitado Hyper-V de Microsoft Windows

Consulte los requisitos mínimos para habilitar el seguimiento de los rangos de grabación en [“Copias de seguridad incrementales”](#) en la página 72.

#### Restricciones

Se aplican las siguientes restricciones:

- Windows Server 2019 con la opción Server Core está soportado. Sin embargo, la opción de instalación Server Core no soporta la característica de restauración granular.
- Solo se realiza una copia de seguridad de los registros de la base de datos en el nodo preferido. Solo una instancia de Exchange Server a la vez puede grabar copias de seguridad del registro en el servidor vSnap.
- Cuando restaura un elemento del buzón (o un buzón) en un archivo de carpetas personales de Outlook (.pst), puede utilizar la vista Navegador de restauración de buzón solo con archivos .pst que no son Unicode.
- Cuando restaura un elemento del buzón (o un buzón) en un buzón diferente, no puede arrastrar elementos de correo electrónico o subcarpetas de la carpeta Elementos recuperables en un buzón de destino.
- Cuando restaura elementos del buzón en un archivo (.pst) de carpetas personales que no son Unicode, cada carpeta puede contener un máximo de 16.383 elementos de correo.

Consulte las restricciones específicas para tecnologías que no están soportadas para el seguimiento de bytes cambiados en [“Copias de seguridad incrementales” en la página 72](#).

## Software

- Instale las actualizaciones y parches de base de datos de Microsoft Exchange más recientes en su entorno.
- Instale una versión soportada de un sistema operativo Windows de 64 bits en el entorno. Asegúrese de que se han instalado los parches y las actualizaciones más recientes.
- Se debe instalar el software siguientes antes de utilizar IBM Spectrum Protect Plus:
  - Windows PowerShell 4 o posterior
  - Windows Management Framework 4 o posterior
- Si utiliza Microsoft Exchange Server 2013 con la característica de restauración granular, el nivel mínimo que se soporta para Microsoft Exchange Messaging API (MAPI) Client y Collaboration Data Objects (CDO) es la versión 6.5.8320.0.
- Si utiliza la característica de restauración granular con Microsoft Exchange Server 2016 o 2019, se requiere Microsoft Outlook 2013, Outlook 2016 o Outlook 2019 de 32 bits.
- El software siguiente, necesario para Microsoft, se instala automáticamente mediante la característica de restauración 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
  - Paquete redistribuible Microsoft ReportViewer 2012 SP1
  - 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 característica de restauración granular de IBM Spectrum Protect Plus.

## Autenticación y privilegios

### Autenticación

Registre cada servidor de Microsoft Exchange con IBM Spectrum Protect Plus por nombre o dirección IP.

**Restricción:** Se debe poder acceder a la dirección IP desde el servidor IBM Spectrum Protect Plus y desde el servidor vSnap. Se debe poder resolver y redirigir el nombre de dominio completo de todos los servidores de Microsoft Exchange desde el servidor IBM Spectrum Protect Plus y desde el servidor vSnap. Se debe poder resolver y redirigir el nombre de dominio completo del servidor IBM Spectrum Protect Plus desde los servidores de Microsoft Exchange.

La identidad de usuario debe tener suficientes privilegios para instalar e iniciar el servicio de herramientas de IBM Spectrum Protect Plus en el nodo. Para obtener más información, consulte el artículo de Microsoft: [Añadir el inicio de sesión como servicio de derecho a una cuenta](#).

### Privilegios

Para utilizar una base de datos de Exchange, un usuario agente de IBM Spectrum Protect Plus debe tener los privilegios adecuados. Para obtener instrucciones sobre la asignación de privilegios, consulte [“Privilegios”](#) en la página 403.

Revise la información siguiente sobre privilegios y restricciones:

- Para gestionar los grupos de roles de Exchange mediante Exchange Admin Center (EAC) o Exchange Powershell Cmdlets, el nombre de usuario debe estar autorizado por la política de seguridad.
- El Sistema de cifrado de archivos (EFS) debe estar habilitado en la política de dominio de grupo o local, y debe haber disponible un certificado de agente de recuperación de datos de dominio (DRA) válido.
- Para utilizar el navegador de buzón para operaciones de restauración granular, los certificados digitales de Exchange deben estar instalados y configurados.

**Consejo:** Con Microsoft Exchange Server 2016 y 2019, Exchange Server está configurado para utilizar la Seguridad de la capa de transporte (TLS) de forma predeterminada. Esta seguridad TLS cifra la comunicación entre los servidores de Exchange internos y entre los servicios de Exchange en el servidor local.

### Requisitos previos y operaciones

#### Requisitos previos

Asegúrese de que se cumplen los requisitos de [“Software”](#) en la página 70, [“Conectividad”](#) en la página 72 y [“Autenticación y privilegios”](#) en la página 70.

Antes de empezar a proteger los recursos, deben cumplirse los requisitos previos siguientes. Si desea obtener más información al respecto, consulte el apartado [“Requisitos previos para el servidor de Exchange”](#) en la página 403.

#### Operaciones

Antes de iniciar una operación de copia de seguridad o restauración:

- Asegúrese de que los servidores de aplicaciones que contienen bases de datos de Exchange de las que desea realizar copia de seguridad están registrados con IBM Spectrum Protect Plus. Para obtener instrucciones, consulte [“Adición de un servidor de aplicaciones de Exchange”](#) en la página 405.
- Configure una política de acuerdo de nivel de servicio (SLA). Para obtener instrucciones, consulte [“Definición de un trabajo de copia de seguridad de Acuerdo de nivel de servicio”](#) en la página 407.
- Asegúrese de que se asignan los roles y grupos de recursos adecuados al usuario que creará los trabajos de copia de seguridad y restauración. Para obtener instrucciones, consulte [Capítulo 18, “Gestión del acceso de usuarios”](#), en la página 533.

Revise la información siguiente sobre la creación de trabajos de copia de seguridad y restauración:

- Para proteger las bases de datos de Microsoft Exchange, puede definir un trabajo de copia de seguridad que se ejecuta de forma continua para crear copias de seguridad incrementales. También puede ejecutar trabajos de copia de seguridad bajo demanda fuera de la planificación. Para obtener instrucciones, consulte [“Copia de seguridad de bases de datos de Exchange”](#) en la página 407.
- Al restaurar archivos desde un archivado de IBM Spectrum Protect, los archivos se migran inicialmente desde el almacenamiento en cintas a una agrupación de almacenamiento de transferencia. En función del tamaño de los archivos que se van a restaurar, este proceso puede tardar varias horas.

- Si tiene previsto restaurar datos en una instancia alternativa o una ubicación de archivo nueva, los directorios de destino que especifica en el campo **Vía de acceso de destino** deben existir en el host de aplicación. Si los directorios no existen en el servidor, debe crearlos antes de completar la operación de restauración.
- Si los datos de una base de datos Exchange se pierden o se dañan, puede restaurarlos desde una copia de seguridad. Utilice el asistente "Restaurar" para configurar una planificación de trabajos de restauración o una operación de restauración bajo demanda. Puede definir un trabajo que restaure datos en la instancia original. Para obtener instrucciones, consulte [Restauración de bases de datos de Exchange](#)

Para obtener las restricciones y requisitos detallados que se aplican a los trabajos de copia de seguridad, consulte [Copias de seguridad incrementales](#)

### **Copias de seguridad incrementales**

IBM Spectrum Protect Plus utiliza la tecnología de diario de cambios de número de secuencia de actualización (USN) para copias de seguridad incrementales en un entorno de Microsoft Exchange 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.

Para habilitar el seguimiento de rangos de grabación, el entorno del sistema debe cumplir los requisitos siguientes:

- Windows Server 2012 R2 o posterior
- New Technology File System (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 Transparent Failover (TFO)
- SMB 3.0 con particiones de archivos de escalado

De forma predeterminada, se asignan 512 MB de espacio para el registro por diario de cambios de USN. Además, cuando se detecta un desbordamiento de diario, el espacio asignado dobla su tamaño, a un máximo de 2 GB.

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.

Se fuerza una copia de seguridad de base de datos de un archivo cuando se detectan las condiciones siguientes:

- Se notifica una discontinuidad del diario. Este problema se puede producir cuando el registro alcanza su tamaño máximo, cuando el registro por diario está inhabilitado o cuando se cambia el ID de 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 ha añadido un archivo después de una operación de copia de seguridad anterior.

### **Conectividad**

Asegúrese de que se cumplen los siguientes requisitos de conectividad:

- El adaptador de red utilizado para la conexión debe configurarse como un cliente para Microsoft Networks.
- El servicio de Microsoft Windows Remote Management (WinRM) debe estar en ejecución.
- Los cortafuegos deben estar configurados para habilitar IBM Spectrum Protect Plus para conectarse al servidor utilizando WinRM.

- La dirección IP del host de cliente que se registra debe ser accesible desde el servidor de IBM Spectrum Protect Plus y desde el servidor vSnap. El servidor de Microsoft Exchange debe tener un servicio WinRM que esté a la escucha en el puerto 5985.
- Todos los servidores, proxies, aplicaciones e hipervisores que se añaden al entorno de IBM Spectrum Protect Plus deben registrarse utilizando un nombre de Sistema de nombres de dominio (DNS) o una dirección de Protocolo Internet (IP).
- Si se utilizan nombres DNS, deben poder resolverse en la red mediante el servidor de dispositivos virtuales IBM Spectrum Protect Plus y desde el servidor vSnap. Todos los componentes de IBM Spectrum Protect Plus también deben poder resolverse mediante sus nombres de DNS.

## Puertos

Los agentes de usuario de IBM Spectrum Protect Plus utilizan los puertos siguientes.

<i>Tabla 29. Puertos de comunicación cuando el destino está en un agente de IBM Spectrum Protect Plus</i>				
<b>Puerto</b>	<b>Protocolo</b>	<b>Iniciador</b>	<b>Objetivo</b>	<b>Descripción</b>
5985	Protocolo de control de transmisiones (TCP)	Dispositivo IBM Spectrum Protect Plus <sup>1</sup>	Microsoft Exchange Server	Proporciona acceso al servicio de Microsoft WinRM para servidores basados en Windows
5986	TCP	Dispositivo IBM Spectrum Protect Plus <sup>1</sup>	Microsoft Exchange Server	Proporciona acceso al servicio de Microsoft WinRM para servidores basados en Windows

<sup>1</sup> El dispositivo virtual IBM Spectrum Protect Plus contiene los siguientes componentes base: el servidor IBM Spectrum Protect Plus, el servidor vSnap y un proxy VADP, como se describe en [“Componentes del producto”](#) en la página 6.

<i>Tabla 30. Puertos de comunicación cuando el iniciador es un usuario agente de IBM Spectrum Protect Plus</i>				
<b>Puerto</b>	<b>Protocolo</b>	<b>Iniciador</b>	<b>Objetivo</b>	<b>Descripción</b>
3260 El iniciador de iSCSI es necesario en este nodo.	TCP	Microsoft Exchange Server	Servidor vSnap	El puerto de destino de vSnap del servicio de iniciador de Microsoft Internet Small Computer System Interface (iSCSI) que se utiliza para montar LUNS para operaciones de copia de seguridad y recuperación

*Tabla 30. Puertos de comunicación cuando el iniciador es un usuario agente de IBM Spectrum Protect Plus (continuación)*

<b>Puerto</b>	<b>Protocolo</b>	<b>Iniciador</b>	<b>Objetivo</b>	<b>Descripción</b>
443	TCP	Microsoft Exchange Server	Dispositivo IBM Spectrum Protect Plus <sup>1</sup>	Puerto que permite al agente comunicarse con IBM Spectrum Protect Plus para enviar alertas en caso de errores de copia de seguridad del registro
445	TCP	Microsoft Exchange Server	Servidor vSnap	Proporciona un puerto de destino de SMB o CIFS de servidor vSnap que se utiliza para montar recursos compartidos del sistema de archivos para operaciones de copia de seguridad y recuperación del registro de transacciones

<sup>1</sup> El dispositivo virtual IBM Spectrum Protect Plus contiene los siguientes componentes base: el servidor IBM Spectrum Protect Plus, el servidor vSnap y un proxy VADP, como se describe en [“Componentes del producto”](#) en la página 6.

#### **Actualización de puertos:**

- En Microsoft Exchange Server, el puerto 443 está disponible en IBM Spectrum Protect Plus V10.1.4 y posterior.
- En versiones anteriores, los agentes de aplicación que utilizan SMBv1 utilizaron los puertos 137, 138 y 139 en el servidor vSnap. A partir de IBM Spectrum Protect Plus V10.1.6, no se utiliza el protocolo SMBv1. Todos los agentes utilizan SMBv2 o posterior, lo que no requiere los puertos 137, 138 o 139.

#### **Hardware**

*Tabla 31. Requisitos mínimos de hardware*

<b>Sistema</b>	<b>Espacio de disco</b>	<b>Espacio de disco para operaciones de restauración granulares</b>
Hardware compatible soportado por el sistema operativo de 64 bits y Microsoft Exchange Server	Se instalará un mínimo de 500 MB de espacio en disco para el producto que se va a instalar	Se necesita al menos 2.1 GB de espacio de disco para el software de Microsoft, que se instala automáticamente

#### **Requisitos de MongoDB**

A partir de IBM Spectrum Protect Plus V10.1.3, se ha añadido soporte para la copia de seguridad y restauración de datos de base de datos de MongoDB. Antes de registrar un servidor de aplicaciones



MongoDB con IBM Spectrum Protect Plus, asegúrese de que el entorno del sistema cumple los requisitos siguientes.

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 obtener los requisitos más actuales, que pueden incluir actualizaciones, consulte [Nota técnica 304861](#).

## Requisitos de configuración

### Versiones de la aplicación

Tabla 32. Matriz de cobertura para niveles de aplicación soportados por IBM Spectrum Protect Plus			
IBM Spectrum Protect Plus	Ediciones de MongoDB V3.6* Community Server y Enterprise Server	Ediciones de MongoDB V4.0* Community Server y Enterprise Server	Ediciones de MongoDB V4.2* Community Server y Enterprise Server
V10.1.3			--
V10.1.4			--
V10.1.5			--
V10.1.6			
* Se admiten el release base y los niveles de mantenimiento y modificación posteriores.			

### Sistemas operativos



























Tabla 33. Matriz de cobertura para sistemas operativos soportados en Linux x86_64					
IBM Spectrum Protect Plus	RHEL 6.8*	RHEL 7.0*	CentOS 6.8*	CentOS 7.0*	SLES 12.0 SP1*
V10.1.3					
V10.1.4					
V10.1.5					
V10.1.6	 IT322842: Consultar restricciones		 IT322842: Consultar restricciones		
* Se admiten el release base y los niveles de mantenimiento y modificación posteriores.					

Tabla 34. Matriz de cobertura para sistemas operativos soportados en Linux on Power Systems (little endian)

IBM Spectrum Protect Plus	RHEL 7.1*	CentOS 7.0*
V10.1.4		
V10.1.5		
V10.1.6	 IT322842: Consultar restricciones	 IT322842: Consultar restricciones
* Se admiten el release base y los niveles de mantenimiento y modificación posteriores.		

Proteja el entorno de MongoDB con IBM Spectrum Protect Plus cuando se ejecute en uno de los siguientes sistemas operativos de invitados:

- Red Hat Enterprise Linux
- Máquina virtual basada en Kernel (KVM) de SUSE Linux Enterprise Server

#### Restricciones

- Todas las instancias de MongoDB sin la autenticación de usuario habilitada aún se soporta para todos los sistemas operativos listados. A partir de APAR IT32842, debido a problemas con credenciales cifradas, no se puede dar soporte a las instancias de MongoDB con la autenticación de usuario habilitada en IBM Spectrum Protect Plus V10.1.6 en los siguientes sistemas operativos:
  - Linux x86\_64: RHEL 6.8 y niveles de mantenimiento y modificación posteriores, CentOS 6.8 y niveles de mantenimiento y modificación posteriores
  - Linux on Power Systems: RHEL7.1 y niveles de mantenimiento y modificación posteriores, CentOS 7.0 y niveles de mantenimiento y modificación posteriores
- En Linux on Power Systems (little endian), solo se da soporte a MongoDB Enterprise Server Edition.
- Las configuraciones de clúster compartido de MongoDB se detectan cuando se ejecuta un inventario, pero estos recursos no son elegibles para operaciones de copia de seguridad o de restauración.
- En MongoDB, el cifrado basado en SSL y la autenticación basada en certificados no están soportados.
- No ejecute trabajos de inventario durante trabajos de copia de seguridad planificados.
- No configure puntos de montaje anidados.

#### Software

- Los paquetes bash y sudo deben estar instalados. Sudo debe estar en la versión 1.7.6p2 o posterior. Ejecute `sudo -V` para comprobar la versión.  
**Consejo:** Los paquetes bash y sudo necesarios se incluyen en los sistemas operativos Linux x86\_64 y Linux on Power Systems (little endian) soportados.
- Instale los parches y actualizaciones de MongoDB más recientes en el entorno.
- Asegúrese de que esté instalada una versión soportada de Linux x86\_64 o Linux on Power Systems (little endian). Asegúrese de que se han instalado los parches y las actualizaciones más recientes.
- Debe instalarse el paquete RPM de International Components for Unicode (**libicu**) correspondiente al sistema operativo.
- Asegúrese de que `ulimit -f`, para el usuario agente de IBM Spectrum Protect Plus y el usuario de instancia de MongoDB, esté establecido en unlimited. Como alternativa, establezca un valor lo

suficientemente alto para dar soporte a 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.

- En un entorno de Linux, en función de su versión o distribución, asegúrese de que el paquete de utilidad de Linux `util-linux-ng` o `util-linux` sea actual.
- **Usuarios de RHEL y CentOS 6:** para asegurarse de que el paquete `util-linux-ng` o `util-linux` es actual, ejecute el mandato siguiente sustituyendo el nombre de paquete en lugar de *nombre\_paquete*:

```
yum update nombre_paquete
```

- **Usuarios de RHEL y CentOS 6:** cuando el servidor de aplicaciones MongoDB ejecuta RHEL 6 o CentOS 6, asegúrese de que el paquete `openssl` esté en la versión 1.0.1e-57 o posterior. Para actualizar la versión, ejecute el mandato siguiente:

```
yum update openssl
```

## Autenticación y privilegios

### Autenticación

- El servidor MongoDB debe registrarse con IBM Spectrum Protect Plus utilizando un usuario de sistema operativo que existe en el servidor MongoDB. A continuación, se hace referencia al usuario como 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.
- Con MongoDB Enterprise Server Edition, solo se da soporte al motor de almacenamiento cifrado.

### Privilegios

Para utilizar una base de datos de MongoDB, un usuario agente de IBM Spectrum Protect Plus debe tener los siguientes permisos:

- Privilegios para ejecutar mandatos como usuario `root` y como usuario propietario de software de MongoDB utilizando `sudo`. IBM Spectrum Protect Plus requiere estos privilegios para varias tareas tales como descubrir diseños de almacenamiento, montar y desmontar discos y gestionar bases de datos.
  - La configuración `sudoers` debe permitir al usuario agente de IBM Spectrum Protect Plus ejecutar mandatos sin una contraseña.
  - Debe especificarse el valor `!requiretty`, como se describe en [“Establecimiento de privilegios sudo”](#) en la página 449.
- Privilegios para leer el módulo de servidor de MongoDB estándar `/usr/local/bin/mongod`. IBM Spectrum Protect Plus requiere estos privilegios para utilizar la API de PyMongo para conectarse a servidores MongoDB utilizando el nombre de Sistema de nombres de dominio (DNS) o el nombre de dirección Protocolo Internet (IP) y puerto asignados de la instancia. Este mecanismo se utiliza para recopilar información sobre instancias y bases de datos de MongoDB.
- Si el servidor MongoDB está protegido por la autenticación basada en roles, debe configurar los privilegios adecuados, tal como se describe en [“Roles para MongoDB”](#) en la página 447.

## Requisitos previos y operaciones

### Requisitos previos

Asegúrese de que se cumplen los requisitos de [“Software”](#) en la página 76, [“Conectividad”](#) en la página 79 y [“Autenticación y privilegios”](#) en la página 77.

Antes de empezar a proteger los recursos, deben cumplirse los requisitos previos siguientes. Si desea obtener más información al respecto, consulte el apartado [“Requisitos previos para MongoDB”](#) en la página 446.

- MongoDB se configura como una instancia autónoma o un conjunto de réplicas. Las copias de seguridad de instancias de clúster compartidas de MongoDB no están soportadas. 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.
- Todas las instancias de MongoDB que se vayan a proteger deben registrarse con IBM Spectrum Protect Plus. Una vez que las instancias están registradas, 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.
- El usuario del registro del servidor de aplicaciones de MongoDB en IBM Spectrum Protect Plus debe poder recuperar información de servidor y el estado de la base de datos de administración de MongoDB.
- Asegúrese de que tiene suficiente espacio libre en los host de origen y de destino y en el repositorio de vSnap. Se necesita espacio adicional para almacenar copias de seguridad del Gestor de volúmenes lógicos (LVM) temporal de volúmenes lógicos donde se encuentran los datos de MongoDB. Estas copias de seguridad temporales, conocidas como instantáneas de LVM, las crea automáticamente el agente de MongoDB. En cada volumen lógico de instantánea de LVM, se debe asignar al menos un 10% 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 reserva hasta el 25 por ciento del tamaño de volumen lógico de origen para el volumen lógico de la instantánea. Para obtener más información, consulte [“Requisitos previos de espacio para la protección de MongoDB”](#) en la página 448.
- Asegúrese de que se ha asignado suficiente espacio de disco en el servidor de destino para las operaciones de restauración.
- Linux Logical Volume Manager (LVM2) gestiona los volúmenes lógicos de las vías de acceso de registro y datos de MongoDB. 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 los datos cambian en el volumen de origen mientras existe la instantánea. Para obtener más información, consulte [“LVM2 de Linux”](#) en la página 448.

## Operaciones

Antes de iniciar una operación de copia de seguridad o restauración:

- Añada los servidores de aplicaciones de los que desea realizar una copia de seguridad. Para obtener instrucciones, consulte [“Adición de un servidor de aplicaciones de MongoDB”](#) en la página 449.
- Configure una política de acuerdo de nivel de servicio (SLA). Para obtener instrucciones, consulte [“Definición de un trabajo de acuerdo de nivel de servicio regular”](#) en la página 455.
- Antes de que un usuario de IBM Spectrum Protect Plus pueda configurar operaciones de copia de seguridad y restauración, deben asignarse roles y grupos de recursos al usuario. Otorgue a los usuarios acceso a recursos y operaciones de copia de seguridad y restauración utilizando el panel Cuentas. Para obtener más información, consulte Capítulo 18, “Gestión del acceso de usuarios”, en la página 533 y [“Roles para MongoDB”](#) en la página 447.

Revise la información siguiente sobre la creación de trabajos de copia de seguridad y restauración:

- Para hacer copia de seguridad regularmente de los datos, defina un trabajo de copia de seguridad que incluya una política de SLA. Para obtener instrucciones, consulte [“Copia de seguridad de datos de MongoDB”](#) en la página 454.
- Para restaurar datos, defina un trabajo que restaure datos de la copia de seguridad más reciente o seleccione una copia de seguridad anterior. Puede restaurar datos en la instancia original o en una instancia alternativa en un host de cliente distinto, 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. Para obtener instrucciones, consulte [“Restauración de datos de MongoDB”](#) en la página 458.
- Asegúrese de que se han asignado volúmenes dedicados para la copia de archivos.
- Asegúrese de que la misma estructura de directorios y el mismo diseño están disponibles en los servidores de origen y de destino.

- Si restaura datos desde un archivado de IBM Spectrum Protect, los archivos se migran inicialmente desde el almacenamiento en cintas a la agrupación de almacenamiento de transferencia. En función del tamaño de los archivos que se van a restaurar, este proceso puede tardar varias horas.
- Para restaurar operaciones en instancias alternativas, MongoDB debe estar en el mismo nivel de versión en los host de cliente y de destino.

## Conectividad

Asegúrese de que se cumplen los siguientes requisitos de conectividad:

- El subsistema de protocolo de transferencia de archivos seguro (SFTP) para Secure Shell (SSH) está habilitado.
- El servicio Secure Shell (SSH) se está ejecutando en el puerto 22 en el servidor host de proxy.
- Los cortafuegos están configurados para permitir que IBM Spectrum Protect Plus se conecte al servidor de host de proxy utilizando SSH.
- IBM Spectrum Protect Plus utiliza el protocolo Network File System (NFS) para montar volúmenes de almacenamiento para las operaciones de copia de seguridad y restauración. Asegúrese de que el cliente de NFS de Linux nativo está instalado en el servidor de host de proxy.
- Todos los servidores, proxies, aplicaciones e hipervisores que se añaden al entorno de IBM Spectrum Protect Plus deben registrarse utilizando un nombre de Sistema de nombres de dominio (DNS) o una dirección de Protocolo Internet (IP).
- Si se utilizan nombres de DNS, deben poder resolverse a través de la red mediante el servidor de dispositivos virtuales de IBM Spectrum Protect Plus y el servidor vSnap. Todos los componentes de IBM Spectrum Protect Plus también deben poder resolverse mediante sus nombres de DNS.
- Si el DNS no está disponible, debe añadir el servidor al archivo `/etc/hosts` en el dispositivo virtual de IBM Spectrum Protect Plus utilizando la línea de mandatos.

## Puertos

Los agentes de usuario de IBM Spectrum Protect Plus utilizan los puertos siguientes.

Tabla 35. Puertos de comunicación cuando el destino está en un agente de IBM Spectrum Protect Plus				
Puerto	Protocolo	Iniciador	Objetivo	Descripción
22	Protocolo de control de transmisiones (TCP)	Dispositivo virtual IBM Spectrum Protect Plus <sup>1</sup>	MongoDB	Proporciona acceso para resolver problemas y mantener servidores de host de proxy remoto que ejecutan componentes de la aplicación de invitado utilizando el protocolo SSH.
<sup>1</sup> El dispositivo virtual IBM Spectrum Protect Plus contiene los componentes base: el servidor IBM Spectrum Protect Plus, sitio, servidor vSnap y el proxy VADP como se describe en <a href="#">“Componentes del producto”</a> en la <a href="#">página 6</a> .				

Tabla 36. Puertos de comunicación cuando el iniciador es el agente de IBM Spectrum Protect Plus

Puerto	Protocolo	Iniciador	Objetivo	Descripción
111	TCP	MongoDB	Servidor vSnap	Permite que los clientes de Open Network Computing (ONC) descubran puertos para las comunicaciones con servidores ONC.
2049	TCP	MongoDB	Servidor vSnap	Se utiliza para la transferencia de datos NFS a y desde servidores vSnap.
20048	TCP	MongoDB	Servidor vSnap	Monta sistemas de archivos vSnap en clientes tales como el proxy de VMware vStorage API for Data Protection (VADP), servidores de aplicaciones y almacenes de datos de virtualización

## Hardware

Tabla 37. Requisitos mínimos de hardware

Sistema	Espacio en disco
Hardware compatible soportado por el sistema operativo y MongoDB.	Se instalará un mínimo de 500 MB de espacio en disco para el producto que se va a instalar.

## Requisitos de Office 365

Este documento detalla los requisitos de copia de seguridad y restauración de Microsoft Office 365 para IBM Spectrum Protect Plus. Antes de registrar un host de proxy con IBM Spectrum Protect Plus, asegúrese de que el entorno del sistema cumple los requisitos siguientes. El servidor de host de proxy se conoce en la interfaz de usuario (UI) como *servidor de aplicaciones*.

### Configuración del servicio en la nube

A partir de IBM Spectrum Protect Plus V10.1.5, se ha añadido soporte para la copia de seguridad y restauración de los datos de Microsoft Office 365.

Si elige proteger Microsoft Office 365 con IBM Spectrum Protect Plus, necesita adquirir IBM Spectrum Protect Plus para Microsoft Office 365. Para obtener más información sobre esta titularidad, consulte [Carta de anuncio de IBM Spectrum Protect V10.1.5](#).

**Actualización del nombre de producto:** Microsoft Corporation ha anunciado nuevos nombres de producto, a partir del 21 de abril de 2020, para sus ofertas de Office 365 para pequeñas y medianas empresas. Con este anuncio, todos los planes para pequeñas y medianas empresas han pasado a la

nueva marca de Microsoft 365. En IBM Spectrum Protect Plus V10.1.6, la interfaz de usuario y la documentación utilizan el nombre de producto original, Office 365. Para obtener más información, consulte [Nuevas ofertas de Microsoft 365 para pequeñas y medianas empresas](#)

Antes de registrar un servidor de host de proxy con IBM Spectrum Protect Plus, asegúrese de que el entorno del sistema cumple los requisitos siguientes.

## Configuración

### Servicio en la nube

Para proteger una aplicación de Microsoft Office 365, debe registrar la aplicación con Azure Active Directory y otorgar los permisos adecuados. Para empezar, debe tener los elementos siguientes:










- Una suscripción de Microsoft Office 365 activa
- Un ID de usuario de administración y una contraseña de Microsoft Office 365

Para obtener instrucciones, consulte [Registro con Azure Active Directory](#).

Si tiene una cuenta administrativa de Microsoft Office 365, puede añadir usuarios para asegurarse de que tienen licencias válidas. Para obtener instrucciones, consulte [Microsoft 365 en suscripciones de Visual Studio](#).

**Nota:** El usuario agente y el servidor de IBM Spectrum Protect Plus no almacenan ID de usuario de administración ni contraseñas para el arrendatario de Microsoft Office 365.






### Versiones de la aplicación

Tabla 38. Matriz de cobertura para niveles de aplicación soportados por IBM Spectrum Protect Plus					
IBM Spectrum Protect Plus	Ediciones de Microsoft 365 Business Basic, Business Standard y Business Premium	Ediciones de Office 365 for Enterprise E1, E3 y E5	Ediciones de Office365 for Education A1, A3 y A5	Office 365 for Firstline Workers F3 Edition	Ediciones de Microsoft 365 for Enterprise E3 y E5
	Nombre de producto anterior: Office 365 Business: Business, Essentials y Business Premium Edition		Nombre de producto anterior: Office 365 Education Edition	Nombre de producto anterior: Microsoft 365 F1	
V10.1.5					
V10.1.6					

### Sistemas operativos

Tabla 39. Matriz de cobertura para sistemas operativos soportados en Linux x86_64			
IBM Spectrum Protect Plus	RHEL 7.0*	RHEL 8.0*	CentOS 7.0*

Tabla 39. Matriz de cobertura para sistemas operativos soportados en Linux x86\_64 (continuación)

V10.1.5		--	
V10.1.6			
* Se admiten el release base y los niveles de mantenimiento y modificación posteriores.			

IBM Spectrum Protect Plus da soporte al servidor de host de proxy que se ejecuta en un servidor físico (bare metal) y en un entorno virtualizado.

### Restricciones

El arrendatario de Microsoft Office 365 debe estar en una región global tal como define Microsoft. No se da soporte a las regiones nacionales. Para obtener más información sobre las regiones, consulte [Despliegues en la nube nacional](#).

### Software

- Asegúrese de que Java<sup>™</sup> 8 está instalado.
- Los paquetes bash y sudo deben estar instalados. Sudo debe estar en la versión 1.7.6p2 o posterior. Ejecute sudo -V para comprobar la versión. Sugerencia: Los paquetes bash y sudo necesarios se incluyen en el sistema operativo Linux x86\_64 soportado.
- Instale los parches y actualizaciones de Microsoft Office 365 más recientes en el entorno.
- Instale una versión soportada de Linux x86\_64 en el entorno.
- Asegúrese de que se han instalado los parches y las actualizaciones más recientes. El paquete RPM de International Components for Unicode (libicu) debe estar instalado para la versión correspondiente al sistema operativo. Asegúrese de que el valor del tamaño de archivo efectivo ulimit -f, que especifica el tamaño de archivo efectivo para el agente de IBM Spectrum Protect Plus se establece en ilimitado. De forma alternativa, establezca el valor en un valor lo suficientemente alto para soportar la copia de los archivos de Office 365 más grandes en los trabajos de copia de seguridad y restauración.
- En un entorno de Linux, dependiendo de la versión o distribución, asegúrese de que el paquete del programa de utilidad de Linux, util-linux-ng o util-linux, es actual.

### Autenticación y privilegios

#### Autenticación

- El servidor de host de proxy se debe registrar con IBM Spectrum Protect Plus utilizando un usuario de sistema operativo que exista en el host de agente. A continuación, se hace referencia al usuario como usuario 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.

#### Privilegios

El usuario agente de IBM Spectrum Protect Plus debe tener privilegios para ejecutar mandatos como usuario root utilizando sudo. La configuración de **sudoers** debe permitir que el usuario agente de IBM Spectrum Protect Plus ejecute mandatos sin una contraseña.

### Requisitos previos y operaciones

#### Requisitos previos

Antes de empezar a proteger los recursos, se deben cumplir los requisitos previos siguientes:



- Para proteger una aplicación de Office 365, debe registrar la aplicación con Azure Active Directory y otorgar los permisos adecuados. Cuando registra una aplicación nueva con Azure Active Directory, las credenciales de aplicación, como el ID de aplicación y el secreto de aplicación están disponibles en el portal de Azure Active Directory. Para obtener instrucciones, consulte [Registro con Azure Active Directory](#)
- Para asegurarse de que el agente de IBM Spectrum Protect Plus puede conectarse al arrendatario de Office 365, debe registrar las credenciales del arrendatario de Office 365 y el servidor de host de proxy con IBM Spectrum Protect Plus. Este procedimiento es necesario para garantizar que se puede realizar copia de seguridad de los datos de Office 365 en IBM Spectrum Protect Plus. Para obtener instrucciones, consulte [Registro del arrendatario de Office 365 con IBM Spectrum Protect Plus](#)

## Operaciones

Antes de iniciar una operación de copia de seguridad o restauración:

- Aplique una política de acuerdo de nivel de servicio (SLA). Para obtener instrucciones, consulte [Crear políticas de copia de seguridad](#).

Revise la información siguiente sobre la creación de trabajos de copia de seguridad y restauración:

- Para hacer copia de seguridad de los correos electrónicos, calendarios, contactos y datos de Microsoft Office 365 en el almacenamiento en la nube de OneDrive, consulte [Copia de seguridad de los datos de Office 365](#).
- Para restaurar datos de Office 365 desde las copias de seguridad en servidores vSnap o almacenamiento remoto, consulte [Restauración de datos de Office 365](#).

## Conectividad

Asegúrese de que se cumplen los siguientes requisitos de conectividad:

- El subsistema de protocolo de transferencia de archivos seguro (SFTP) para Secure Shell (SSH) está habilitado.
- El servicio Secure Shell (SSH) se está ejecutando en el puerto 22 en el servidor host de proxy.
- Los cortafuegos están configurados para permitir que IBM Spectrum Protect Plus se conecte al servidor de host de proxy utilizando SSH.
- IBM Spectrum Protect Plus utiliza el protocolo NFS (Network File System) para montar volúmenes de almacenamiento para operaciones de copia de seguridad y restauración. Asegúrese de que el cliente de NFS de Linux nativo está instalado en el servidor de host de proxy.
- Todos los servidores, proxies, aplicaciones e hipervisores que se añaden al entorno de IBM Spectrum Protect Plus deben registrarse utilizando un nombre de sistema de nombres de dominio (DNS) o una dirección IP (Protocolo Internet).
- Si se utilizan nombres de DNS, deben poder resolverse en la red mediante el servidor de dispositivos virtuales IBM Spectrum Protect Plus y el servidor vSnap. Todos los componentes de IBM Spectrum Protect Plus también deben poder resolverse mediante sus nombres de DNS.
- Si el DNS no está disponible, debe añadir el servidor al archivo /etc/hosts en el dispositivo virtual IBM Spectrum Protect Plus utilizando la línea de mandatos.

## Puertos

Los usuarios agente de IBM Spectrum Protect Plus utilizan los puertos siguientes.

*Tabla 40. Puertos de comunicación cuando el destino es un usuario agente de IBM Spectrum Protect Plus*

<b>Puerto</b>	<b>Protocolo</b>	<b>Iniciador</b>	<b>Objetivo</b>	<b>Descripción</b>
22	Protocolo de control de transmisiones (TCP)	Dispositivo virtual IBM Spectrum Protect Plus <sup>1</sup>	Servidor de host de proxy	Proporciona acceso para resolver problemas y mantener servidores de host de proxy remoto que ejecutan componentes de la aplicación de invitado utilizando el protocolo SSH

<sup>1</sup> El dispositivo virtual IBM Spectrum Protect Plus contiene los siguientes componentes base: el servidor IBM Spectrum Protect Plus, el servidor vSnap y un proxy VADP, como se describe en [Componentes de producto](#)

*Tabla 41. Puertos de comunicación cuando el iniciador es un usuario agente de IBM Spectrum Protect Plus*

<b>Puerto</b>	<b>Protocolo</b>	<b>Iniciador</b>	<b>Objetivo</b>	<b>Descripción</b>
111	TCP	Servidor de host de proxy	servidor vSnap	Permite que los clientes descubran los puertos que los clientes de Open Network Computing (ONC) requieren para comunicarse con servidores ONC
443	TCP	Servidor de host de proxy	servidor vSnap	Puerto que permite al agente comunicarse con IBM Spectrum Protect Plus para enviar alertas en caso de errores de copia de seguridad del registro
2049	TCP	Servidor de host de proxy	servidor vSnap	Se utiliza para la transferencia de datos NFS hacia y desde los servidores vSnap

Tabla 41. Puertos de comunicación cuando el iniciador es un usuario agente de IBM Spectrum Protect Plus (continuación)

Puerto	Protocolo	Iniciador	Objetivo	Descripción
20048	TCP	Servidor de host de proxy	servidor vSnap	Monta sistemas de archivos vSnap en clientes tales como el proxy de VMware vStorage API for Data Protection (VADP), servidores de aplicaciones y almacenes de datos de virtualización

## Hardware

Tabla 42. Requisitos mínimos de hardware

Sistema	Espacio en disco	Memoria
Hardware compatible con procesadores de cuatro núcleos soportados por el sistema operativo	5 GB de espacio de disco disponible para archivos temporales en tiempo de ejecución	4 GB de memoria de acceso aleatorio (RAM)

## Requisitos de copia de seguridad y restauración de bases de datos del servidor Oracle

Revise los requisitos de copia de seguridad y restauración de bases 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 obtener los requisitos más actuales, que pueden incluir actualizaciones, consulte [Nota técnica 304861](#).

## Configuración

### Versiones de la aplicación

Tabla 43. Matriz de cobertura para niveles de aplicación soportados por IBM Spectrum Protect Plus















IBM Spectrum Protect Plus	Oracle 11g R2* Enterprise Edition	Oracle 12c R1* Enterprise Edition	Oracle 12c R2* Enterprise Edition	Oracle 18c* Enterprise Edition	Oracle 19c* Enterprise Edition
V10.1.1				--	--
V10.1.2				--	--
V10.1.3					--
V10.1.4					--

Tabla 43. Matriz de cobertura para niveles de aplicación soportados por IBM Spectrum Protect Plus (continuación)

IBM Spectrum Protect Plus	Oracle 11g R2*	Oracle 12c R1*	Oracle 12c R2*	Oracle 18c*	Oracle 19c*
	Enterprise Edition	Enterprise Edition	Enterprise Edition	Enterprise Edition	Enterprise Edition
V10.1.5					
V10.1.6					
* Se admiten el release base y los niveles de mantenimiento y modificación posteriores.					

**Consejo:** 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 las PDB específicas se puede realizar utilizando una operación de recuperación de restauración de disco instantánea combinada con el gestor de recuperación (RMAN).

### Sistemas operativos

Tabla 44. Matriz de cobertura para sistemas operativos soportados en IBM PowerPC

IBM Spectrum Protect Plus	IBM AIX 6.1 TL9*	IBM AIX 7.1*
V10.1.1		
V10.1.2		
V10.1.3		
V10.1.4		
V10.1.5		
V10.1.6		
* Se admiten el release base y los niveles de mantenimiento y modificación posteriores.		

Tabla 45. Matriz de cobertura para sistemas operativos soportados en Linux® x86\_64

IBM Spectrum Protect Plus	RHEL 6.5*	RHEL 7.0*	RHEL 8.0*	CentOS 6.5*	CentOS 7.0*	CentOS 8.0*	SLES 11.0 SP4*	SLES 12.0 SP1*	SLES 15.0*
V10.1.1			--			--			--

Tabla 45. Matriz de cobertura para sistemas operativos soportados en Linux® x86\_64 (continuación)

IBM Spectrum Protect Plus	RHEL 6.5*	RHEL 7.0*	RHEL 8.0*	CentOS 6.5*	CentOS 7.0*	CentOS 8.0*	SLES 11.0 SP4*	SLES 12.0 SP1*	SLES 15.0*
V10.1.2	✓	✓	--	✓	✓	--	✓	✓	--
V10.1.3	✓	✓	--	✓	✓	--	✓	✓	--
V10.1.4	✓	✓	--	✓	✓	--	✓	✓	✓
V10.1.5	✓	✓	--	✓	✓	--	✓	✓	✓
V10.1.6	✓	✓	✓	✓	✓	✓	✓	✓	✓

\* Se admiten el release base y los niveles de mantenimiento y modificación posteriores.

### Restricciones

- 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 operaciones de recuperación 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 restaurada no es multihebra. La base de datos restaurada se debe volver a configurar manualmente para que utilice la configuración multihebra.
- 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.

### Network File System (NFS)

El servidor Oracle debe tener instalado el cliente de 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.

En las operaciones de restauración de 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` de cada directorio de inicio de Oracle debe ser propiedad del usuario root y tener privilegios **setuid**.

Normalmente, el instalador de Oracle preconfigura el binario, pero en determinados sistemas, es posible que este binario no tenga los privilegios necesarios. Ejecute los mandatos siguientes para establecer los privilegios correctos:

- `chown root:oinstall oracle_home/bin/oradism`

donde `oinstall` especifica el grupo propietario de la instalación y `orace_home` especifica el directorio de inicio de Oracle.

- `chmod 750 oracle_home/bin/oradism`

### Descubrimiento de bases de datos

IBM Spectrum Protect Plus descubre las instalaciones y bases de datos de Oracle buscando los archivos `/etc/orainst.loc` y `/etc/oratab` y la lista de 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 instancias en ejecución y consultando las ubicaciones de sus archivos de datos, archivos de registro y otros archivos. Para que IBM Spectrum Protect Plus descubra correctamente las bases de datos durante las operaciones de catalogación y copia, las bases de datos deben estar en 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 el seguimiento de cambios de bloque de Oracle esté habilitado en bases de datos protegidas para realizar copias de seguridad incrementales de forma eficaz. Si el seguimiento de cambios de bloque no está habilitado todavía, IBM Spectrum Protect Plus lo habilita automáticamente durante el trabajo de copia de seguridad.

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

- Si se establece el parámetro **db\_create\_file\_dest**, el archivo de seguimiento de cambios de bloque se crea en la ubicación especificada por este parámetro.
- Si el parámetro **db\_create\_file\_dest** no está establecido, el archivo de seguimiento de cambios de bloque se crea en el mismo directorio que el espacio de tabla SYSTEM.

### Software

- Los paquetes **bash** y **sudo** deben estar instalados. El paquete **sudo** debe ser la versión 1.7.6p2 o posterior. Ejecute **sudo -V** para comprobar la versión.

**Consejo:** Los paquetes **bash** y **sudo** necesarios se incluyen en los sistemas operativos Linux x86\_64 soportados.

- Instale los parches y actualizaciones del servidor de Oracle más recientes en el entorno.
- Asegúrese de que esté instalada una versión soportada de Linux x86\_64 o Linux on Power Systems (little endian). Asegúrese de que se han instalado los parches y las actualizaciones más recientes.
- El paquete RPM de International Components for Unicode (**libicu**) debe estar instalado para la versión correspondiente del sistema operativo.
- Asegúrese de que el tamaño de archivo efectivo **ulimit -f** para el usuario agente de IBM Spectrum Protect Plus y el usuario de instancia de Oracle esté establecido 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 Oracle para finalizar la configuración.
- En un entorno de Linux, en función de su versión o distribución, asegúrese de que el paquete de programa de utilidad de Linux **util-linux-ng** o el paquete **util-linux** sea actual.

- Para los usuarios de Red Hat Enterprise Linux y CentOS 6: para asegurarse de que el paquete `util-linux-ng` o `util-linux` es actual, ejecute el mandato siguiente:

```
yum update package_name
```

## Autenticación y privilegios

### Autenticación

- El servidor de Oracle debe estar registrado en IBM Spectrum Protect Plus utilizando un usuario del sistema operativo que exista en el servidor de Oracle. A continuación, se hace referencia al usuario como 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.

### Privilegios

Para utilizar un servidor de Oracle, el usuario agente de IBM Spectrum Protect Plus debe tener los permisos siguientes:

- Privilegios para ejecutar mandatos como usuario root y como usuario propietario del software de Oracle (por ejemplo, `oracle` o `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 (Automatic Storage Management).
  - 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 las páginas de inicio de Oracle.

Para conseguir estos privilegios, 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 usuario nuevo con los privilegios necesarios, consulte [“Configuración de ejemplo de un usuario agente de IBM Spectrum Protect Plus” en la página 89](#).

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

Los mandatos siguientes son ejemplos para crear y configurar un usuario de sistema operativo que IBM Spectrum Protect Plus utiliza para iniciar 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 designado como usuario agente de IBM Spectrum Protect Plus:

```
useradd -m sppagent
```

- Establezca una contraseña:

```
passwd sppagent_password
```

- Si utiliza la autenticación basada en claves, coloque la clave pública en el directorio `/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. Los mandatos se estructuran tal como se muestra en el ejemplo siguiente:

```
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 del sistema operativo (OSDBA):

```
usermod -a -G oinstall,dba sppagent
```

- Si tiene previsto utilizar ASM, 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 sudoers existente está configurado para importar una 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
```

## Requisitos previos y operaciones

### Requisitos previos

Asegúrese de que se cumplen los requisitos de [“Software”](#) en la página 88, [“Conectividad”](#) en la página 91 y [“Autenticación y privilegios”](#) en la página 89.

### Operaciones

Antes de iniciar una operación de copia de seguridad o restauración:

- 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 recursos y roles utilizando el panel **Cuentas**. Para obtener más información, consulte [Capítulo 18, “Gestión del acceso de usuarios”](#), en la página 533.
- Registre los proveedores cuya copia de seguridad desea realizar. Para obtener más información, consulte [“Adición de un servidor de aplicaciones Oracle”](#) en la página 476.
- Configure una política de acuerdo de nivel de servicio (SLA). Para obtener más información, consulte [“Crear políticas de copia de seguridad”](#) en la página 169.

Revise la información siguiente sobre la creación de trabajos de copia de seguridad y restauración:

- 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. Para obtener información sobre los valores de uid y gid, consulte la documentación de la base de datos de Oracle.
- 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. Para evitar este problema, 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 del registro para una única base de datos 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 del registro habilitada, una copia de seguridad del registro de un trabajo podría truncar un registro antes de que se realice una copia de seguridad con el siguiente trabajo. Este comportamiento puede provocar que fallen los trabajos de restauración de punto en el tiempo.
- Utilice un trabajo de copia de seguridad para realizar copias de seguridad de entornos de Oracle con instantáneas, tal como se describe en [“Copia de seguridad de datos de Oracle”](#) en la página 478.
- Utilice un trabajo de restauración para restaurar un entorno de Oracle a partir de instantáneas. IBM Spectrum Protect Plus crea un clon de vSnap a partir de la versión seleccionada durante la definición de trabajo y crea un recurso compartido NFS. 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, como se describe en “Restauración de datos de Oracle” en la página 481.

- Al restaurar datos desde un archivo de IBM Spectrum Protect, los archivos se migran inicialmente desde el almacenamiento en cintas a una agrupación de transferencia. En función del tamaño de los archivos que se van a restaurar, este proceso puede tardar varias horas.
- Si se monta una base de datos Oracle 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.

### 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`.

### Conectividad

Asegúrese de que se cumplen los siguientes requisitos de conectividad:

- El subsistema de protocolo de transferencia de archivos seguro (SFTP) para Secure Shell (SSH) está habilitado.
- El servicio SSH debe estar en ejecución en el puerto 22 en el servidor de host de proxy.
- Los cortafuegos están configurados para permitir que IBM Spectrum Protect Plus se conecte al servidor de host de proxy utilizando SSH.
- IBM Spectrum Protect Plus utiliza el protocolo Network File System (NFS) para montar volúmenes de almacenamiento para las operaciones de copia de seguridad y restauración. Asegúrese de que el cliente de NFS de Linux nativo está instalado en el servidor de host de proxy.
- Todos los servidores, proxies, aplicaciones e hipervisores que se añaden al entorno de IBM Spectrum Protect Plus deben registrarse utilizando un nombre de Sistema de nombres de dominio (DNS) o una dirección de Protocolo Internet (IP).
- Si se utilizan nombres DNS, deben poder resolverse a través del servidor de dispositivos virtuales IBM Spectrum Protect Plus y desde el servidor vSnap. Todos los componentes de IBM Spectrum Protect Plus también deben poder resolverse mediante sus nombres de DNS.
- Si el DNS no está disponible, debe añadir el servidor al archivo `/etc/hosts` en el dispositivo virtual de IBM Spectrum Protect Plus utilizando la línea de mandatos.
- Los nodos RAC de Oracle están registrados por su nombre o IP física. No utilice un nombre virtual o un nombre de acceso de cliente único (SCAN).

### Puertos

Los agentes de usuario de IBM Spectrum Protect Plus utilizan los puertos siguientes.

*Tabla 46. Puertos de comunicación cuando el destino está en un agente de IBM Spectrum Protect Plus*

<b>Puerto</b>	<b>Protocolo</b>	<b>Iniciador</b>	<b>Objetivo</b>	<b>Descripción</b>
22	Protocolo de control de transmisiones (TCP)	Dispositivo virtual IBM Spectrum Protect Plus <sup>1</sup>	Servidor Oracle	Proporciona acceso para resolver problemas y mantener servidores de host de proxy remoto que ejecutan componentes de aplicaciones de invitado mediante el protocolo SSH

<sup>1</sup> El dispositivo virtual IBM Spectrum Protect Plus contiene los componentes base: el servidor IBM Spectrum Protect Plus, el servidor vSnap y un proxy VADP, como se describe en “Componentes del producto” en la página 6.

*Tabla 47. Puertos de comunicación cuando el iniciador es un usuario agente de IBM Spectrum Protect Plus*

<b>Puerto</b>	<b>Protocolo</b>	<b>Iniciador</b>	<b>Objetivo</b>	<b>Descripción</b>
111	TCP	Servidor Oracle	Servidor vSnap	Permite que los clientes descubran los puertos que los clientes de Open Network Computing (ONC) requieren para comunicarse con servidores ONC
443	TCP	Servidor Oracle	Dispositivo virtual IBM Spectrum Protect Plus <sup>1</sup>	Puerto que permite al agente comunicarse con IBM Spectrum Protect Plus para enviar alertas en caso de errores de copia de seguridad del registro
2049	TCP	Servidor Oracle	Servidor vSnap	Se utiliza para la transferencia de datos NFS hacia y desde los servidores vSnap

Tabla 47. Puertos de comunicación cuando el iniciador es un usuario agente de IBM Spectrum Protect Plus (continuación)

Puerto	Protocolo	Iniciador	Objetivo	Descripción
20048	TCP	Servidor Oracle	Servidor vSnap	Monta sistemas de archivos vSnap en clientes tales como el proxy de VMware vStorage API for Data Protection (VADP), servidores de aplicaciones y almacenes de datos de virtualización

<sup>1</sup> El dispositivo virtual IBM Spectrum Protect Plus contiene los componentes base: el servidor IBM Spectrum Protect Plus, el servidor vSnap y un proxy VADP, como se describe en “Componentes del producto” en la página 6.

## Hardware

Tabla 48. Requisitos mínimos de hardware

Sistema	Espacio en disco
Hardware compatible soportado por el sistema operativo y el servidor de Oracle	Se instalará un mínimo de 500 MB de espacio en disco para el producto que se va a instalar

## Requisitos de copia de seguridad y restauración de bases de datos 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 obtener los requisitos más actuales, que pueden incluir actualizaciones, consulte [Nota técnica 304861](#).

## Configuración

### Versiones de la aplicación

Tabla 49. Matriz de cobertura para niveles de aplicación soportados por IBM Spectrum Protect Plus

IBM Spectrum Protect Plus	Microsoft SQL Server 2008 R2 SP3* Ediciones Standard y Enterprise	Microsoft SQL Server 2012* Ediciones Standard y Enterprise	Microsoft SQL Server 2014* Ediciones Standard y Enterprise	Microsoft SQL Server 2016* Ediciones Standard y Enterprise	Microsoft SQL Server 2017* Ediciones Standard y Enterprise	Microsoft SQL Server 2019* Ediciones Standard y Enterprise
V10.1.1					 A partir de V10.1.1 parche 1	--
V10.1.2						--
V10.1.3						--
V10.1.4						--
V10.1.5						 A partir de V10.1.5 parche 1
V10.1.6						

\* Se admiten el release base y los niveles de mantenimiento y actualizaciones acumulativas posteriores.

## Sistemas operativos

Tabla 50. Matriz de cobertura para sistemas operativos soportados en Windows x64

















IBM Spectrum Protect Plus	Microsoft Windows Server 2012 R2* Ediciones Standard y Datacenter	Microsoft Windows Server 2016* Ediciones Standard y Datacenter	Microsoft Windows Server 2019* Ediciones Standard y Datacenter
V10.1.1			--
V10.1.2			--
V10.1.3			
V10.1.4			

Tabla 50. Matriz de cobertura para sistemas operativos soportados en Windows x64 (continuación)

IBM Spectrum Protect Plus	Microsoft Windows Server 2012 R2* Ediciones Standard y Datacenter	Microsoft Windows Server 2016* Ediciones Standard y Datacenter	Microsoft Windows Server 2019* Ediciones Standard y Datacenter
V10.1.5			
V10.1.6			
* Se admiten el release base y los niveles de mantenimiento posteriores.			

## Restricciones

Se aplican las siguientes restricciones:

- IBM Spectrum Protect Plus no admite la copia de seguridad del registro de modelos de recuperación simples.
- La migración tras error de una instancia de clúster SQL durante operaciones de copia de seguridad no está soportada.
- La vía de acceso de archivo de restauración del Servicio de instantáneas de volumen (VSS) está limitada a 256 caracteres o menos. Si la vía de acceso original supera esta longitud, considere la posibilidad de utilizar una vía de acceso de archivo de restauración personalizada para trabajos de restauración de producción para reducir la longitud.
- Debido a limitaciones de la infraestructura de VSS, los espacios iniciales, los espacios finales y los caracteres no imprimibles no deben utilizarse en nombres de base de datos. Para obtener más información, consulte [La copia de seguridad de una base de datos de SQL Server utilizando una aplicación de copia de seguridad de VSS puede fallar en algunas bases de datos.](#)
- No puede restaurar datos en un NTFS (New Technology File System) o un volumen comprimido de la tabla de asignación de archivos (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.](#)

## Software

- Instale los parches y las actualizaciones de Microsoft SQL Server más recientes en el entorno.
- Instale una versión soportada de un sistema operativo Windows de 64 bits en el entorno. Asegúrese de que se han instalado los parches y las actualizaciones más recientes.

## Autenticación y privilegios

### Autenticación

Registre cada Microsoft SQL Server con IBM Spectrum Protect Plus por nombre o dirección IP. Al registrar un nodo de clúster de SQL Server, registre cada nodo por nombre o dirección IP.

**Restricción:** Se debe poder acceder a la dirección IP desde el servidor IBM Spectrum Protect Plus y desde el servidor vSnap. Ambos servidores deben tener un servicio Windows Remote Management (WinRM) que esté a la escucha en el puerto 5985. Se debe poder resolver y redirigir el nombre de dominio completo desde el servidor IBM Spectrum Protect Plus y desde el servidor vSnap.

La identidad de usuario debe tener derechos suficientes para instalar e iniciar el servicio de herramientas de IBM Spectrum Protect Plus en el nodo. Estos permisos incluyen los derechos `Iniciar sesión como servicio` e `Iniciar sesión como trabajo por lotes` en la política de seguridad local. Para obtener más información, consulte el artículo de Microsoft: [Añadir el inicio de sesión como servicio de derecho a una cuenta](#)

Si SQL Server está conectado a un dominio, la identidad de usuario sigue el formato `domain\Name` predeterminado. Si el usuario es un administrador local, la identidad de usuario coincide con el nombre del administrador local.

### Autenticación Kerberos

La autenticación basada en Kerberos se puede habilitar especificando un archivo de configuración en el dispositivo virtual IBM Spectrum Protect Plus. Los valores sustituyen el protocolo Windows NT LAN Manager (NTLM) predeterminado.

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

### Privilegios

Para utilizar un Microsoft SQL Server, un usuario agente de IBM Spectrum Protect Plus debe tener los permisos siguientes:

- Permisos de Microsoft SQL Server `public` y `sysadmin`
- Los permisos de administración local de Windows, que son necesarios 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 Always On y de instancia de clústeres de migración tras error (FCI) de SQL Server

Todos los host de Microsoft SQL Server pueden utilizar una cuenta de usuario específica para acceder a los recursos de esa instancia de SQL Server.

La infraestructura basada en VDI (Virtual Device Interface) de SQL Server se utiliza para interactuar con bases de datos de SQL Server y para registrar operaciones de copia de seguridad del registro y restauración. Una conexión de VDI requiere permisos `sysadmin` de Microsoft SQL Server. 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 artículo de Microsoft: [Las operaciones de copia de seguridad y restauración VDI de SQL Server requieren privilegios Sysadmin](#)

La cuenta de servicio de Microsoft SQL Server de destino debe tener permisos para acceder a los archivos de restauración de Microsoft SQL Server. Consulte la sección Consideraciones administrativas en el artículo de Microsoft: [Protección de archivos de datos y registros](#)

El Planificador de tareas de Windows se utiliza para planificar copias de seguridad del registro. Dependiendo del entorno, los usuarios pueden recibir el siguiente error:

Una sesión de inicio de sesión especificada no existe. Es posible que ya se haya terminado.

Este comportamiento tiene lugar cuando se habilita un valor de política de grupo de acceso de red. Para obtener instrucciones sobre la inhabilitación del valor, consulte el artículo de soporte de Microsoft: [Error del planificador de tareas “No existe ninguna sesión de inicio de sesión especificada”](#)

### Objeto de política de grupo

Para el valor **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**, especifique una de las siguientes opciones:

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

La opción **Enviar solo respuesta NTLM** no es compatible con la versión de vSnap Common Internet File System (CIFS) y Server Message Block (SMB) y puede provocar problemas de autenticación de CIFS.

Puede especificar el valor de Objeto de política de grupo (GPO) navegando a:

- **Configuración del sistema > Políticas > Valores de Windows > Configuración de seguridad > Políticas locales > Opciones de seguridad > Seguridad de red: Restringir NTLM: tráfico de NTLM entrante**

O bien,

- **Configuración del sistema > Políticas > Valores de Windows > Configuración de seguridad > Políticas locales > Opciones de seguridad > Seguridad de red: Restringir NTLM: tráfico de NTLM de salida**

A continuación, elija una de las opciones siguientes:

- **Permitir todo**
- **Permitir todas las cuentas**

## Requisitos previos y operaciones

### Requisitos previos

Asegúrese de que se cumplen los requisitos de [“Software”](#) en la página 95, [“Conectividad”](#) en la página 100 y [“Autenticación y privilegios”](#) en la página 95.

Antes de empezar a proteger los recursos, se deben cumplir los requisitos previos siguientes:

- Debe habilitarse una ruta iSCSI (Internet Small Computer Interface) entre el sistema Microsoft SQL Server y el servidor vSnap. Para obtener más información, consulte [Guía de paso a paso de Microsoft iSCSI Initiator](#).
- La vía de acceso binaria de Windows PowerShell debe establecerse en la variable de entorno %PATH%.
- Si tiene previsto realizar copias de seguridad de bases de datos que se han restaurado en modalidad de prueba, utilice la preferencia global para limitar el tamaño de los volúmenes de destino de copia de seguridad a menos de 64 TB. Debe establecer esta preferencia global antes de ejecutar la primera copia de seguridad para el acuerdo de nivel de servicio (SLA) que protege las bases de datos. Si el tamaño de los volúmenes de destino de copia de seguridad es de 64 o más, el trabajo de copia de seguridad falla.

### Operaciones

Antes de iniciar una operación de copia de seguridad o restauración:

- Registre los SQL Server a los que desea hacer copia de seguridad. Cuando se añade un servidor de aplicaciones SQL Server, se captura un inventario de las instancias y bases de datos asociadas al servidor de aplicaciones y se añade a IBM Spectrum Protect Plus. El inventario es necesario para los trabajos de copia de seguridad y restauración y para ejecutar informes. Para obtener instrucciones, consulte [“Adición de un servidor de aplicaciones SQL Server”](#) en la página 489.
- Configure las políticas de acuerdo de nivel de servicio (SLA). Para obtener instrucciones, consulte [“Crear políticas de copia de seguridad”](#) en la página 169.
- 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 utilizando el panel **Cuentas**. Para obtener instrucciones, consulte [Capítulo 18, “Gestión del acceso de usuarios”](#), en la página 533.
- Antes de configurar y ejecutar trabajos de copia de seguridad de SQL, configure los valores de almacenamiento de copia de duplicación para los volúmenes en los que se encuentran las bases de datos 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 haga clic en la pestaña **Duplicaciones**. Establezca el valor **Tamaño máximo** en **Sin límite** o un tamaño razonable basándose en el tamaño de volumen de origen y las actividades de entrada/salida (E/S) y, a

continuación, pulse **Aceptar**. El área de almacenamiento de duplicación debe estar en el mismo volumen o en otro volumen disponible durante un trabajo de copia de seguridad.

- 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 para el número máximo de hebras Worker es 0. El servidor determina automáticamente el número máximo de hebras Worker que se basan en el número de procesadores disponibles para 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 tiene un gran número de bases de datos en un trabajo de copia de seguridad, es posible que el valor predeterminado para el número máximo de hebras Worker no sea suficiente para realizar una copia de seguridad de todas las bases de datos y el trabajo falla. Para obtener instrucciones sobre cómo aumentar la opción de número máximo de hebras Worker, consulte [Configurar la opción de configuración de servidor de hebras Worker máximo](#).
- 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](#).

Revise la información siguiente sobre la creación de trabajos de copia de seguridad y restauración:

- Utilice un trabajo de copia de seguridad para realizar copias de seguridad de entornos SQL Server con instantáneas. Para obtener instrucciones, consulte [“Copia de seguridad de datos de SQL Server”](#) en la [página 491](#).
- IBM Spectrum Protect Plus soporta copias de seguridad de base de datos y copias de seguridad del registro de transacciones. El nombre de producto se llena en msdb . dbo . backupset para los registros que crearon las copias de seguridad iniciadas desde IBM Spectrum Protect Plus.
- Utilice un trabajo de restauración para restaurar un entorno de Microsoft SQL Server a partir de 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 rastrea todas las instancias clonadas, tal como se describe en [“Restauración de datos de SQL Server”](#) en la [página 496](#).
- 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.
- 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.
- Al restaurar datos desde un archivo de IBM Spectrum Protect, los archivos se migran inicialmente desde el almacenamiento en cintas a una agrupación de almacenamiento de transferencia. Dependiendo del tamaño de la restauración, este proceso puede tardar varias horas.
- 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, debe inicializarse un trabajo de restauración secundario desde el punto de restauración con el espacio de Número de secuencia de registro (LSN) más corto de la instancia primaria. Las copias de seguridad del registro del último momento específico que crea IBM Spectrum Protect Plus deben restaurarse si la copia de seguridad del 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 \(motor de base de datos\)](#).

### Proceso de transacción en línea (OLTP) en memoria

El proceso de transacción en línea (OLTP) en memoria 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 Microsoft SQL Server 2014 y posterior. Los requisitos y las limitaciones siguientes se aplican al uso de OLTP en memoria:

- La vía de acceso de archivo de restauración está limitada a 256 caracteres o menos. 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 pueden restaurarse están sujetos al Servicio de instantáneas de volumen (VSS) y a las prestaciones de restauración de Microsoft SQL Server.

### Configuración de los grupos de disponibilidad Siempre activado

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

1. Seleccione el nodo **Grupo de disponibilidad**.
2. Seleccione el grupo de disponibilidad que desea configurar. A continuación, seleccione **Propiedades**.
3. En el cuadro de diálogo **Propiedades de grupo de disponibilidad**, seleccione **Preferencias de copia de seguridad**.
4. En el panel **Dónde deben realizarse las copias de seguridad**, seleccione cualquier opción.

Cuando se prefiere una réplica secundaria y hay más de una réplica secundaria disponible, el ejecutor de trabajos de IBM Spectrum Protect Plus selecciona la primera réplica secundaria en la lista preferida notificada por el agente de IBM Spectrum Protect Plus SQL Server.

El agente de Microsoft SQL Server establece el tipo de copia de seguridad de VSS en COPY\_ONLY.

La opción **Sin recuperación** no da soporte a las operaciones de restauración de modalidad de producción para grupos de disponibilidad AlwaysOn de SQL.

### Copias de seguridad incrementales

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 Microsoft 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.

Para habilitar el seguimiento de rangos de grabación, el entorno del sistema debe cumplir los requisitos siguientes:

- 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 3.0
- SMB Transparent Failover (TFO)
- 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. Además, cuando se detecta un desbordamiento de diario, el espacio asignado dobla su tamaño cuando se detecta un desbordamiento, a un máximo de 2 GB.

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. Si el espacio libre en el volumen de origen es inferior a 100 MB, el agente de Microsoft SQL Server comprueba el espacio de volumen de origen y hace que falle la operación de copia de seguridad. 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 de base de datos se fuerza cuando se detectan las condiciones siguientes:

- Se notifica una discontinuidad del diario. Esta condición se puede producir cuando el registro alcanza su tamaño máximo, cuando el registro por diario está inhabilitado o cuando se cambia el ID de 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.

### Copias de seguridad de registros

Para asegurarse de que la copia de seguridad del registro de SQL funciona correctamente, es posible que tenga que actualizar los valores de Objeto de política de grupo de Windows. Par obtener más información, consulte [Objeto de política de grupo](#).

### Conectividad

Asegúrese de que se cumplen los siguientes requisitos de conectividad:

- El adaptador de red utilizado para la conexión debe configurarse como un cliente para Microsoft Networks.
- El servicio de Microsoft Windows Remote Management (WinRM) debe estar en ejecución.
- Los cortafuegos deben estar configurados para habilitar IBM Spectrum Protect Plus para conectarse al servidor utilizando WinRM.
- La dirección IP de la máquina que registra debe ser accesible desde el servidor IBM Spectrum Protect Plus y desde el servidor vSnap. SQL Server debe tener un servicio WinRM que esté a la escucha en el puerto 5985.
- Todos los servidores, proxies, aplicaciones e hipervisores que se añaden al entorno de IBM Spectrum Protect Plus deben registrarse utilizando un nombre de Sistema de nombres de dominio (DNS) o una dirección de Protocolo Internet (IP).
- Si se utilizan nombres DNS, deben poder resolverse en la red mediante el servidor de dispositivos virtuales IBM Spectrum Protect Plus y desde el servidor vSnap. Todos los componentes de IBM Spectrum Protect Plus también deben poder resolverse mediante sus nombres de DNS.

### Puertos

Los agentes de usuario de IBM Spectrum Protect Plus utilizan los puertos siguientes.

<i>Tabla 51. Puertos de comunicación cuando el destino está en un agente de IBM Spectrum Protect Plus</i>				
<b>Puerto</b>	<b>Protocolo</b>	<b>Iniciador</b>	<b>Objetivo</b>	<b>Descripción</b>
5985	Protocolo de control de transmisiones (TCP)	Dispositivo virtual IBM Spectrum Protect Plus <sup>1</sup>	Microsoft SQL Server	Proporciona acceso al servicio de Microsoft WinRm para servidores basados en Windows

*Tabla 51. Puertos de comunicación cuando el destino está en un agente de IBM Spectrum Protect Plus (continuación)*

<b>Puerto</b>	<b>Protocolo</b>	<b>Iniciador</b>	<b>Objetivo</b>	<b>Descripción</b>
5986	TCP	Dispositivo virtual IBM Spectrum Protect Plus <sup>1</sup>	Microsoft SQL Server	Proporciona acceso al servicio de Microsoft WinRm para servidores basados en Windows

<sup>1</sup> El dispositivo virtual IBM Spectrum Protect Plus contiene los componentes base: el servidor IBM Spectrum Protect Plus, el servidor vSnap y un proxy VADP, como se describe en [Componentes de producto](#).

*Tabla 52. Puertos de comunicación cuando el iniciador es un usuario agente de IBM Spectrum Protect Plus*

<b>Puerto</b>	<b>Protocolo</b>	<b>Iniciador</b>	<b>Objetivo</b>	<b>Descripción</b>
3260 El iniciador de iSCSI es necesario en este nodo.	TCP	Microsoft SQL Server	Servidor vSnap	El puerto de destino de vSnap del servicio de iniciador de Microsoft que se utiliza para montar LUNS para operaciones de copia de seguridad y recuperación
443	TCP	Agente de Microsoft SQL Server	Dispositivo virtual IBM Spectrum Protect Plus <sup>1</sup>	Puerto que permite al agente comunicarse con IBM Spectrum Protect Plus para enviar alertas en caso de errores de copia de seguridad del registro
445	TCP	Agente de Microsoft SQL Server	Servidor vSnap	Proporciona un puerto de destino de SMB o CIFS de servidor vSnap que se utiliza para montar recursos compartidos del sistema de archivos para operaciones de copia de seguridad y recuperación del registro de transacciones

<sup>1</sup> El dispositivo virtual IBM Spectrum Protect Plus contiene los componentes base: el servidor IBM Spectrum Protect Plus, el servidor vSnap y un proxy VADP, como se describe en [Componentes de producto](#).

## Actualización de puertos

- En Microsoft SQL Server, el puerto 443 está disponible en IBM Spectrum Protect Plus V10.1.4 y posterior.
- En versiones anteriores, los agentes de aplicación que utilizan SMBv1 utilizaron los puertos 137, 138 y 139 en el servidor vSnap. A partir de IBM Spectrum Protect Plus V10.1.6, no se utiliza el protocolo SMBv1. Todos los agentes utilizan SMBv2 o posterior, lo que no requiere los puertos 137, 138 o 139.

## Hardware

Tabla 53. Requisitos mínimos de hardware	
Sistema	Espacio en disco
Hardware compatible soportado por el sistema operativo y Microsoft SQL Server	Se instalará un mínimo de 500 MB de espacio en disco para el producto que se va a instalar

## 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 5693313](#).

### 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 181](#)

Puede actualizar el dispositivo virtual de IBM Spectrum Protect Plus o los 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 103](#)

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 105](#)

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 un servidor vSnap” en la página 111](#)

Cuando se despliega un dispositivo de IBM Spectrum Protect Plus, se instala automáticamente un servidor vSnap. Debe tener al menos un servidor vSnap instalado como parte del entorno de IBM Spectrum Protect Plus. Este servidor es el destino de copia de seguridad primario. En entornos de

empresa más grandes, es posible que se necesiten servidores vSnap adicionales. Los Blueprints le ayudarán a determinar cuántos servidores vSnap son necesarios.

## 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 23 y “Requisitos de copia de seguridad y restauración de hipervisor (Microsoft Hyper-V y VMware) e instancia en la nube (Amazon EC2)” en la página 41.
- Descargue el archivo de instalación de la plantilla del dispositivo virtual `<part_number>.ova` desde Passport Advantage Online. Para obtener información sobre la descarga de archivos, consulte [Nota técnica 5693313](#).
- 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 107.

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.

**Nota:** IBM Spectrum Protect Plus y el dispositivo vSnap es un sistema cerrado y no se admite la instalación antivirus (AV) en despliegues virtuales o físicos.

### Procedimiento

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

1. Despliegue IBM Spectrum Protect Plus. Utilizando vSphere Client (HTML5) o vSphere Web Client (FLEX), desde el menú **Acciones**, haga clic en **Desplegar plantilla OVF**.
2. Especifique la ubicación del archivo `<part_number>.ova` y selecciónela. Pulse **Siguiente**.
3. 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**.
4. Seleccione un recurso de cálculo de destino adecuado. Pulse **Siguiente**.

5. Revise los detalles de la plantilla. Pulse **Siguiente**.

**Importante:** Si utiliza vSphere Web Client (FLEX), verifique que `disk.enableUUID = true` aparezca en **Configuración adicional**. Si no es el caso o si utiliza vSphere Client (HTML5), continúe con los pasos de instalación y habilite esta opción desde vSphere Web Client más adelante.

6. Lea 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**.
7. 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**.
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. Especifique los valores de propiedad para el dispositivo virtual: Nombre de host, 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:** Estas propiedades se pueden configurar utilizando la herramienta de Interfaz de usuario de texto de 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 ( <code>nmtui</code> ).	Consulte <a href="#">Asignación de una dirección IP estática</a> .
Cargue la clave del producto.	Consulte “Carga de la clave de producto” en la <a href="#">página 107</a> .
Inicie IBM Spectrum Protect Plus desde un navegador web soportado.	Consulte “Iniciar IBM Spectrum Protect Plus” en la <a href="#">página 167</a> .

## 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 23 y “Requisitos de copia de seguridad y restauración de hipervisor (Microsoft Hyper-V y VMware) e instancia en la nube (Amazon EC2) ” en la página 41.
- Descargue el archivo de instalación `<part_number>.exe` desde Passport Advantage Online. Para obtener información sobre la descarga de archivos, consulte [Nota técnica 5693313](#).
- 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.

**Nota:** IBM Spectrum Protect Plus y el dispositivo vSnap es un sistema cerrado y no se admite la instalación antivirus (AV) en despliegues virtuales o físicos.

### Procedimiento

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

1. Copie el archivo `<part_number>.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 de navegación, haga clic en **Hardware > Controlador IDE 0 > 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 12, utilice un nombre distinto. 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 107](#).

**Importante:** Las máquinas virtuales de IBM Spectrum Protect Plus o vSnap que se despliegan utilizando clústeres de migración tras error Hyper-V deben configurarse con una dirección de control de acceso a soportes (MAC) estática para cada adaptador de red virtual. Si se utiliza una dirección MAC dinámica, la configuración de red de Linux se puede perder después de la migración tras error porque se asigna una nueva dirección MAC al adaptador de red virtual. La dirección MAC se puede configurar editando los valores de la máquina virtual en Hyper-V Manager o el gestor de clústeres de migración tras error. Asegurarse de que cada adaptador de red virtual tiene asignada una dirección MAC estática evitará la pérdida de la configuración de red.

### 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 <a href="#">“Carga de la clave de producto” en la página 107</a> .
Inicie IBM Spectrum Protect Plus desde un navegador web soportado.	Consulte <a href="#">“Iniciar IBM Spectrum Protect Plus” en la página 167</a> .



## 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-SysXyz`. Se le solicitará que cambie esta contraseña durante el primer inicio de sesión. Se imponen ciertas reglas al crear una contraseña nueva. Para obtener más información, consulte las reglas de requisitos de contraseña en [“Iniciar IBM Spectrum Protect Plus”](#) en la página 167.
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 103

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 105

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.

La aplicación de una clave de producto válida que utiliza el procedimiento siguiente habilitará las características de IBM Spectrum Protect Plus de forma indefinida.

### Procedimiento

**Nota:** Cuando se restaura una copia de seguridad del catálogo desde un servidor de IBM Spectrum Protect Plus que está utilizando una licencia para evaluación durante el periodo de evaluación en otro servidor IBM Spectrum Protect Plus que también utiliza una licencia para evaluación en el periodo de evaluación, se seguirá aplicando el recuento de días restantes de la licencia para evaluación del servidor de origen de copia de seguridad del catálogo. Esto no se aplica a las licencias de producción con claves de producto válidas.

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-SysXyz`.

Se le solicitará que cambie esta contraseña durante el primer inicio de sesión. Se imponen ciertas reglas al crear una contraseña nueva. Para obtener más información, consulte las reglas de requisitos de contraseña en [“Iniciar IBM Spectrum Protect Plus” en la página 167](#).

3. Haga clic en **Gestión de licencias**.
4. Haga clic en el botón **Actualizar licencia** y, a continuación, **Seleccionar archivo** para buscar la clave de producto en el sistema.
5. Pulse **Cargar una licencia nueva**.
6. Cuando se haya cargado el archivo de licencia, pulse **Cerrar 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 <a href="#">“Iniciar IBM Spectrum Protect Plus” en la página 167</a> .

## 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

Utilice los mandatos siguientes para abrir puertos en servidores proxy VADP remotos o servidores de aplicaciones.

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 de Linux incluyen Red Hat Enterprise Linux 6.8, Red Hat Enterprise Linux 7 y posterior, CentOS 7 y posterior 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 mandato siguiente 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 mandato siguiente 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
```

## Instalación de los programas de utilidad de iniciador iSCSI

Debe instalar los programas de utilidad de la Interfaz para pequeños sistemas de Internet (iSCSI) si los dispositivos de almacenamiento montados en iSCSI están conectados directamente al dispositivo de IBM Spectrum Protect Plus o en un servidor vSnap. Después de instalar los programas de utilidad de iniciador de iSCSI, los dispositivos de almacenamiento montados en iSCSI se pueden conectar al dispositivo o al servidor en el que está instalado el paquete.

### Acerca de esta tarea

Los programas de utilidad de iniciador iSCSI se pueden instalar en el dispositivo de IBM Spectrum Protect Plus o en un servidor vSnap. Los programas de utilidad de iniciador de iSCSI se entregan junto con IBM Spectrum Protect Plus, pero no se instalan automáticamente. Para instalar los programas de utilidad, siga el procedimiento.

### Procedimiento

1. Inicie sesión en el dispositivo o el servidor que se va a conectar directamente al almacenamiento montado en iSCSI.
  - Para el dispositivo de IBM Spectrum Protect Plus, utilice el protocolo Secure Shell (SSH) y auténtíquese con las credenciales administrativas adecuadas.
  - Para un servidor vSnap, utilice SSH o acceda al servidor directamente y auténtíquese con las credenciales administrativas adecuadas.
2. Instale los programas de utilidad de iniciador de iSCSI ejecutando el mandato siguiente:

```
sudo /usr/bin/yum --disablerepo=* --enablerepo=base,updates install iscsi-initiator-utils
```

---

## Capítulo 3. Instalación 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 IBM Spectrum Protect Plus. Un servidor de vSnap incorporado reside en una partición del dispositivo IBM Spectrum Protect Plus y se registra e inicializa en IBM Spectrum Protect Plus. El servidor vSnap incluido solo se debe utilizar para fines de demostración o prueba y no se utiliza en un entorno de producción. Se debe desplegar al menos un servidor vSnap en el entorno.

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 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 un servidor vSnap

Cuando se despliega un dispositivo de IBM Spectrum Protect Plus, se instala automáticamente un servidor vSnap. Debe tener al menos un servidor vSnap instalado como parte del entorno de IBM Spectrum Protect Plus. Este servidor es el destino de copia de seguridad primario. En entornos de empresa más grandes, es posible que se necesiten servidores vSnap adicionales. Los Blueprints le ayudarán a determinar cuántos servidores vSnap son necesarios.

#### Antes de empezar

Lleve a cabo los pasos siguientes:

1. Revise los requisitos del sistema vSnap en “Requisitos de los componentes ” en la página 23.
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 y otra información útil, consulte la siguiente página de soporte <https://www.ibm.com/support/pages/node/567387>.

**Nota:** IBM Spectrum Protect Plus y el dispositivo vSnap es un sistema cerrado y no se admite la instalación antivirus (AV) en despliegues virtuales o físicos.

**Importante:** Los componente de IBM Spectrum Protect Plus, incluido vSnap, no deben instalarse en la misma máquina, física o virtual, que IBM Spectrum Protect Server.

### 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 [“Instalación física del servidor vSnap”](#) en la [página 32](#) 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 a Permisiva:

```
SELINUX=permissive
```

3. Emita `setenforce 0` para aplicar el ajuste inmediatamente sin necesidad de reiniciar:

```
$ setenforce 0
```

4. Descargue el archivo de instalación de vSnap `<part_number>.run` desde Passport Advantage Online. Para obtener información sobre la descarga de archivos, consulte [Nota técnica 5693313](#).
5. Convierta el archivo en ejecutable y, a continuación, ejecútelo.

```
$ chmod +x <part_number>.run
```

6. Ejecute el ejecutable. Se instalan los paquetes de vSnap, además de todos los componentes necesarios.

```
$ ./<part_number>.run
```

De forma alternativa, las instalaciones no interactivas o las actualizaciones de vSnap se pueden iniciar utilizando la opción `noprompt`. Cuando se utiliza esta opción, el instalador de vSnap omitirá la solicitud de información para respuestas y asume una respuesta de "sí" a las siguientes solicitudes:

- Acuerdo de licencia
- Instalación o actualización de Kernel
- Vuelva a arrancar el final de la instalación o actualización si es necesario

Para utilizar la opción `noprompt`, emita el mandato siguiente. Observe el espacio deliberado antes y después de los guiones dobles:

```
$ sudo ./<part_number>.run -- noprompt
```

### 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 <a href="#">Capítulo 4, “Gestión de servidores vSnap”</a> , en la <a href="#">página 117</a> .

## Instalación de un servidor virtual vSnap en un entorno VMware

Para instalar un servidor vSnap virtual en un entorno de VMware, despliegue una plantilla OVF (Open Virtualization Format). Esto crea una máquina que contiene el servidor vSnap.

### 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 107](#), Trabajar con el administrador de red al configurar las propiedades de red.

## Procedimiento

1. Descargue el archivo de plantilla de servidor vSnap <part\_number>.ova desde Passport Advantage Online. Para obtener información sobre la descarga de archivos, consulte [Nota técnica 5693313](#).
2. Despliegue el servidor vSnap. Utilizando vSphere Client (HTML5) o vSphere Web Client (FLEX), haga clic en el menú **Acciones** y, a continuación, haga clic en **Desplegar plantilla OVF**.
3. Especifique la ubicación del archivo <part\_number>.ova y selecciónela. Pulse **Siguiente**.
4. 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**.
5. Seleccione un recurso de cálculo de destino adecuado. Pulse **Siguiente**.
6. Revise los detalles de la plantilla. Pulse **Siguiente**.
7. Lea 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 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**.
9. 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**.
10. 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.

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:** Es importante mantener encendida la máquina virtual.

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 <a href="#">Capítulo 4, “Gestión de servidores vSnap”</a> , en la <a href="#">página 117</a> .

Acción	Cómo
Para facilitar la administración de red, asigne una dirección IP estática a la máquina virtual. Utilice la herramienta de Interfaz de usuario de texto de NetworkManager (nmtui) para asignar la dirección IP.	Para obtener instrucciones, consulte <a href="#">“Asignación de una dirección IP estática”</a> en la página 107. Trabaje con el administrador de red cuando configure las propiedades de red.

## 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 un 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 `<part_number>.exe` desde Passport Advantage Online. Para obtener información sobre la descarga de archivos, consulte [Nota técnica 5693313](#).
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 107.

### 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 <a href="#">Capítulo 4, “Gestión de servidores vSnap”</a> , en la página 117.

## Desinstalación de un servidor vSnap

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

### Antes de empezar

Al suprimir de forma permanente el servidor vSnap, debe limpiar el servidor de IBM Spectrum Protect Plus. Los elementos que deben limpiarse en este caso son los siguientes:

- Registros de copias de seguridad que se almacenan en el servidor vSnap.
- Relaciones de duplicación con otros servidores vSnap.
- 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**. Debe anular el registro del servidor vSnap desde el servidor de IBM Spectrum Protect Plus. Consulte [“Anulación del registro de un servidor vSnap”](#) en la página 118 para obtener más información.



**Atención:** La desinstalación de un servidor vSnap puede dar como resultado la pérdida de datos.

### Procedimiento

1. Inicie la sesión en la consola del servidor vSnap con el ID de usuario `serveradmin`. La contraseña inicial es `sppDP758-SysXyz`. Se le solicitará que cambie esta contraseña durante el primer inicio de sesión. Se imponen ciertas reglas al crear una contraseña nueva. Para obtener más información, consulte las reglas de requisitos de contraseña en [“Iniciar IBM Spectrum Protect Plus”](#) en la página 167.

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 131.

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 de Hyper-V, suprima el dispositivo IBM Spectrum Protect Plus de Hyper-V y, a continuación, 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. Gestión de servidores vSnap

Para habilitar los trabajos de copia de seguridad y restauración, IBM Spectrum Protect Plus requiere al menos un servidor vSnap. El servidor vSnap es su propio dispositivo, desplegado virtualmente o instalado físicamente en un sistema que cumple los requisitos mínimos. Cada servidor vSnap del entorno debe registrarse en IBM Spectrum Protect Plus para que se pueda reconocer. El servidor vSnap registrado en el sitio de demostración que se incluye con IBM Spectrum Protect Plus se debe utilizar únicamente para fines de realización de pruebas y demostración, no se debe utilizar nunca como destino de copia de seguridad en un entorno de producción.

### Registro 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 y registrar un servidor vSnap como proveedor de almacenamiento de copias de seguridad, puede elegir configurar y administrar determinados aspectos de vSnap, como la configuración de red o la gestión de agrupaciones de almacenamiento. Para obtener más información, consulte el apartado [“Configuración de las opciones de almacenamiento de copias de seguridad”](#) en la página 120.

Si el servidor vSnap se va a registrar como un proxy VADP, la cuenta añadida en el campo **Propiedades de almacenamiento** para vSnap debe tener privilegios **sudo** para que ese registro de proxy VADP tenga éxito. Para obtener más información, consulte el apartado [“Tipos de permisos”](#) en la página 539.

#### Procedimiento

Para registrar un servidor vSnap como dispositivo de almacenamiento de copias de seguridad, realice los pasos siguientes:

1. Inicie la sesión en la consola del servidor vSnap con el ID de usuario `serveradmin`. La contraseña inicial es `sppDP758-SysXyz`.  
Se le solicitará que cambie esta contraseña durante el primer inicio de sesión. Se imponen ciertas reglas al crear una contraseña nueva. Para obtener más información, consulte las reglas de requisitos de contraseña en [“Iniciar IBM Spectrum Protect Plus”](#) en la página 167.
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 117](#).

#### 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 <a href="#">“Inicialización del servidor vSnap”</a> en la <a href="#">página 128</a> .
Expanda la agrupación de almacenamiento de vSnap.	Consulte <a href="#">“Configuración de socios de almacenamiento de copias de seguridad”</a> en la <a href="#">página 122</a> .
Si es necesario, configure y administre determinados aspectos de vSnap, como por ejemplo, la configuración de red o la gestión de agrupaciones de almacenamiento.	Consulte <a href="#">“Configuración de las opciones de almacenamiento de copias de seguridad”</a> en la <a href="#">página 120</a> .

#### Tareas relacionadas

[“Iniciar IBM Spectrum Protect Plus”](#) en la [página 167](#)


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**.

#### Anulación del registro de un servidor vSnap

Si es necesario, puede anular el registro de un servidor vSnap que ya no se utilice en el entorno de IBM Spectrum Protect Plus.

#### Antes de empezar

Cuando se anula el registro de un servidor vSnap, se depuran todos los puntos de recuperación asociados con el servidor vSnap de IBM Spectrum Protect Plus durante el siguiente trabajo de mantenimiento.



**Atención:** La anulación del registro de un servidor vSnap puede dar como resultado la pérdida de datos.

Antes de anular el registro de un servidor vSnap, revise los escenarios para determinar si la anulación del registro es apropiada o si se debe realizar otra acción.

**Escenario 1:** el servidor vSnap se ha caído temporalmente debido a problemas de red o almacenamiento.

- No anule el registro del servidor vSnap. Si anula el registro del servidor vSnap, se depurarán los puntos de recuperación asociados con el servidor y las copias de seguridad se reorganizarán.
- Complete el mantenimiento de red o almacenamiento necesario para que el servidor vSnap vuelva a estar en línea.

**Escenario 2:** el servidor vSnap tiene asignado un nombre de host o una dirección IP nuevos.

- No anule el registro del servidor vSnap. Si anula el registro del servidor vSnap, se depurarán los puntos de recuperación asociados con el servidor y las copias de seguridad se reorganizarán.
- Edite la configuración del servidor vSnap para especificar el nombre de host o la dirección IP nuevos. Para editar la configuración de un servidor vSnap, siga las instrucciones de [“Edición de valores para un servidor vSnap” en la página 118](#).

**Escenario 3:** el servidor vSnap no está en uso y no hay planes para reutilizarlo.

- Anule el registro del servidor vSnap y ejecute un trabajo de mantenimiento para garantizar que los puntos de recuperación asociados con el servidor vSnap se purgan desde IBM Spectrum Protect Plus.
  - Las copias de seguridad incrementales de los datos presentes en el servidor vSnap ya no serán posibles.
  - La recuperación de los datos presentes en el servidor vSnap ya no será posible.
- Las ejecuciones posteriores de los trabajos de copia de seguridad crearán automáticamente nuevos volúmenes en otro servidor vSnap en el mismo sitio y realizará nuevas copias de seguridad de base de datos.

**Escenario 4:** la agrupación de vSnap se ha perdido y desea crear una nueva agrupación en el mismo servidor vSnap.


1. Anule el registro del servidor vSnap y ejecute un trabajo de mantenimiento para garantizar que los puntos de recuperación asociados con la agrupación de vSnap antigua se depuran desde IBM Spectrum Protect Plus.
  - Las copias de seguridad incrementales de los datos presentes en la agrupación antigua ya no serán posibles.
  - La recuperación de los datos presentes en la agrupación antigua ya no será posible.
2. En el servidor vSnap, cree una agrupación.
3. Añada el servidor vSnap de nuevo IBM Spectrum Protect Plus. Para añadir un servidor vSnap a IBM Spectrum Protect Plus, consulte [“Registro de un servidor vSnap como proveedor de almacenamiento de copias de seguridad” en la página 117](#).
  - Las ejecuciones posteriores de los trabajos de copia de seguridad crearán automáticamente nuevos volúmenes en este o en otro servidor vSnap en el mismo sitio y realizará nuevas copias de seguridad de base de datos.

**Escenario 5:** la agrupación o el servidor vSnap se ha perdido y tiene la intención de repararlo. Esto puede lograrse replicando datos desde un servidor vSnap de réplica.

- No anule el registro del servidor vSnap de IBM Spectrum Protect Plus. El proceso de supresión provocará que las copias de seguridad se reorganicen.
- Sustituya el servidor vSnap. Para obtener información sobre la sustitución de un servidor vSnap primario que ha fallado, consulte esta sección [“Resolución de problemas de servidores vSnap” en la página 138](#).

## Procedimiento

Para anular el registro 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 suprimir  que está asociado a un servidor vSnap.
3. Confirme la eliminación del servidor vSnap escribiendo el código en el cuadro de texto. Haga clic en **DELETE** para suprimir el servidor de IBM Spectrum Protect Plus.

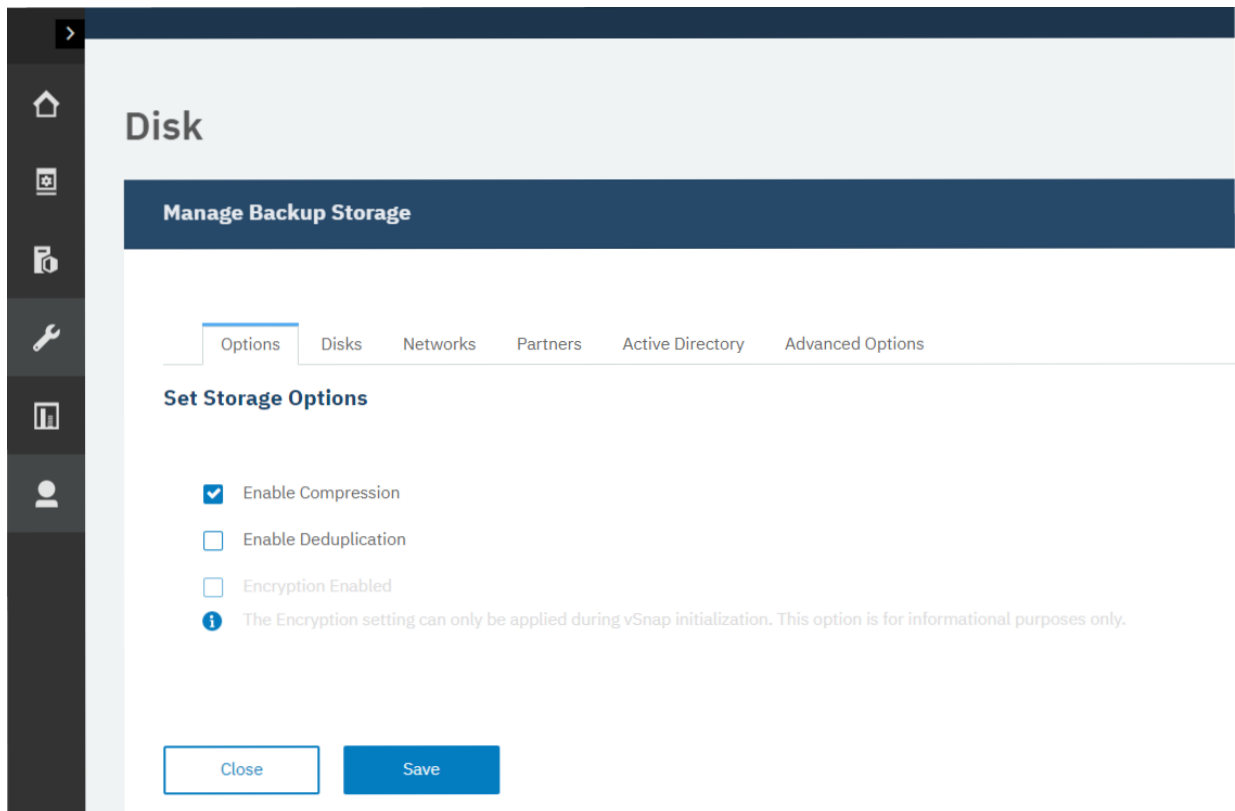
## Configuración de las opciones de almacenamiento de copias de seguridad

Puede configurar opciones relacionadas con el almacenamiento adicional para los host de almacenamiento de copias de seguridad primarias y secundarias.

### Procedimiento

Para configurar las opciones de almacenamiento de copias de seguridad para los discos registrados, complete los pasos siguientes:

1. En el panel de navegación, haga clic en **Configuración del sistema** , **Almacenamiento de copias de seguridad** > **Disco**.  
La tabla **Almacenamiento de disco** lista el nombre de host de los sitios primario y secundario con la versión y el uso de capacidad.
2. En el panel **Almacenamiento de disco**, haga clic en el icono de valores  asociado con el disco que desea actualizar.
3. Seleccione de las opciones de almacenamiento tal como se muestra.



**Habilitar compresión:** seleccione esta opción para comprimir los bloques de datos de entrada utilizando un algoritmo de compresión antes de que los datos se graben en la agrupación de almacenamiento. La compresión consume una cantidad moderada de recursos de CPU adicionales.

**Habilitar deduplicación:** seleccione esta opción para que a cada bloque de datos de entrada se le aplique un algoritmo hash y se compare 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 deduplicación no

está seleccionada 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 deduplicación de hashes de bloque.

**Cifrado habilitado:** esta opción muestra el estado de cifrado del host de almacenamiento de copias de seguridad primarias y secundarias. El cifrado solo se puede habilitar durante la inicialización de vSnap. Esta opción no se puede cambiar en este panel.



4. Pulse **Guardar**.

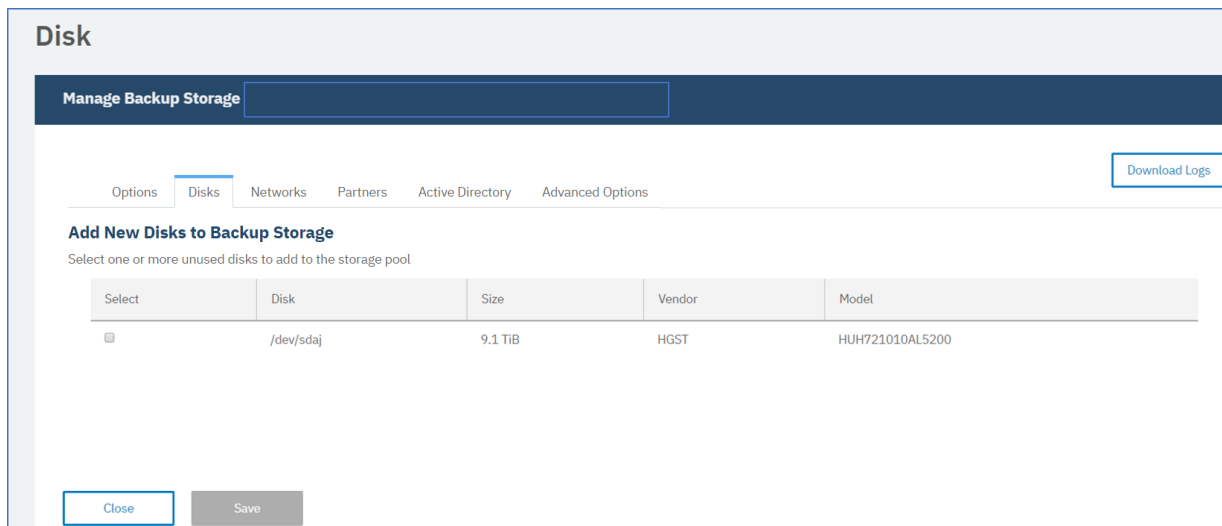
### Adición de nuevos discos al almacenamiento de copias de seguridad

Si necesita más espacio para las operaciones de copia de seguridad en una agrupación de almacenamiento seleccionada, puede añadir almacenamiento de disco no utilizado. Esto se aplica al almacenamiento de copias de seguridad primarias y secundarias.

### Procedimiento

Para añadir discos no utilizados nuevos a una agrupación de almacenamiento de disco, complete los pasos siguientes:

1. En el panel de navegación, haga clic en **Configuración del sistema** , **Almacenamiento de copias de seguridad** > **Disco**.
2. En el panel **Almacenamiento de disco**, haga clic en el icono de gestión  asociado con el servidor que desea editar.
3. Seleccione un disco para añadirlo a su entorno de almacenamiento de la lista de discos disponibles en la tabla **Añadir discos nuevos al almacenamiento de copias de seguridad**.



Select	Disk	Size	Vendor	Model
<input type="checkbox"/>	/dev/sdaj	9.1 TiB	HGST	HUH721010AL5200

4. Pulse **Guardar**.


### Configuración de controladores de interfaz de red

Puede configurar el almacenamiento de copias de seguridad primarias y secundarias para utilizar varios controladores de interfaz de red (NIC) para distintas funciones específicas. Se pueden configurar los NIC del entorno de IBM Spectrum Protect Plus para transferir datos para operaciones de copia de seguridad, restauración y réplica. Puede configurar un NIC para transferencias de datos de copia de seguridad, restauración y réplica, o para transferencias de datos de copia de seguridad y restauración o de réplica. Cuando configura NIC individuales, puede dedicar una red a operaciones de réplica y otra red a operaciones de copia de seguridad y restauración.

### Antes de empezar

Las versiones del servidor vSnap anteriores a V10.1.6 no dan soporte a esta característica. Para actualizar un servidor vSnap, siga las instrucciones en [“Actualización de servidores vSnap”](#) en la página 184.


## Acerca de esta tarea

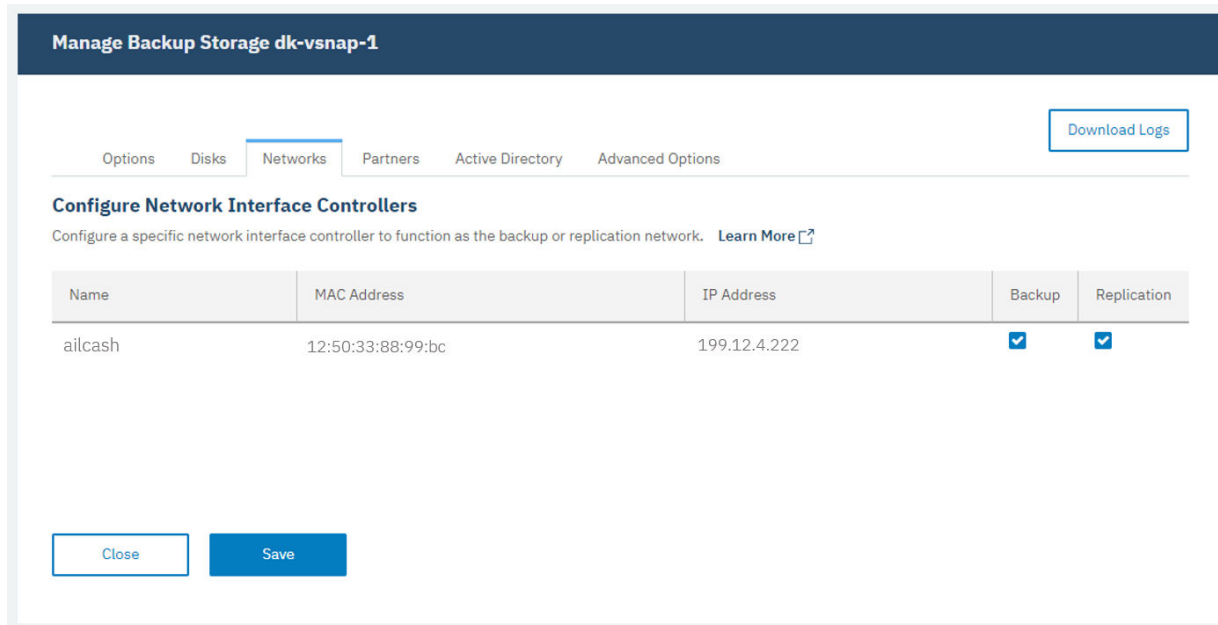
La red que se dedica a enviar mandatos de gestión desde IBM Spectrum Protect Plus al servidor vSnap se indica mediante el siguiente icono en la página **Red**, .

Se pueden establecer conexiones entre el servidor vSnap y un rango de clientes, incluidos servidores de aplicaciones, hosts de hipervisor, proxies VADP y cualquier otro componente del entorno que transfiera datos a y desde el almacenamiento de copias de seguridad.

## Procedimiento

Para configurar un NIC para las operaciones de réplica y de copia de seguridad, complete los pasos siguientes:

1. En el panel de navegación, haga clic en **Configuración del sistema** , **Almacenamiento de copias de seguridad > Disco**.
2. En la pestaña **Redes**, seleccione la configuración que desea para los NIC listados:
  - Para configurar un NIC para transferencias de datos únicamente para operaciones de copia de seguridad y restauración, seleccione **Copia de seguridad**. Durante las operaciones de copia de seguridad y restauración, las conexiones se establecen en el servidor vSnap mediante la dirección IP de este NIC. Si varios NIC especifican la opción **Copia de seguridad**, se utiliza el primero que se conecta correctamente.
  - Para configurar un NIC para transferencias de datos únicamente para fines de réplica, seleccione **Réplica**. Durante las operaciones de réplica de entrada en un servidor vSnap, las conexiones se establecen utilizando la dirección IP de este NIC en el servidor vSnap de destino. Si se especifica la opción **Réplica** para varios NIC en el servidor vSnap de destino, se utiliza la primera dirección IP de destino que se conecta correctamente desde el servidor vSnap de origen.
  - Para configurar un NIC para las transferencias de datos de réplica y, de copia de seguridad y restauración, seleccione **Copia de seguridad y Réplica**.



Manage Backup Storage dk-vsnap-1

Options Disks **Networks** Partners Active Directory Advanced Options [Download Logs](#)

**Configure Network Interface Controllers**  
Configure a specific network interface controller to function as the backup or replication network. [Learn More](#)

Name	MAC Address	IP Address	Backup	Replication
ailcash	12:50:33:88:99:bc	199.12.4.222	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[Close](#) [Save](#)

3. Pulse **Guardar**.

## Configuración de socios de almacenamiento de copias de seguridad

Puede configurar los sitios primario y secundario de almacenamiento de copias de seguridad para establecer asociaciones de réplica con otros sitios para ampliar el entorno. Después de configurar los socios de replicación, puede copiar datos de un sitio a otro para una capa añadida de protección de datos.




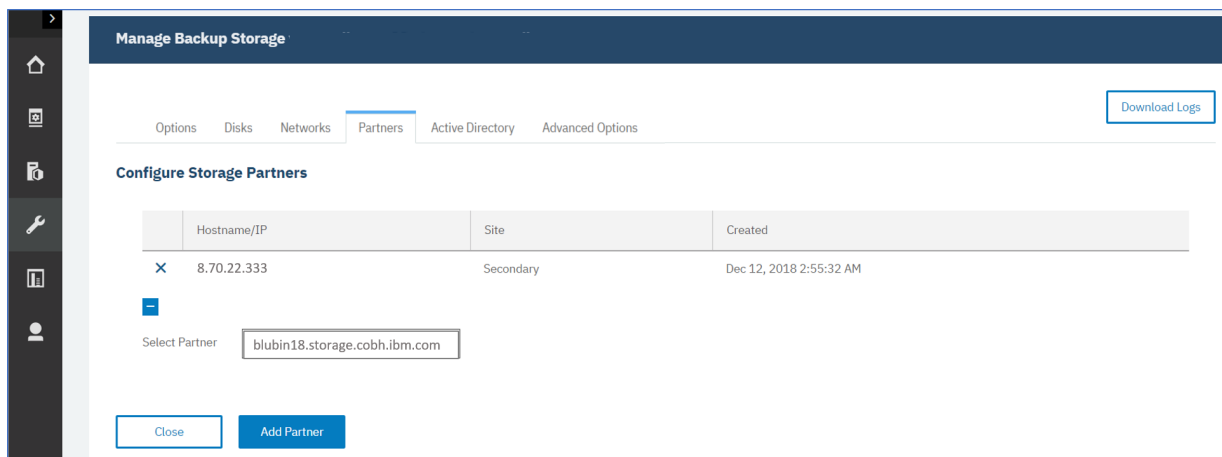
## Antes de empezar

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 añadir socios a un servidor en el entorno de almacenamiento, complete los pasos siguientes:

1. En el panel de navegación, haga clic en **Configuración del sistema** , **Almacenamiento de copias de seguridad > Disco**.  
Los socios configurados que ya se han añadido se listan en la tabla.
2. En el panel **Socios**, seleccione un socio para añadirlo al host de almacenamiento de copias de seguridad primarias y secundarias desde el menú desplegable.



3. Haga clic en **Añadir socio** para añadir el socio y cerrar la ventana.

## Configuración de Active Directory



Puede asociar el almacenamiento de copia de seguridad primario y secundario con un dominio de Active Directory. Cuando se añade el host primario o secundario a un dominio, los trabajos de copia de seguridad del registro de Microsoft SQL Server asociados con ese host utilizarán la autenticación de dominio para montar el volumen de copia de seguridad del registro. De esta forma, puede evitar el requisito para utilizar un área de transferencia local en el servidor de aplicaciones cuando se trate de operaciones de copia de seguridad del registro.

## Antes de empezar

Es posible que tenga que configurar el servidor Sistema de nombres de dominio (DNS) para que el controlador de dominio esté disponible en la red y se pueda asociar al host primario y secundario.

## Procedimiento

Para añadir un Active Directory para operaciones de seguridad y restauración, complete los pasos siguientes:

1. En el panel de navegación, haga clic en **Configuración del sistema** , **Almacenamiento de copias de seguridad > Disco**.
2. En la pestaña **Active Directory**, haga clic en el icono de gestión  que está asociado con el host primario o secundario que desea editar.
3. Especifique el nombre de dominio de Active Directory, junto con el nombre de usuario y contraseña para el administrador de Active Directory tal como se muestra en la imagen siguiente.

**Disk**

Manage Backup Storage veguardian-ce12.storage.tucson.ibm.com

Options Disks Networks Partners **Active Directory** Advanced Options

[Download Logs](#)

**Join Active Directory**

Domain Name: cupoftea\_aib.storage.n.com

Domain Administrator Username: admin

Domain Administrator Password: \*\*\*\*\*

[Close](#) [Join](#)



4. Pulse **Unir**.

### Configuración de opciones de almacenamiento avanzadas

Puede configurar opciones avanzadas relacionadas con el almacenamiento para el almacenamiento de copias de seguridad primarias o secundarias en su entorno.

### Procedimiento

Para configurar opciones avanzadas para el almacenamiento de copias de seguridad, complete los pasos siguientes:

1. En el panel de navegación, haga clic en **Configuración del sistema** , **Almacenamiento de copias de seguridad** > **Disco**.
2. En el panel **Gestionar almacenamiento de copias de seguridad**, haga clic en el icono de valores  asociado al host que está gestionando.
3. En la pestaña **Opciones avanzadas**, configure las opciones avanzadas como muestra el ejemplo siguiente:

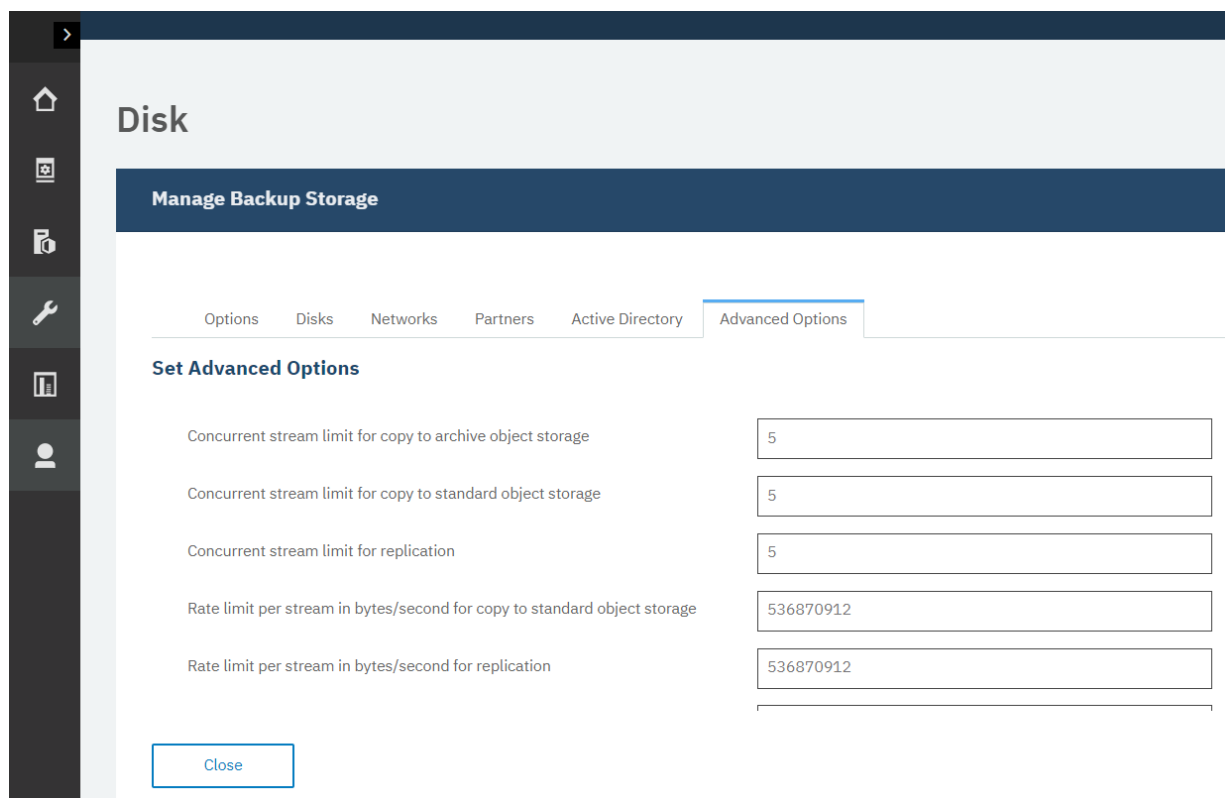


Figura 10. Gestionar opciones avanzadas del almacenamiento de copias de seguridad

- **Límite de secuencias simultáneas para copiar en el almacenamiento de objetos de archivado:** este valor define el número máximo de secuencias simultáneas que utiliza este host de copia de seguridad cuando está copiando datos en el almacenamiento de objetos de archivado.
- **Límite de secuencias simultáneas para copiar en el almacenamiento de objetos estándar:** este valor define el número máximo de secuencias simultáneas que utiliza este host de copia de seguridad cuando está copiando datos en el almacenamiento de objetos estándar.
- **Límite de secuencias simultáneas para réplica:** este valor define el número máximo de secuencias simultáneas que utiliza este host de copia de seguridad cuando está replicando datos en otros hosts de copia de seguridad.
- **Límite de velocidad por secuencia en bytes/segundo para copiar en el almacenamiento de objetos estándar:** este valor define la velocidad de transferencia máxima en bytes por segundo que utiliza el host de copia de seguridad para cada secuencia de datos cuando está copiando datos en el almacenamiento de objetos estándar. El valor especificado es el máximo en ausencia de otros factores de limitación. La velocidad actual de cada secuencia de datos puede ser menor que este valor y depende de los recursos del sistema disponibles, las condiciones de red y las limitaciones de ancho de banda definidas en las opciones del sitio.
- **Límite de velocidad por secuencia en bytes/segundo para réplica:** este valor define la velocidad de transferencia máxima en bytes por segundo que utiliza el host de copia de seguridad para cada secuencia de datos cuando está replicando. El valor especificado es el máximo en ausencia de otros factores de limitación. La velocidad actual de cada secuencia de datos puede ser menor que este valor y depende de los recursos del sistema disponibles, las condiciones de red y las limitaciones de ancho de banda definidas en las opciones del sitio.
- **Nivel de recuperación para la restauración desde el almacenamiento de objetos de archivado AWS (Masivo, Estándar o Acelerado):** este valor especifica el nivel de recuperación que utiliza este host de copia de seguridad durante las operaciones de restauración del almacenamiento de objetos de archivado de Amazon Glacier. Este valor debe especificarse como Masivo, Estándar o Acelerado. El nivel de recuperación se puede modificar para lograr tiempos de operación de restauración más rápidos a costa de cargos de datos más altos. Para obtener información sobre las

opciones de nivel de recuperación disponibles y el precio asociado, consulte la documentación de Amazon Web Services.


- **Copia de seguridad simultánea:** esta opción especifica el número máximo de secuencias de copias de seguridad paralelas en el host cuando se están ejecutando varios trabajos simultáneamente. Para las operaciones de copia de seguridad de aplicaciones, cada base de datos se trata como una única corriente. Para las operaciones de copia de seguridad de hipervisores, cada disco virtual se trata como una única corriente. Las opciones de copia de seguridad simultánea se pueden utilizar para impedir que varias políticas de SLA o políticas de SLA grandes envíen demasiadas secuencias de datos a un host de copia de seguridad pequeño que no puede alojar la carga. Para reducir el tiempo de procesamiento de las operaciones de copia de seguridad, establezca esta opción en una de las opciones siguientes:

**Ilimitado:** se puede ejecutar un número ilimitado de secuencias de copias de seguridad simultáneas.

**Pausar:** para pausar el uso de este host de copia de seguridad. Los trabajos que intentan utilizar este host de copia de seguridad se pondrán en pausa mientras este valor esté seleccionado. Esta opción debe utilizarse en situaciones en las que el host de copia de seguridad requiere mantenimiento de emergencia y evitará temporalmente que se utilice en cualquier trabajo.

**Limitar:** para establecer un límite máximo en el número de secuencias de copia de seguridad que se pueden ejecutar simultáneamente. Especifique un valor numérico que especifique el número máximo de secuencias simultáneas.

**Consejo:** Cuando cambia el valor de opción, el nuevo valor se aplica al hacer clic en el campo de

opción siguiente. Junto a la opción actualizada, se visualiza el siguiente mensaje,  **Updated**.

4. Haga clic en **Cerrar**.

## ¿Cómo puedo eliminar y volver a crear una agrupación de almacenamiento de vSnap?

Cuando surge un escenario con el requisito de suprimir una agrupación de almacenamiento vSnap debido a que está dañada o a cualquier otro motivo, puede seguir los pasos para suprimir y volver a crear la agrupación de almacenamiento. Este procedimiento es una operación destructiva que descarta todos los datos de una agrupación de almacenamiento de vSnap existente. Se pierden todos los datos de copia de seguridad de la agrupación y ya no se pueden recuperar, así que es necesaria cierta precaución antes de continuar. Cuando está hecho, puede crear una agrupación de sustitución vacía.

### Procedimiento

1. Para preparar la eliminación de una agrupación de almacenamiento, primero debe anular el registro del servidor vSnap eliminándolo.

Para obtener más información sobre anulación del registro del servidor vSnap, consulte [“Anulación del registro de un servidor vSnap”](#) en la página 118.

2. Ejecute un trabajo de mantenimiento en el servidor vSnap abriendo **Trabajos y operaciones** > **Planificar**. Busque el trabajo de *Mantenimiento* en la lista. Haga clic en el icono de acciones,



y, a continuación, en **Inicio**.

Cuando se completa el trabajo de mantenimiento, toda la información sobre el servidor vSnap se elimina del catálogo de SPP. Se eliminan todos los puntos de recuperación y metadatos asociados con las copias de seguridad de máquinas virtuales y todas las copias de réplica almacenadas en el vSnap no registrado. Se eliminan todos los datos y ya no están disponibles para recuperación.

Para obtener más información sobre los trabajos de mantenimiento, consulte [“Tipos de trabajo”](#) en la página 509.

3. En el servidor vSnap, ejecute el siguiente mandato para inicializar el servidor vSnap limpio.

```
$ vsnap system init --skip_pool
```

Si el sistema se ha inicializado previamente, es seguro volver a ejecutar este mandato. Este paso garantiza que los módulos de kernel necesarios estén instalados y cargados.

- Identifique el identificador de la agrupación de almacenamiento existente ejecutando el mandato siguiente:

```
$ vsnap pool show
```

Si la agrupación de almacenamiento está en línea, el identificador se muestra en el campo *ID*. Si la agrupación de almacenamiento está fuera de línea, se muestra un mensaje de error que indica que no se puede visualizar la información de la agrupación. El identificador de la agrupación se muestra en este mensaje de error.

- Ejecute el mandato delete para que el identificador de agrupación de almacenamiento suprima a la fuerza la agrupación de almacenamiento.

```
$ vsnap pool delete --id <ID> --force
```

Cuando el mandato finaliza, se muestra el siguiente mensaje:

```
La agrupación de almacenamiento se ha suprimido correctamente pero la agrupación no se ha
desmontado porque se ha establecido la opción 'force'.
Reinicie el sistema para asegurarse de que los discos que se estaban utilizando
anteriormente ahora se han liberado.
```

- Reinicie el sistema para liberar los discos que todavía están en uso. Escriba el mandato siguiente:

```
$ sudo reboot -n
```

Es importante reiniciar el sistema después de ejecutar este mandato para asegurarse de que se liberan los discos que todavía están utilizando las agrupaciones más antiguas.

- Cuando finalice el reinicio, ejecute el mandato de estado:

```
$ vsnap_status
```

La salida de este mandato muestra el estado de todos los servicios de servidor vSnap. Asegúrese de que todos los servicios están activos. Si se están activando uno o más servicios, compruebe el estado más tarde para ver que todos están en estado activo.

- Identifique los discos que deben añadirse a la agrupación.

Si está reutilizando el mismo conjunto de discos que componían la agrupación antigua, el siguiente mandato le ayudará a identificarlos:

```
$ vsnap disk show
```

En la salida del mandato show, la columna **USED AS** indica si existe una tabla de particiones o sistema de archivos en el disco. Los discos que formaban parte de la agrupación antigua se identifican como vsnap\_pool. Si la agrupación antigua estaba cifrada, algunos o todos los discos se pueden identificar como CRYPTO\_LUKS.

Ejemplo de salida

UUID KNAME   NAME	TYPE	VENDOR	MODEL	SIZE	USED AS
6000c299371bdc647c80720602079bc   sda   /dev/sda	SCSI	VMware	Virtual disk	70.00GB	LVM2_member
6000c29b8ea25349e3a884d58f72e640   sdb   /dev/sdb	SCSI	VMware	Virtual disk	100.00GB	vsnap_pool
6000c297cb8078cf9f56ab688a326a24   sdc   /dev/sdc	SCSI	VMware	Virtual disk	128.00GB	LVM2_member
6000c2950248c5d831b6661ab0ec8843   sdd   /dev/sdd	SCSI	VMware	Virtual disk	16.00GB	vsnap_pool
6000c29359661cbd915a7f24c8b44cf8   sde   /dev/sde	SCSI	VMware	Virtual disk	16.00GB	vsnap_pool

9. **Importante:** El mandato de este paso suprime las tablas de particiones y los metadatos del sistema de archivos de los discos especificados y los marca como no utilizados. Utilice este mandato con precaución y asegúrese de especificar solo discos que ya no estén en uso.

Ejecute el mandato siguiente para especificar una lista separada por comas de los nombres de disco que se van a marcar como no utilizados.

```
$ vsnap disk wipe <disk_list>
```

El mandato siguiente es un ejemplo del mandato disk wipe: `$ vsnap disk wipe /dev/sdb,/dev/sdd,/dev/sde`.

10. Cree la nueva agrupación con el siguiente mandato:

```
$ vsnap pool create --name <pool_name> <options> --disk_list <disk_list>
```

Donde *pool\_name* es el nombre de la nueva agrupación; *options* especifica opciones de cifrado o de tipo RAID. Dejar esta opción en blanco aplica las opciones predeterminadas. *disk\_list* representa la lista separada por comas de discos que se van a añadir a la agrupación. Los discos que especifique deben tener un estado de no utilizado al ejecutar el mandato **vsnap disk show**.

El mandato siguiente es un ejemplo del mandato create:

```
$ vsnap pool create --name primary --disk_list /dev/sdb,/dev/sdd
```

Cuando especifique la lista de discos, especifique solo los discos que desea utilizar como discos de datos principales. Se pueden añadir discos de registro o de memoria caché más tarde ejecutando mandatos independientes. Para obtener más información sobre las recomendaciones e instrucciones para configurar los discos de registro y de memoria caché, consulte [Blueprints](#).

#### Consejo:

Para abrir la ayuda, ejecute el mandato `vsnap pool create --help`.

11. Para ver la información de agrupación, ejecute el mandato siguiente:

```
$ vsnap pool show
```

Asegúrese de que el mandato muestra la información de agrupación correcta y de que el mandato se completa sin un error.

12. Registre el servidor vSnap en IBM Spectrum Protect Plus en un sitio elegido para finalizar la configuración.

Para obtener más información sobre cómo registrar un servidor vSnap, consulte [“Registro de un servidor vSnap como proveedor de almacenamiento de copias de seguridad”](#) en la página 117.

## 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 debe ejecutarse en instalaciones nuevas.

#### Acerca de esta tarea

Durante el proceso de inicialización, vSnap crea una agrupación de almacenamiento utilizando los discos no utilizados disponibles conectados al sistema para una instalación física. Si no se encuentra ningún disco no utilizado, el proceso de inicialización se completa sin crear una agrupación. Para un despliegue virtual de vSnap, se define un disco virtual no utilizado de 100 GB predeterminado y se utiliza para crear la agrupación.

Para obtener información sobre cómo expandir, crear y administrar agrupaciones de almacenamiento, consulte [“Gestión de almacenamiento”](#) en la página 133.

Puede utilizar la interfaz de usuario de IBM Spectrum Protect Plus o la interfaz de línea de mandatos (CLI) de vSnap para inicializar servidores vSnap.

En el caso de los servidores que se despliegan o añaden a IBM Spectrum Protect Plus, la interfaz de usuario de IBM Spectrum Protect Plus proporciona un método simple para ejecutar la operación de inicialización.

En el caso de los servidores que se despliegan en un entorno físico, la interfaz de línea de mandatos (CLI) 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 el vSnap incorporado que se instala como parte de una instalación de IBM Spectrum Protect Plus, se le solicitará que inicie el proceso de inicialización la primera vez que inicie sesión en la interfaz de usuario. No es necesario realizar pasos adicionales. El servidor vSnap que está en el sitio de demostración que se incluye con IBM Spectrum Protect Plus se debe utilizar únicamente para fines de realización de pruebas y demostración, no se debe utilizar nunca como destino de copia de seguridad en un entorno de producción.

### 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 icono del menú de acciones  asociado con el 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. 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` mediante SSH. Cuando se despliega virtualmente, la contraseña inicial es `sppDP758-SysXyz`. Se le solicitará que cambie esta contraseña durante el primer inicio de sesión. Se imponen ciertas reglas al crear una contraseña nueva. Para obtener más información, consulte las reglas de requisitos de contraseña en [“Iniciar IBM Spectrum Protect Plus” en la página 167](#). Si se despliega físicamente, utilice la contraseña que ha creado para la cuenta de `serveradmin` durante la instalación. También puede utilizar un ID de usuario que tenga privilegios de vSnap que se han creado anteriormente 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 131.

2. Emita el mandato **\$ vsnap system init** con la opción **--skip\_pool** para inicializar el servidor vSnap pero sin crear una agrupación de almacenamiento. El proceso puede tardar entre 5 y 10 minutos en completarse. Emita el mandato siguiente:

```
$ vsnap system init --skip_pool
```

### Qué hacer a continuación

Después de completar la inicialización, complete la acción siguiente:

Acción	Cómo
Crear una agrupación de almacenamiento	Consulte <a href="#">“Gestión de almacenamiento”</a> en la página 133.

## 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.

### Antes de empezar

Se deben añadir discos virtuales o físicos al servidor vSnap antes de este procedimiento. No se admite la ampliación de volúmenes existentes.

### 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.

## Cambio de la tasa de rendimiento

Cambie el rendimiento de las operaciones de réplica y copia 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 11. 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.

## Sustitución de un servidor vSnap que falla

En un entorno de IBM Spectrum Protect Plus, el servidor vSnap de destino es el destino para la copia de seguridad de datos. Si el servidor vSnap no puede responder o está dañado, puede sustituirlo por un servidor nuevo y recuperar los datos almacenados.

### Antes de empezar

**Importante:** No anule el registro del servidor vSnap que ha fallado de IBM Spectrum Protect Plus. El servidor que ha fallado debe permanecer registrado para que el procedimiento de sustitución funcione correctamente.

Debe existir uno o más servidores de réplica vSnap iniciado y activo en el entorno para que se pueda completar correctamente este proceso.

### Acerca de esta tarea

El procedimiento para sustituir un servidor vSnap que ha fallado se documenta en la [nota técnica 1103847](#).

## 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.


Es posible que tenga que 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

El servidor vSnap se puede gestionar mediante la interfaz de línea de mandatos y es el principal medio de administración de un servidor vSnap. Ejecute el mandato **vsnap** desde la interfaz del servidor vSnap después de conectarse a través de SSH utilizando el ID de usuario **serveradmin** o cualquier otro usuario de sistema operativo que tenga asignados privilegios de administración de vSnap. La contraseña de **serveradmin** inicial es **sppDP758-SysXyz**. Se le solicitará que cambie esta contraseña durante el primer inicio de sesión. Se imponen ciertas reglas al crear una contraseña nueva. Para obtener más información, consulte las reglas de requisitos de contraseña en [“Iniciar IBM Spectrum Protect Plus” en la página 167](#).

La interfaz de línea de mandatos consta de varios mandatos y submandatos que gestionan varios aspectos del sistema. 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 editar sus valores.

#### Tareas relacionadas

[“Gestión de servidores vSnap” en la página 117](#)

Para habilitar los trabajos de copia de seguridad y restauración, IBM Spectrum Protect Plus requiere al menos un servidor vSnap. El servidor vSnap es su propio dispositivo, desplegado virtualmente o instalado físicamente en un sistema que cumple los requisitos mínimos. Cada servidor vSnap del entorno debe registrarse en IBM Spectrum Protect Plus para que se pueda reconocer. El servidor vSnap registrado en el sitio de demostración que se incluye con IBM Spectrum Protect Plus se debe utilizar únicamente para fines de realización de pruebas y demostración, no se debe utilizar nunca como destino de copia de seguridad en un entorno de producción.

[“Configuración de opciones de almacenamiento avanzadas” en la página 124](#)

Puede configurar opciones avanzadas relacionadas con el almacenamiento para el almacenamiento de copias de seguridad primarias o secundarias en su entorno.

### Gestión de usuarios

Puede gestionar usuarios del servidor vSnap emitiendo el mandato **vsnap user**. Este mandato y las opciones disponibles se utilizan para crear usuarios, otorgar y revocar privilegios de usuario, consultar usuarios y actualizar la contraseña de un usuario.

Los usuarios que se crean en un servidor vSnap son usuarios del sistema operativo que se añaden al grupo de sistemas operativos de vSnap. Los usuarios del grupo de sistemas operativos de vSnap no tienen privilegios **sudo** asignados. Como resultado, estos usuarios necesitan una contraseña para ejecutar un mandato.

Puede crear un usuario de vSnap emitiendo el mandato **create**. De este modo, puede crear un usuario de sistema operativo asignado al grupo **vsnap** que puede ejecutar mandatos vSnap y realizar llamadas de API. Emita el mandato **create**:

```
$ vsnap user create
```

Si se ejecuta interactivamente, se le solicitará que especifique el nombre de usuario, la contraseña y la contraseña una segunda vez para la confirmación. Si se ejecuta de una forma no interactiva, están disponibles las siguientes opciones para el mandato **create**:

**--username <username>**

Especifique el nombre de usuario del usuario.

**--password <password>**

Especifique la contraseña del usuario.

Puede otorgar privilegios a una cuenta de sistema operativo existente para asegurarse de que el usuario puede ejecutar mandatos de vSnap y realizar llamadas de API. Para otorgar privilegios, emita el mandato **grant**:

```
$ vsnap user grant
```

Si se ejecuta interactivamente, se le solicitará que especifique el nombre de usuario, la contraseña y la contraseña una segunda vez para la confirmación. Si se ejecuta de una forma no interactiva, están disponibles las siguientes opciones para el mandato **grant**:

**--username <username>**

Especifique el nombre de usuario del usuario.

**--password <password>**

Especifique la contraseña del usuario. Esta debe ser la contraseña de la cuenta de sistema operativo si la cuenta ya existe en el sistema.

Puede revocar privilegios de un usuario asignado al grupo **vsnap**. El usuario permanecerá como usuario de sistema operativo pero ya no podrá ejecutar mandatos de vSnap o realizar llamadas de API. Para revocar privilegios, emita el mandato **Revoke**:

```
$ vsnap user revoke
```

Si se ejecuta interactivamente, se le solicitará que especifique el nombre de usuario. Si se ejecuta de una forma no interactiva, están disponibles las siguientes opciones para el mandato **revoke**:

**--username <username>**

Especifique el nombre de usuario del usuario.

Para visualizar una lista de los usuarios de vSnap que forman parte del grupo **vsnap** en el servidor vSnap, emita el mandato **show**:

```
$ vsnap user show
```

Un usuario de vSnap puede cambiar la contraseña de la cuenta que actualizará esa contraseña de usuario en el sistema. Emita el mandato **update**:

```
$ vsnap user update
```

Si se ejecuta interactivamente, se le solicitará que especifique el nombre de usuario, la contraseña antigua, la contraseña nueva y la contraseña nueva una segunda vez para la confirmación. Si se ejecuta de una forma no interactiva, están disponibles las siguientes opciones para el mandato **update**:

**--username <username>**

Especifique el nombre de usuario del usuario.

**--password <old\_password>**

Especifique la contraseña antigua del usuario.

**--new\_password <new\_password>**

Especifique la contraseña nueva del usuario.

## 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 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.



**Atención:** Una vez que se ha añadido un disco a una agrupación de almacenamiento, no debe eliminarse. La eliminación de un disco dañará la agrupación de almacenamiento.

Si vSnap se ha desplegado como parte de un dispositivo virtual, ya contiene un disco virtual de inicio de 100 GB. Revise los detalles en [Blueprints](#) para obtener información sobre cómo gestionar este disco y cómo eliminarlo. 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 utilicen configuraciones RAID y 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. 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 en otra ubicación fuera del servidor vSnap. Después de crear una agrupación, utilice los mandatos siguientes como usuario `serveradmin` para copiar las claves en una ubicación temporal y, a continuación, copiarlas en una ubicación de copia de seguridad segura y deseada fuera del host vSnap.

En primer lugar, cree un directorio en el que se realizará una copia de seguridad de las claves.

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

A continuación, copie los archivos de claves en la ubicación temporal.


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

Por último, copie el directorio keybackup-*<hostname>* donde *<hostname>* es el nombre asignado al servidor vSnap en una ubicación de copia de seguridad segura fuera del host de vSnap.

## 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:** Haga clic en **Configuración del sistema > Almacenamiento de copia de seguridad > Disco** en el panel de navegación y, a continuación, haga clic en el icono del menú de acciones  al lado del servidor vSnap relevante y seleccione **Volver a explorar**.

## 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 129](#), 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 135](#). Para obtener información sobre las opciones disponibles, pase la opción **-- 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 135](#).

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. Haga clic en el icono de gestión  para que lo gestione un servidor vSnap y, a continuación, expanda la pestaña **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.

La red en un servidor vSnap se puede modificar a través de la interfaz de línea de mandatos (CLI) mediante el uso del mandato **network**. Se puede obtener información adicional utilizando la opción **-- help** después de cualquier mandato.

### Mostrar información de interfaz de red

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

```
$ vsnap network show
```

De forma predeterminada, los siguientes servicios de vSnap están disponibles en todas las interfaces de red:

#### mgmt

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

#### repl

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

## nfs

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

## smb

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

## iscsi

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

## Modificación de servicios asociados con interfaces de red

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

```
$ vsnap network update
```

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. Los valores siguientes son valores válidos: **mgmt**, **repl**, **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.

## Instalación de herramientas y cabeceras de kernel

Las herramientas y cabeceras de kernel no están instaladas de forma predeterminada. Si tiene previsto compilar y utilizar controladores personalizados, módulos o otro software, instale la herramienta o cabecera de kernel adecuada en el servidor vSnap.

### Acerca de esta tarea

Cuando se instala o actualiza vSnap, el kernel de Linux versión 4.19 está instalado de forma predeterminada. Si renuncia a la actualización de kernel a V4.19 y permanece en V3.10, se instala y utiliza un kernel V3.10 que es compatible con el servidor vSnap. En ambos casos, no se instalan las herramientas y cabeceras de kernel asociadas con el kernel. Si tiene previsto compilar y utilizar controladores personalizados, módulos o otro software, debe instalar los paquetes de kernel. Los instaladores de Red Hat Package Manager (RPM) para las herramientas y cabeceras de kernel están disponibles en el directorio de instalación de vSnap.

### Procedimiento

1. Inicie la sesión en el servidor vSnap como el usuario **serveradmin**. La contraseña inicial es **sppDP758-SysXyz**. Se le solicitará que cambie esta contraseña durante el primer inicio de sesión. Se imponen ciertas reglas al crear una contraseña nueva. Para obtener más información, consulte las reglas de requisitos de contraseña en [“Iniciar IBM Spectrum Protect Plus” en la página 167](#).
2. Para determinar la versión de kernel de Linux, abra una línea de mandatos y emita el mandato siguiente:

```
$ uname -r
```

Se muestra la salida, donde **xxxx** representa el número de revisión del kernel:

```
$ 4.19.xxxx
```

3. Vaya hasta este directorio:

```
$ cd /opt/vsnap/config/pkgs/kernel/
```

4. En el directorio, localice el archivo `xxxxxxx.rpm`, que es el paquete que se va a instalar. Asegúrese de que se ha identificado el paquete correcto para la versión de kernel de Linux instalada. Para instalar la herramienta o cabecera de kernel, emita el mandato siguiente:

```
$ sudo yum localinstall xxxxxx.rpm
```

### Resultados

Se ha instalado la herramienta o cabecera de kernel.

## Resolución de problemas de servidores vSnap

Los servidores vSnap en un entorno de IBM Spectrum Protect Plus proporcionan almacenamiento de disco para proteger los datos mediante procesos de copia de seguridad y de réplica. El servidor vSnap configurado en el entorno puede utilizarse como destino, origen o como servidor y destino. Para reparar o sustituir un servidor vSnap que ha fallado, hay pasos a seguir para que el servidor vSnap afectado se lleve primero a un estado de trabajo para que se puedan reanudar los servicios de copia de seguridad y réplica. Esto es para garantizar una pérdida de datos mínima.

### Impedir errores en trabajos sincronizando las contraseñas de vSnap y CIFS

Las comunicaciones entre un servidor vSnap y un recurso compartido de Common Internet File System (CIFS) se pueden interrumpir si se comparten las credenciales, pero las contraseñas no están sincronizadas. Para impedir que los trabajos fallen, debe sincronizar las contraseñas de vSnap y CIFS.

#### Acerca de esta tarea

Para obtener información sobre cómo sincronizar contraseñas, consulte [“Gestión de usuarios” en la página 132](#).

### ¿Por qué el servidor vSnap sigue fuera de línea?

Después de reiniciar el servidor vSnap, continúa mostrando un estado de fuera de línea en la interfaz de usuario de IBM Spectrum Protect Plus .

Si la deduplicación de datos está habilitada o se había habilitado previamente en un servidor vSnap, la tabla de deduplicación (DDT) se precarga en la memoria durante el proceso de inicio del servidor vSnap. El proceso de precarga de DDT puede introducir un retraso de 15 minutos en el inicio de los servicios de servidor vSnap. Durante este tipo, el servidor vSnap se muestra con un estado de Fuera de línea. Espere al menos 15 minutos para que se complete el proceso y para que el servidor vSnap vuelva al estado En línea. Puede ejecutar el mandato `vsnap_status` para supervisar los servicios del servidor vSnap.

Si alguno de los servicios de vSnap está en estado Activando, esto significa que los servicios de vSnap se están iniciando. Cuando todos los servicios están en el estado activo, el servidor vSnap vuelve a estar en línea.

### ¿Cómo puedo reparar un servidor vSnap fallido en mi entorno de IBM Spectrum Protect Plus?

Los servidores vSnap configurados en el entorno de IBM Spectrum Protect Plus proporcionan almacenamiento en disco para proteger los datos mediante procesos de copia de seguridad y de réplica. Si uno de los servidores vSnap de su entorno falla o debe sustituirse, debe realizar pasos para reparar el servidor para restaurar los datos almacenados ahí, y para que pueda proporcionar correctamente servicios de copia de seguridad y réplica.



## Acerca de esta tarea

### Importante:

**Nota:** Se supone que todos los servidores vSnap del entorno están protegidos por la réplica. Si un servidor vSnap no se replica y se pierde, no se puede recuperar en un estado que le permita continuar actuando en su rol de almacenamiento de disco de origen o destino. En ausencia de réplica, debe crear servidores vSnap nuevos y configurar políticas de acuerdo de nivel de servicio (SLA). Cuando se ejecutan, se produce un nuevo proceso de copia de seguridad completo.

Un servidor vSnap puede funcionar en su entorno en los roles siguientes:

- vSnap como almacenamiento de disco de *origen* para operaciones de copia de seguridad
- vSnap como almacenamiento de disco de *destino* para aplicaciones de réplica de otro servidor vSnap
- El servidor vSnap que sirve como *origen* y *destino* para servicios de copia de seguridad y réplica.

La operación de reparación está diseñada para recuperar un servidor vSnap en un estado que le permite continuar el proceso normal. Los resultados de la operación de reparación dependen de los roles del servidor vSnap que se está reparando:

- Si está reparando un servidor vSnap de origen, la operación de reparación recuperará el último punto de recuperación del servidor vSnap de destino para que las operaciones de copia de seguridad puedan continuar procesando los cambios incrementales de las cargas de trabajo de producción y no requieran una copia de seguridad completa. Tenga en cuenta que en este caso los puntos de recuperación anteriores al punto de recuperación más reciente en el servidor vSnap de origen no se restaurarán, pero aún estarán disponibles para la recuperación y reutilización en el servidor vSnap de destino.
- Si está reparando un servidor vSnap de destino, la operación de reparación restablecerá la relación de forma que la siguiente operación de réplica se pueda ejecutar normalmente. El proceso de reparación no transferirá datos. Una vez que finalice el proceso de reparación, el procesamiento continuará de la siguiente manera:
  - Los datos de copia de seguridad incremental se enviarán al servidor vSnap de destino de origen por la ejecución de planificación de SLA.
  - El trabajo de réplica se iniciará por la planificación de SLA y replicará todos los puntos de recuperación creados en el servidor vSnap de origen después de que se haya ejecutado el proceso de reparación. En este momento los datos se replicarán desde el servidor vSnap de origen al servidor vSnap de destino. Esta es una transferencia de datos completa de todos los datos necesarios para representar los puntos de recuperación más recientes mencionados anteriormente.

En función del rol del servidor vSnap, siga las instrucciones de las secciones siguientes:

## Procedimiento

### ¿Cómo reparo un vSnap de origen que ha fallado en un entorno de IBM Spectrum Protect Plus?

Los servidores vSnap en un entorno de IBM Spectrum Protect Plus proporcionan almacenamiento de disco para proteger los datos mediante procesos de copia de seguridad y de réplica. Puede reparar y sustituir un servidor vSnap que ha fallado que esté configurado en el entorno de IBM Spectrum Protect Plus para que actúe como el *origen* para los servicios de copia de seguridad y réplica. El servidor vSnap de origen debe repararse para que puedan reanudarse los servicios de copia de seguridad y réplica.

### Antes de empezar

**Importante:** Se supone que todos los servidores vSnap del entorno están protegidos por la réplica. Si un servidor vSnap no se replica y falla, no se puede recuperar en un estado que le permita continuar como un origen de almacenamiento de disco o un destino. En ausencia de procesos de réplica, debe crear un servidor vSnap nuevo y configurar políticas de acuerdo de nivel de servicio (SLA). Cuando ejecuta las políticas, se ejecuta un nuevo proceso de copia de seguridad completo en el nuevo servidor vSnap.

Para determinar qué tipo de proceso de reparación es aplicable al servidor vSnap, consulte [nota técnica 1103847](#).

### Acerca de esta tarea

**Importante:** No anule el registro ni suprima el servidor vSnap que ha fallado de IBM Spectrum Protect Plus. El servidor vSnap fallido debe permanecer registrado para que el procedimiento de sustitución funcione correctamente.

Este procedimiento establece un servidor vSnap de origen nuevo en el entorno de IBM Spectrum Protect Plus para sustituir un servidor vSnap de origen que ha fallado. El nuevo servidor vSnap de origen solo contendrá los puntos de recuperación más recientes.

**Nota:** La versión del nuevo servidor vSnap debe coincidir con la versión del dispositivo IBM Spectrum Protect Plus desplegado.

### Procedimiento

1. Inicie sesión en la consola de servidor vSnap de destino con el ID serveradmin mediante el protocolo Secure Shell (SSH).

Escriba el mandato siguiente: `$ ssh serveradmin@MGMT_ADDRESS`

Por ejemplo, `$ ssh serveradmin@10.10.10.2`

2. Obtenga el ID del servidor vSnap de origen fallido abriendo un indicador de mandatos y especificando el siguiente mandato:

`$ vsnap partner show`

La salida es similar a la que se muestra en el ejemplo siguiente:

```
ID: 12345678901234567890123456789012
PARTNER TYPE: vsnap
MGMT ADDRESS: 10.10.10.1
API PORT: 8900
SSH PORT: 22
```

3. Verifique que MGMT ADDRESS es la dirección del servidor vSnap de origen que ha fallado. Tome nota del número de ID del servidor vSnap de origen que ha fallado.
4. En el entorno con el servidor vSnap de origen, instale un servidor vSnap nuevo del mismo tipo y versión, y con la misma asignación de almacenamiento, que el servidor vSnap de origen que ha fallado.

Para obtener instrucciones sobre la instalación de un servidor vSnap, consulte [Instalación de un servidor vSnap físico](#).

**Importante:** No registre el nuevo servidor vSnap con IBM Spectrum Protect Plus. No utilice el asistente Añadir almacenamiento de disco.

- a) Primero deberá inicializar el servidor vSnap con el siguiente mandato:

`$ vsnap system init ----skip_pool id partner_id`

Por ejemplo: `$ vsnap system init --skip_pool --id 12345678901234567890123456789012` utilizando el ID de socio del vSnap de origen que ha fallado. Un mensaje indica que la inicialización se ha completado.

**Nota:** Este mandato es diferente al mandato de inicialización de vSnap listado en IBM Knowledge Center y en Blueprints.

5. Complete el proceso de creación de agrupación y del servidor vSnap como se indica en *Capítulo 5: instalación y configuración del servidor vSnap* en Blueprints.
6. Coloque el nuevo servidor vSnap de origen en modalidad de mantenimiento especificando el siguiente mandato:

`$ vsnap system maintenance begin`

La colocación del servidor vSnap en modalidad de mantenimiento suspende operaciones como la creación de instantáneas, los trabajos de restauración de datos y las operaciones de réplica.

7. Inicialice el nuevo servidor vSnap de origen con el ID de socio del servidor vSnap de origen que ha fallado. Escriba el mandato siguiente:

```
$ vsnap system init --id partner_id
```

El mandato siguiente es un ejemplo: `$ vsnap system init --id 12345678901234567890123456789012`

8. En el nuevo servidor vSnap de origen, añada los servidores vSnap de socio. Cada socio debe añadirse por separado. Para añadir un socio, escriba el mandato siguiente:

```
$ vsnap partner add --remote_addr remote_ip_address --local_addr local_ip_address
```

donde, *remote\_ip\_address* especifica la dirección IP del servidor vSnap de origen y *local\_ip\_address* especifica la dirección IP del nuevo servidor vSnap de origen.

El mandato siguiente es un ejemplo:

```
$ vsnap partner add --remote_addr 10.10.10.2 --local_addr 10.10.10.1
```

9. Cuando se le solicite, especifique el ID de usuario y la contraseña para el servidor vSnap de destino. Los mensajes informativos indican cuándo se crean y actualizan los socios correctamente.

10. Cree una tarea de reparación en el nuevo servidor vSnap de origen especificando el mandato siguiente:

```
$ vsnap repair create --async
```

La salida de este mandato es similar al ejemplo siguiente:

```
ID: 12345678901234567890123456789012
PARTNER TYPE: vsnap
PARTNER ID: abcdef7890abcdef7890abcdef7890ab
TOTAL VOLUMES: N/A
SNAPSHOTS RESTORED: N/A
RETRY: No
CREATED: 2019-11-01 15:49:31 UTC
UPDATED: 2019-11-01 15:49:31 UTC
ENDED: N/A
STATUS: PENDING
MESSAGE: La reparación se ha planificado
```

11. Supervise el número de volúmenes implicados en la operación de reparación especificando el siguiente mandato:

```
$ vsnap repair show
```

La salida de este mandato es similar al ejemplo siguiente:

```
ID: 12345678901234567890123456789012
PARTNER TYPE: vsnap
PARTNER ID: abcdef7890abcdef7890abcdef7890ab
TOTAL VOLUMES: 3
SNAPSHOTS RESTORED: N/A
RETRY: No
CREATED: 2019-11-01 15:49:31 UTC
UPDATED: 2019-11-01 15:49:31 UTC
ENDED: N/A
STATUS: ACTIVE
MESSAGE: Se han creado 0 volúmenes. Hay 3 volúmenes primarios que tienen instantáneas recuperables, se restaurará la instantánea más reciente de cada uno de ellos. Restaurando 3 instantáneas: 3 activas, 0 pendientes, 0 completadas y 0 han fallado
```

El número de volúmenes implicados en la operación de reparación se indica en el campo TOTAL VOLUMES.

12. Supervise el estado de la tarea de reparación visualizando el archivo `repair.log` en el nuevo servidor vSnap de origen, en el siguiente directorio `/opt/vsnap/log/repair.log`. Alternativamente, puede escribir el mandato siguiente:

```
$ vsnap repair show
```

La salida de este mandato es similar al ejemplo anterior. Se pueden visualizar los siguientes mensajes de estado durante el proceso de reparación:

- STATUS: PENDING indica que el trabajo de reparación se va a ejecutar.
- STATUS: ACTIVE indica que el trabajo de reparación está activo.
- STATUS: COMPLETED indica que el trabajo de reparación se ha completado.
- STATUS: FAILED indica que el trabajo de reparación ha fallado y debe reenviarse.

13. Durante la operación de reparación, ejecute el mandato vSnap repair show para verificar cuando se ha completado el estado.

```
$ vsnap repair session show
```

La salida de este mandato es similar al ejemplo siguiente:

```
ID: 1 RELATIONSHIP: 72b19f6a9116a46aae6c642566906b31
PARTNER TYPE: vsnap
LOCAL SNAP: 1313
REMOTE SNAP: 311
STATUS: ACTIVE
SENT: 102.15GB
STARTED: 2019-11-01 15:51:18 UTC
ENDED: N/A
Se han creado 0 volúmenes.
Hay 3 volúmenes de réplica cuyas instantáneas se restaurarán en la próxima réplica.
```

Se muestra una sesión para cada volumen implicado en la operación de reparación.

Emita periódicamente el mandato `$vsnap repair session show` para asegurarse de que la cantidad de datos que se envían para cada volumen aumenta en incrementos. Cuando finalicen las sesiones, verá el cambio de estado a COMPLETED. Cuando finalicen todas las sesiones, emita el mandato `$ vsnap repair session show` para verificar que el estado global es COMPLETED. Se visualiza un mensaje final que indica el número de volúmenes para los que se han restaurado las instantáneas. La salida del mensaje es similar al ejemplo siguiente:

```
Se han creado 0 volúmenes.
Hay 3 volúmenes primarios que tienen instantáneas recuperables, se restaurará la
instantánea más reciente de cada uno de ellos.
Se han restaurado 3 instantáneas.
```

14. Para las instantáneas que no se han restaurado y que indican un estado FAILED, vuelva a enviar el proceso de reparación especificando el siguiente mandato:

```
$ vsnap repair create --async --retry
```

15. Cuando el proceso de reparación informa de un estado COMPLETED, puede reanudar las operaciones normales para el servidor vSnap sacándolo de la modalidad de mantenimiento. Para reanudar el procesamiento normal, escriba el mandato siguiente:

```
$ vsnap system maintenance complete
```

16. Elimine las claves de host de SSH guardadas del servidor vSnap de origen reparado y de los servidores vSnap de destino.

Ejecute los mandatos siguientes en los servidores vSnap de origen y de destino:

```
$ sudo rm -f /home/vsnap/.ssh/known_hosts
```

```
$ sudo rm -f /root/.ssh/known_hosts
```

La eliminación de las claves SSH garantiza que las transferencias de réplica posteriores no generan errores que resulten de la clave de host modificada del servidor vSnap reparado.

17. Reinicie el servicio de vSnap en el servidor sustituido escribiendo el mandato siguiente:

```
$ sudo systemctl restart vsnap
```

18. Haga clic en **Configuración del sistema > Almacenamiento de copias de seguridad > Disco** para verificar que el servidor vSnap nuevo se ha registrado correctamente, de la siguiente manera:
  - Si el nuevo servidor vSnap utiliza el mismo nombre de host o dirección IP para el registro, no es necesario ningún cambio.
  - Si el nuevo servidor vSnap utiliza un nombre de host o una dirección IP distintos para el registro, debe actualizar el registro seleccionando el icono de lápiz.
19. Para eliminar los puntos de recuperación que ya no están disponibles en el servidor vSnap de origen, inicie un trabajo de mantenimiento desde la interfaz de usuario de IBM Spectrum Protect Plus. Para obtener instrucciones, consulte [Creación de trabajos y planificaciones de trabajos](#).

**Consejo:** Es posible que vea mensajes informativos similares al ejemplo siguiente:

```
CTGGA1843 storage snapshot spp_1004_2102_2_16de41fcbc3 not found on live Storage2101  
Snapshot Type vsnap
```

20. Para reanudar los trabajos que han fallado después de que el servidor vSnap pasara a no estar disponible, ejecute un trabajo de inventario del servidor de almacenamiento. Para obtener instrucciones, consulte [Creación de trabajos y planificaciones de trabajos](#).

### Resultados

El servidor vSnap de origen se ha reparado solo con los puntos de recuperación más recientes. El siguiente trabajo de copia de seguridad que se ejecuta como parte de un SLA realizará una copia de seguridad de los datos de forma incremental. Si crea un trabajo de restauración, solo estará disponible el punto de recuperación más reciente en el repositorio de copia de seguridad. Todos los puntos de recuperación estarán disponibles en los repositorios de réplica, y en los repositorios del almacenamiento de objetos y del almacenamiento de archivos, si es aplicable a su entorno.

## ¿Cómo reparo un vSnap de destino que ha fallado en un entorno de IBM Spectrum Protect Plus?

Los servidores vSnap en un entorno de IBM Spectrum Protect Plus proporcionan almacenamiento de disco para proteger los datos mediante procesos de copia de seguridad y de réplica. Puede reparar y sustituir un servidor vSnap que ha fallado que esté configurado en el entorno de IBM Spectrum Protect Plus para que actúe como el *destino* para los servicios de copia de seguridad y réplica. El servidor vSnap de origen debe repararse para que puedan reanudarse los servicios de copia de seguridad y réplica.

### Antes de empezar

**Importante:** Se supone que todos los servidores vSnap del entorno están protegidos por la réplica. Si un servidor vSnap no se replica y falla, no se puede recuperar en un estado que le permita continuar como un origen de almacenamiento de disco o un destino. En ausencia de procesos de réplica, debe crear un servidor vSnap nuevo y configurar políticas de acuerdo de nivel de servicio (SLA). Cuando ejecuta las políticas, se ejecuta un nuevo proceso de copia de seguridad completo en el nuevo servidor vSnap.

### Acercas de esta tarea

**Importante:** No anule el registro ni suprima el servidor vSnap que ha fallado de IBM Spectrum Protect Plus. El servidor vSnap fallido debe permanecer registrado para que el procedimiento de sustitución funcione correctamente.

Este procedimiento establece un servidor vSnap de destino nuevo en el entorno de IBM Spectrum Protect Plus para sustituir un servidor vSnap de destino que ha fallado. El nuevo servidor vSnap de destino no contendrá datos pero se llenará con los puntos de recuperación más recientes durante la siguiente operación de réplica planificada.

**Nota:** La versión del nuevo servidor vSnap debe coincidir con la versión del dispositivo IBM Spectrum Protect Plus desplegado.

Para determinar qué tipo de proceso de reparación es aplicable al servidor vSnap, consulte [nota técnica 1103847](#).

## Procedimiento

1. Inicie sesión en la consola de servidor vSnap que está funcionando con el ID serveradmin mediante el protocolo Secure Shell (SSH).  
Escriba el mandato siguiente: `$ ssh serveradmin@MGMT_ADDRESS`  
Por ejemplo, `$ ssh serveradmin@10.10.10.1`
2. Obtenga el ID del servidor vSnap fallido abriendo un indicador de mandatos y especificando el siguiente mandato:

```
$ vsnap partner show
```

La salida es similar a la que se muestra en el ejemplo siguiente:

```
ID: 12345678901234567890123456789012
PARTNER TYPE: vsnap
MGMT ADDRESS: 10.10.10.2
API PORT: 8900
SSH PORT: 22
```

3. Verifique que MGMT ADDRESS es la dirección del servidor vSnap que ha fallado. Tome nota del número de ID del servidor vSnap que ha fallado.
4. En el entorno con el servidor vSnap de destino, instale un servidor vSnap nuevo del mismo tipo y versión, y con la misma asignación de almacenamiento, que el servidor vSnap de destino que ha fallado.

Para obtener instrucciones sobre la instalación de un servidor vSnap, consulte [Instalación de un servidor vSnap físico](#).

**Importante:** No registre el nuevo servidor vSnap con IBM Spectrum Protect Plus. No utilice el asistente Añadir almacenamiento de disco.

- a) Primero deberá inicializar el servidor vSnap con el siguiente mandato:

```
$ vsnap system init --skip_pool --id <partner_id>
```

Por ejemplo: `$ vsnap system init --skip_pool --id 12345678901234567890123456789012` utilizando el ID de socio del vSnap de origen que ha fallado. Un mensaje indica que la inicialización se ha completado.

**Nota:** Este mandato es diferente al mandato de inicialización de vSnap listado en IBM Knowledge Center y en Blueprints.

5. Complete el proceso de creación de agrupación y del servidor vSnap como se indica en [Capítulo 5: instalación y configuración del servidor vSnap](#) en [Blueprints](#).
6. Coloque el nuevo servidor vSnap en modalidad de mantenimiento especificando el siguiente mandato:

```
$ vsnap system maintenance begin
```

La colocación del servidor vSnap en modalidad de mantenimiento suspende operaciones como la creación de instantáneas, los trabajos de restauración de datos y las operaciones de réplica.

7. Inicialice el nuevo servidor vSnap de destino con el ID de socio del servidor vSnap de destino que ha fallado. Escriba el mandato siguiente:

```
$ vsnap system init --id <partner_id>
```

El mandato siguiente es un ejemplo:

```
$ vsnap system init --id 12345678901234567890123456789012
```

- En el nuevo servidor vSnap de destino, añada los servidores vSnap de socio. Cada socio debe añadirse por separado. Para añadir un socio, escriba el mandato siguiente:

```
$ vsnap partner add --remote_addr <remote_ip_address> --local_addr <local_ip_address>
```

donde, *<remote\_ip\_address>* especifica la dirección IP del servidor vSnap de origen y *<local\_ip\_address>* especifica la dirección IP del nuevo servidor vSnap de destino.

El mandato siguiente es un ejemplo:

```
$ vsnap partner add --remote_addr 10.10.10.1 --local_addr 10.10.10.2
```

- Cuando se le solicite, especifique el ID de usuario y la contraseña para el servidor vSnap de origen. Los mensajes informativos indican cuándo se crean y actualizan los socios correctamente.
- Cree una tarea de reparación en el nuevo servidor vSnap de origen especificando el mandato siguiente:

```
$ vsnap repair create --async
```

La salida de este mandato es similar al ejemplo siguiente:

```
ID: 12345678901234567890123456789012
PARTNER TYPE: vsnap
PARTNER ID: abcdef7890abcdef7890abcdef7890ab
TOTAL VOLUMES: N/A
SNAPSHOTS RESTORED: N/A
RETRY: No
CREATED: 2019-11-01 15:49:31 UTC
UPDATED: 2019-11-01 15:49:31 UTC
ENDED: N/A
STATUS: PENDING
MESSAGE: La reparación se ha planificado
```

- Supervise el número de volúmenes implicados en la operación de reparación especificando el siguiente mandato:

```
$ vsnap repair show
```

La salida de este mandato es similar al ejemplo siguiente:

```
ID: 12345678901234567890123456789012
PARTNER TYPE: vsnap
PARTNER ID: abcdef7890abcdef7890abcdef7890ab
TOTAL VOLUMES: 3
SNAPSHOTS RESTORED: N/A
RETRY: No
CREATED: 2019-11-01 15:49:31 UTC
UPDATED: 2019-11-01 15:49:31 UTC
ENDED: N/A
STATUS: ACTIVE
MESSAGE: Creando 3 volúmenes para el socio 670d61a10f78456bb895b87c45e20999
```

El número de volúmenes implicados en la operación de reparación se indica en el campo TOTAL VOLUMES.

- Supervise el estado de la tarea de reparación visualizando el archivo repair.log en el nuevo servidor vSnap de origen, en el siguiente directorio /opt/vsnap/log/repair.log. Alternativamente, puede escribir el mandato siguiente:

```
$ vsnap repair show
```

La salida de este mandato es similar al ejemplo anterior. Se pueden visualizar los siguientes mensajes de estado durante el proceso de reparación:

- STATUS: PENDING indica que el trabajo de reparación se va a ejecutar.
- STATUS: ACTIVE indica que el trabajo de reparación está activo.
- STATUS: COMPLETED indica que el trabajo de reparación se ha completado.

- STATUS: FAILED indica que el trabajo de reparación ha fallado y debe reenviarse.
13. Durante la operación de reparación, ejecute el mandato vSnap repair show para verificar cuando se ha completado el estado.

```
$ vsnap repair session show
```

El mensaje final indica el número de volúmenes cuyas instantáneas se restaurarán en la siguiente réplica, de la siguiente manera:

```
Se han creado 0 volúmenes.  
Hay 3 volúmenes de réplica cuyas instantáneas se restaurarán en la próxima réplica.
```

14. Para las instantáneas que no se han restaurado y que indican un estado FAILED, vuelva a enviar el proceso de reparación especificando el siguiente mandato:

```
$ vsnap repair create --async --retry
```

15. Cuando el proceso de reparación informa de un estado COMPLETED, puede reanudar las operaciones normales para el servidor vSnap sacándolo de la modalidad de mantenimiento. Para reanudar el procesamiento normal, escriba el mandato siguiente:

```
$ vsnap system maintenance complete
```

16. Elimine las claves de host de SSH guardadas del servidor vSnap de origen reparado y de los servidores vSnap de destino.

Ejecute los mandatos siguientes en los servidores vSnap de origen y de destino:

```
$ sudo rm -f /home/vsnap/.ssh/<known_hosts>
```

```
$ sudo rm -f /root/.ssh/<known_hosts>
```

La eliminación de las claves SSH garantiza que las transferencias de réplica posteriores no generan errores que resulten de la clave de host modificada del servidor vSnap reparado.

17. Reinicie el servicio de vSnap en el servidor sustituido escribiendo el mandato siguiente.

```
$ sudo systemctl restart vsnap
```

18. Haga clic en **Configuración del sistema > Almacenamiento de copias de seguridad > Disco** para verificar que el servidor vSnap nuevo se ha registrado correctamente, de la siguiente manera:

- Si el nuevo servidor vSnap utiliza el mismo nombre de host o dirección IP para el registro, no es necesario ningún cambio.
- Si el nuevo servidor vSnap utiliza un nombre de hostname o una dirección IP distintos para el registro, debe actualizar el registro seleccionando el icono de lápiz.

19. Para eliminar los puntos de recuperación que ya no están disponibles en el servidor vSnap de origen, inicie un trabajo de mantenimiento desde la interfaz de usuario de IBM Spectrum Protect Plus.

**Consejo:** Es posible que vea mensajes informativos similares al ejemplo siguiente:

```
CTGGA1843 storage snapshot spp_1004_2102_2_16de41fcbc3 not found on live Storage2101  
Snapshot Type vsnap
```

20. Para reanudar los trabajos que han fallado después de que el servidor vSnap pasara a no estar disponible, ejecute un trabajo de inventario del servidor de almacenamiento.

## Resultados

No se ha podido reparar el servidor vSnap de destino. Se debe ejecutar un trabajo de copia de seguridad nuevo en el servidor vSnap de origen antes de realizar ninguna acción adicional en el nuevo servidor vSnap de destino.



Si se intenta un trabajo de réplica en el nuevo servidor vSnap de destino, se muestra un mensaje de la siguiente manera:

```
CTGGA0289 - omisión del volumen <id_volumen> porque no hay instantáneas nuevas desde la última copia de seguridad
```

Después de ejecutar un trabajo de copia de seguridad nuevo en el servidor vSnap de origen, el siguiente trabajo de réplica planificado replica los puntos de recuperación creados por el trabajo de copia de seguridad. En este punto, si crea un trabajo de restauración, solo estará disponible el punto de recuperación más reciente en el repositorio de réplica. Si el servidor vSnap de destino también actuaba como origen de copia para el almacenamiento de objetos o archivos, el trabajo de réplica debe ejecutarse primero en el servidor vSnap de destino antes de que puedan completarse correctamente operaciones de copia adicionales. La primera copia de datos en el almacenamiento de objetos será una copia completa.

## ¿Cómo puedo reparar un vSnap de rol dual que ha fallado en un entorno de IBM Spectrum Protect Plus?

Puede reparar y sustituir un servidor vSnap que ha fallado que esté configurado en el entorno de IBM Spectrum Protect Plus para actuar como *origen* y *destino* para los servicios de copia de seguridad y de réplica.

### Acerca de esta tarea

**Importante:** No anule el registro ni suprima el servidor vSnap fallido de IBM Spectrum Protect Plus. El servidor vSnap fallido debe permanecer registrado para que el procedimiento de sustitución funcione correctamente.

Este procedimiento establece un nuevo servidor vSnap en el entorno de IBM Spectrum Protect Plus para sustituir el servidor vSnap que ha fallado. Una vez completado el proceso de reparación, el nuevo servidor vSnap se recupera en un punto en el que los trabajos de copia de seguridad pueden continuar haciendo copia de seguridad de los cambios incrementales (no se requiere una copia de seguridad completa) y los trabajos de réplica pueden continuar.

Para determinar qué tipo de proceso de reparación es aplicable al servidor vSnap, consulte [nota técnica 1103847](#).

**Nota:** La versión del nuevo servidor vSnap debe coincidir con la versión del dispositivo IBM Spectrum Protect Plus desplegado.

### Procedimiento

1. Inicie sesión en el servidor vSnap que está funcionando en la consola de entorno con el ID `serveradmin` utilizando el protocolo Secure Shell (SSH).  
Escriba el mandato siguiente: `$ ssh serveradmin@MGMT_ADDRESS`  
Por ejemplo, `$ ssh serveradmin@10.10.10.2`
2. Obtenga el ID del servidor vSnap fallido abriendo un indicador de mandatos y especificando el siguiente mandato:

```
$ vsnap partner show
```

La salida es similar a la que se muestra en el ejemplo siguiente:

```
ID: 12345678901234567890123456789012
PARTNER TYPE: vsnap
MGMT ADDRESS: 10.10.10.1
API PORT: 8900
SSH PORT: 22
```

3. Verifique que `MGMT ADDRESS` es la dirección del servidor vSnap que ha fallado. Tome nota del número de ID del servidor vSnap que ha fallado.
4. En el servidor vSnap de destino, instale un nuevo servidor vSnap del mismo tipo y versión, y con la misma asignación de almacenamiento, que el servidor vSnap de origen que ha fallado.

Para obtener instrucciones sobre la instalación de un servidor vSnap, consulte [Instalación de un servidor vSnap físico](#).

**Importante:** No registre el nuevo servidor vSnap con IBM Spectrum Protect Plus. No utilice el asistente Añadir almacenamiento de disco.

a) Primero deberá inicializar el servidor vSnap con el siguiente mandato:

```
$ vsnap system init ----skip_pool id partner_id
```

Por ejemplo: `$ vsnap system init --skip_pool --id 12345678901234567890123456789012` utilizando el ID de socio del vSnap de origen que ha fallado. Un mensaje indica que la inicialización se ha completado.

**Nota:** Este mandato es diferente al mandato de inicialización de vSnap listado en IBM Knowledge Center y en Blueprints.

5. Complete el proceso de creación de agrupación y del servidor vSnap como se indica en *Capítulo 5: instalación y configuración del servidor vSnap* en [Blueprints](#).

6. Coloque el nuevo servidor vSnap en modalidad de mantenimiento especificando el siguiente mandato:

```
$ vsnap system maintenance begin
```

La colocación del servidor vSnap en modalidad de mantenimiento suspende operaciones como la creación de instantáneas, los trabajos de restauración de datos y las operaciones de réplica.

7. Inicialice el nuevo servidor vSnap de destino con el ID de socio del servidor vSnap de destino que ha fallado. Especifique el siguiente mandato para inicializar el vSnap:

```
$ vsnap system init --id partner_id
```

El mandato siguiente es un ejemplo: `$ vsnap system init --id 12345678901234567890123456789012`

8. En el nuevo servidor vSnap de destino, añada los servidores vSnap de socio. Si hay más de un servidor asociado, cada socio debe añadirse por separado. Para añadir un socio, escriba el mandato siguiente:

```
$ vsnap partner add --remote_addr remote_ip_address --local_addr local_ip_address
```

donde, `remote_ip_address` especifica la dirección IP del servidor vSnap de origen y `local_ip_address` especifica la dirección IP del nuevo servidor vSnap de destino.

El mandato siguiente es un ejemplo:

```
$ vsnap partner add --remote_addr 10.10.10.1 --local_addr 10.10.10.2
```

9. Cuando se le solicite, especifique el ID de usuario y la contraseña para el servidor vSnap de origen. Los mensajes informativos indican cuándo se crean y actualizan los socios correctamente.

10. Cree una tarea de reparación en el nuevo servidor vSnap de origen especificando el mandato siguiente:

```
$ vsnap repair create --async
```

La salida de este mandato es similar al ejemplo siguiente:

```
ID: 12345678901234567890123456789012
PARTNER TYPE: vsnap
PARTNER ID: abcdef7890abcdef7890abcdef7890ab
TOTAL VOLUMES: N/A
SNAPSHOTS RESTORED: N/A
RETRY: No
CREATED: 2019-11-01 15:49:31 UTC
UPDATED: 2019-11-01 15:49:31 UTC
ENDED: N/A
STATUS: PENDING
MESSAGE: La reparación se ha planificado
```

- Supervise el número de volúmenes implicados en la operación de reparación especificando el siguiente mandato:

```
$ vsnap repair show
```

La salida de este mandato es similar al ejemplo siguiente:

```
ID: 12345678901234567890123456789012
PARTNER TYPE: vsnap
PARTNER ID: abcdef7890abcdef7890abcdef7890ab
TOTAL VOLUMES: 6
SNAPSHOTS RESTORED: N/A
RETRY: No
CREATED: 2019-11-01 15:49:31 UTC
UPDATED: 2019-11-01 15:49:31 UTC
ENDED: N/A
STATUS: ACTIVE
MESSAGE: Se han creado 0 volúmenes
Hay 3 volúmenes de réplica cuyas instantáneas se restaurarán en la próxima réplica.
Hay 3 volúmenes primarios que tienen instantáneas recuperables, se restaurará la
instantánea más reciente de cada uno de ellos.
El número de volúmenes implicados en la operación de reparación se indica en el campo TOTAL
VOLUMES
```

- Supervise el estado de la tarea de reparación visualizando el archivo repair.log en el nuevo servidor vSnap de origen, en el siguiente directorio /opt/vsnap/log/repair.log. Alternativamente, puede escribir el mandato siguiente:

```
$ vsnap repair show
```

- Cuando el estado de la operación de reparación está en el estado ACTIVE, puede ver el estado de las sesiones de reparación individuales especificando el siguiente mandato:

```
$ vsnap repair session show
```

La salida es similar a este ejemplo:

```
ID: 1
RELATIONSHIP: 72b19f6a9116a46aae6c642566906b31
PARTNER TYPE: vsnap
LOCAL SNAP: 1313
REMOTE SNAP: 311
STATUS: ACTIVE
SENT: 102.15GB
STARTED: 2019-11-01 15:51:18 UTC
ENDED: N/A
```

Vea una sesión para cada uno de los volúmenes de origen en la operación de reparación. La cantidad de datos que se envían para cada volumen muestra el aumento de los valores incrementales hasta que se completa el proceso. El mensaje final indica el número de volúmenes cuyas instantáneas se restaurarán mediante la siguiente operación de réplica, tal como se muestra en este ejemplo:

```
Se han creado 0 volúmenes. Hay 3 volúmenes de réplica cuyas instantáneas se restaurarán en
la próxima réplica.
```

- Para las instantáneas que no se han restaurado y que indican un estado FAILED, vuelva a enviar el proceso de reparación especificando el siguiente mandato:

```
$ vsnap repair create --async --retry
```

- Cuando el proceso de reparación informa de un estado COMPLETED, puede reanudar las operaciones normales para el servidor vSnap sacándolo de la modalidad de mantenimiento. Para reanudar el procesamiento normal, escriba el mandato siguiente:

```
$ vsnap system maintenance complete
```

- Opcional: Para ver los volúmenes totales y el número de instantáneas que se han restaurado durante la operación de reparación, ejecute el mandato show para el servidor vSnap.

La salida incluye la siguiente información:

- **TOTAL VOLUMES** lista el número total de volúmenes que se han inspeccionado durante la operación de reparación. Esta lista incluye los volúmenes de origen (volúmenes primarios) donde se ha restaurado la copia de seguridad de punto de recuperación más reciente y los volúmenes de destino (volúmenes de réplica) que se vuelven a llenar durante las próximas operaciones de réplica tal como se ha planificado en los SLA.
  - **SNAPSHOTS RESTORED** lista el número de volúmenes de origen que se han restaurado.
17. Elimine las claves de host de SSH guardadas del servidor vSnap de origen reparado y de los servidores vSnap de destino.

Ejecute los mandatos siguientes en los servidores vSnap de origen y de destino:

```
$ sudo rm -f /home/vsnap/.ssh/known_hosts
```

```
$ sudo rm -f /root/.ssh/known_hosts
```

La eliminación de las claves SSH garantiza que las transferencias de réplica posteriores no generan errores que resulten de la clave de host modificada del servidor vSnap reparado.

18. Reinicie el servicio de vSnap en el servidor sustituido escribiendo el mandato siguiente:

```
$ sudo systemctl restart vsnap
```

19. Haga clic en **Configuración del sistema > Almacenamiento de copias de seguridad > Disco** para verificar que el servidor vSnap nuevo se ha registrado correctamente, de la siguiente manera:
- Si el nuevo servidor vSnap utiliza el mismo nombre de host o dirección IP para el registro, no es necesario ningún cambio.
  - Si el nuevo servidor vSnap utiliza un nombre de host o una dirección IP distintos para el registro, debe actualizar el registro seleccionando el icono de lápiz.
20. Para eliminar los puntos de recuperación que ya no están disponibles en el servidor vSnap de origen, inicie un trabajo de mantenimiento desde la interfaz de usuario de IBM Spectrum Protect Plus. Siga las instrucciones aquí para hacerlo, [Creación de trabajos y planificaciones de trabajos](#).

**Consejo:** Es posible que vea mensajes informativos similares al ejemplo siguiente:

```
CTGGA1843 storage snapshot spp_1005_2102_2_16de41fcbc3 not found on live Storage2101
Snapshot Type vsnap
```

21. Para reanudar los trabajos que han fallado después de que el servidor vSnap pasara a no estar disponible, ejecute un trabajo de inventario del servidor de almacenamiento. Para obtener instrucciones, consulte [Creación de trabajos y planificaciones de trabajos](#).

## Resultados

Para los datos de copia de seguridad primaria que se almacenan en el servidor vSnap reparado, está disponible el punto de recuperación más reciente para los datos de copia de seguridad primario. Las copias de seguridad posteriores para el servidor vSnap reparado continúan enviando solo cambios incrementales desde la última copia de seguridad. Para los datos replicados almacenados en el servidor vSnap reparado, no hay datos replicados disponibles inmediatamente después de la reparación. Los trabajos de réplica posteriores del servidor vSnap asociado llenarán las copias de seguridad que se hayan creado en el servidor vSnap asociado después de que se haya completado el proceso de reparación. Si se intenta un trabajo de réplica en el servidor vSnap asociado antes de que se complete la copia de seguridad en el servidor vSnap asociado, se muestra un mensaje de advertencia que indica que no hay nuevas instantáneas desde la última copia de seguridad:

```
CTGGA0289 - Omisión del volumen <id_volumen> porque no hay nuevas instantáneas desde la última
copia de seguridad
```

Si el servidor vSnap reparado actuaba como un origen de copia en el almacenamiento de objetos o archivado, se debe ejecutar primero un trabajo de copia de seguridad en el servidor vSnap reparado antes

de que las operaciones de copia adicionales se realicen correctamente. La primera copia de datos en el almacenamiento de objetos será una copia completa.



## Capítulo 5. Instalación de Soporte de copia de seguridad de Kubernetes

Para proteger volúmenes pertinentes en contenedores, el administrador de copia de seguridad debe instalar y configurar Soporte de copia de seguridad de Kubernetes en el entorno de Kubernetes.

### Requisitos previos para Soporte de copia de seguridad de Kubernetes

Antes de poder instalar Soporte de copia de seguridad de Kubernetes, asegúrese de que se cumplen todos los requisitos previos y los requisitos del sistema.

Para ver los requisitos del sistema del Soporte de copia de seguridad de Kubernetes, consulte [“Requisitos de Soporte de copia de seguridad de Kubernetes”](#) en la página 56.

A continuación, para cumplir los requisitos previos para Soporte de copia de seguridad de Kubernetes, complete las siguientes acciones en el entorno de Kubernetes:

- [“Habilitación de la característica VolumeSnapshotDataSource”](#) en la página 153
- [“Verificar si Metrics Server está en ejecución”](#) en la página 154
- [“Definición de la relación de la aplicación y la reclamación de volumen persistente”](#) en la página 155
- [“Creación de un secreto de extracción de imagen para su uso con un registro externo”](#) en la página 155

#### Habilitación de la característica VolumeSnapshotDataSource

Solo para Kubernetes 1.16: debe habilitar la característica alfa **VolumeSnapshotDataSource** para dar soporte a las operaciones de copia de seguridad de copia y restauración de instantánea.

Para obtener más información sobre las características alfa, consulte [Puertas de características](#).

Para habilitar la característica alfa **VolumeSnapshotDataSource**, debe parchear el planificador, el controlador y el servidor de API de Kubernetes de la siguiente manera:

1. Utilizando el mandato **sudo**, edite los siguientes archivos YAML:

```
/etc/kubernetes/manifests/kube-apiserver.yaml  
/etc/kubernetes/manifests/kube-controller-manager.yaml  
/etc/kubernetes/manifests/kube-scheduler.yaml
```

2. En cada archivo YAML, añada la siguiente sentencia en la sección de mandatos:

```
- --feature-gates=VolumeSnapshotDataSource=true
```

**Importante:** Asegúrese de que edita los archivos YAML directamente y no cree copias de seguridad de estos archivos en el mismo directorio. La presencia de copias de seguridad en el directorio `/etc/kubernetes/manifests` puede negar los cambios que haya realizado para habilitar la puerta de la característica **VolumeSnapshotDataSource**.

Es posible que tenga que esperar un minuto o dos para que Kubernetes detecte los cambios.

3. Verifique si la característica está habilitada emitiendo los mandatos siguientes:

```
ps aux | grep apiserver | grep feature-gates
```

```
ps aux | grep scheduler | grep feature-gates
```

```
ps aux | grep controller-manager | grep feature-gates
```

La salida de uno de estos mandatos es similar al ejemplo siguiente:

```

root      13121  7.4  2.5 518276 305424 ?          Ssl  Sep06 120:37 kube-apiserver --
authorization-mode=Node,RBAC --advertise-address=192.0.2.0
--allow-privileged=true --client-ca-file=/etc/kubernetes/pki/ca.crt --enable-admission-
plugins=NodeRestriction --enable-bootstrap-token-auth=true
--etcd-cafile=/etc/kubernetes/pki/etcd/ca.crt --etcd-certfile=/etc/kubernetes/pki/apiserver-
etcd-client.crt --etcd-keyfile=/etc/kubernetes/pki/apiserver-etcd-client.key
--etcd-servers=https://127.0.0.1:2379 --insecure-port=0 --kubectl-client-certificate=/etc/
kubernetes/pki/apiserver-kubectl-client.crt
--kubectl-client-key=/etc/kubernetes/pki/apiserver-kubectl-client.key --kubectl-preferred-
address-types=InternalIP,ExternalIP,Hostname
--proxy-client-cert-file=/etc/kubernetes/pki/front-proxy-client.crt --proxy-client-key-
file=/etc/kubernetes/pki/front-proxy-client.key
--requestheader-allowed-names=front-proxy-client --requestheader-client-ca-file=/etc/
kubernetes/pki/front-proxy-ca.crt
--requestheader-extra-headers-prefix=X-Remote-Extra- --requestheader-group-headers=X-Remote-
Group --requestheader-username-headers=X-Remote-User
--secure-port=6443 --service-account-key-file=/etc/kubernetes/pki/sa.pub --service-cluster-
ip-range=198.51.100.0/24 --tls-cert-file=/etc/kubernetes/pki/apiserver.crt
--tls-private-key-file=/etc/kubernetes/pki/apiserver.key --feature-
gates=VolumeSnapshotDataSource=true

```

## Verificar si Metrics Server está en ejecución

Opcional: para ayudar a optimizar el rendimiento del producto y la escalabilidad, asegúrese de que Kubernetes Metrics Server v0.3.5 o posterior está instalado y se está ejecutando correctamente en el clúster. El planificador de Soporte de copia de seguridad de Kubernetes utiliza Metrics Server para determinar los recursos que utilizan las instancias del transportador de datos.

Si Metrics Server no devuelve datos, el número de transportadores de datos utilizados para las operaciones de copia de seguridad es limitado, lo que puede afectar negativamente al rendimiento.

Para obtener instrucciones sobre el despliegue de Metrics Server, revise el archivo README.md en <https://github.com/kubernetes-sigs/metrics-server>. Para obtener información sobre Kubernetes Metrics Server, consulte [Interconexión de métricas de recursos](#).

Puede verificar que Metrics Server está instalado y devolviendo datos de métricas completando los pasos siguientes:

1. Verifique la instalación emitiendo el mandato siguiente:

```
kubectl get deploy,svc -n kube-system | egrep metrics-server
```

La salida es similar a la que se muestra en el ejemplo siguiente:

```

deployment.extensions/metrics-server 1/1 1 1 3d4h
service/metrics-server ClusterIP 198.51.100.0 <none> 443/TCP 3d4h

```

2. Verifique que Metrics Server está devolviendo datos para todos los nodos emitiendo el mandato siguiente:

```
kubectl get --raw "/apis/metrics.k8s.io/v1beta1/nodes"
```

La salida es similar a la que se muestra en el ejemplo siguiente:

```

{"kind": "NodeMetricsList", "apiVersion": "metrics.k8s.io/v1beta1", "metadata": {"selfLink": "/
apis/metrics.k8s.io/v1beta1/nodes"}, "items": [{"metadata":
{"name": "cirrus12", "selfLink": "/apis/metrics.k8s.io/v1beta1/nodes/cirrus12",
"creationTimestamp": "2019-08-08T23:59:49Z", "timestamp": "2019-08-08T23:59:08Z",
"window": "30s", "usage": {"cpu": "1738876098n", "memory": "8406880Ki"}}}]

```

**Consejo:** Es posible que el mandato falle con la salida vacía para la clave "items". Probablemente, el error se deba a la instalación de Metrics Server con un certificado firmado automáticamente. Para resolver este problema, instale Metrics Server con un certificado firmado correctamente reconocido por el clúster.



## Definición de la relación de la aplicación y la reclamación de volumen persistente

De forma opcional, puede enlazar las aplicaciones con estado con las reclamaciones de volumen persistente (PVC) utilizando una relación dependiente del propietario. Al definir esta relación, puede habilitar las acciones en cascada para las aplicaciones.

Por ejemplo, el escalado hacia arriba y el escalado hacia abajo de una aplicación puede provocar que las copias de seguridad planificadas de la PVC se detengan y se reanuden. De forma similar, la supresión de la aplicación provoca la supresión de la PVC, que a su vez desencadena la supresión de las copias de seguridad.

Después de que una aplicación empiece a utilizar una PVC para almacenar datos persistentes, puede volver a configurar la definición de PVC con la aplicación de propietario.

El ejemplo siguiente es un archivo de configuración de ejemplo para una PVC que muestra la relación dependiente del propietario entre una aplicación y un objeto PVC. El objeto PVC incluye los detalles del despliegue de propietario.

```
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: demo-pvc
  ownerReferences:
    - apiVersion: apps/v1beta1
      blockOwnerDeletion: true
      kind: Deployment
      name: Dept10-deployment
      uid: 3b760e89-7da5-11e9-8c5a-0050568ba59c
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi
  storageClassName: csi-rbd
```

## Creación de un secreto de extracción de imagen para su uso con un registro externo

Si tiene previsto extraer una imagen de un registro o repositorio de Docker externo, debe crear un secreto de extracción de imagen. Durante el despliegue, Kubernetes extrae los contenedores necesarios del registro externo y suministra los pods para Soporte de copia de seguridad de Kubernetes.

El secreto de extracción de imagen se utiliza para proporcionar las credenciales que necesita Kubernetes para extraer imágenes de Docker del registro externo.

El nombre del secreto de extracción de imagen que crea debe coincidir con el valor para el parámetro `PRODUCT_IMAGE_REGISTRY_SECRET_NAME` en el archivo de configuración de `baas_config.cfg`.

El secreto de extracción de imagen debe estar en cada espacio de nombres de los PVC que estarán protegidos por Soporte de copia de seguridad de Kubernetes.

Este procedimiento no es necesario si está utilizando un registro de Docker interno. Para un registro interno, especifique una serie vacía ("" ) para el parámetro `PRODUCT_IMAGE_REGISTRY_SECRET_NAME`.

**Consejo:** Si está instalando Soporte de copia de seguridad de Kubernetes desde IBM Helm Chart Repository e IBM Entitled Registry, consulte el archivo léame del producto en <https://github.com/IBM/charts/tree/master/entitled/ibm-spectrum-protect-plus-prod> para obtener instrucciones sobre cómo crear un secreto de extracción de imagen para su uso con IBM Helm Chart Repository e IBM Entitled Registry.

Antes de empezar:

- Asegúrese de que existe el espacio de nombres del producto `baas` emitiendo el mandato siguiente:

```
kubectl get namespace baas
```

- Si el espacio de nombres baas no existe, emita el mandato siguiente para crearlo:

```
kubectl create namespace baas
```

Para crear un secreto de extracción de imagen para el registro de Docker:

1. Emita el mandato siguiente para crear el secreto de extracción de imagen:

```
kubectl create secret docker-registry secret_name --namespace namespace_name --docker-server=registry_name --docker-username=docker_user or "token" --docker-password=password/token --docker-email=email
```

2. Determine los espacios de nombres de cualquier PVC de volumen persistente que desee proteger emitiendo el siguiente mandato:

```
kubectl get pvc --all-namespaces
```

3. Para cada PVC que desea proteger, copie el secreto al espacio de nombres de la PVC. Por ejemplo, para copiar el secreto baas-registry-secret que ha creado para el espacio de nombres baas al espacio de nombre namespace1, emita el mandato siguiente:

```
kubectl get secret "baas-registry-secret" --namespace="baas" --export -o yaml | kubectl apply --namespace="namespace1" -f -
```

## Instalación y despliegue de imágenes de Soporte de copia de seguridad de Kubernetes en el entorno de Kubernetes

Antes de poder hacer copia de seguridad y restaurar los volúmenes persistentes conectados a los contenedores en un entorno de clúster Kubernetes, debe instalar y desplegar imágenes de Soporte de copia de seguridad de Kubernetes.

### Antes de empezar

Puede instalar el soporte de copia de seguridad de Kubernetes utilizando uno de los métodos siguientes:

#### Descargando e instalando el paquete Helm desde IBM Helm Charts Repository e IBM Entitled Registry

El paquete Helm tiene un tamaño más pequeño y, por lo tanto, tarda menos tiempo en descargar. Es necesario acceso a Internet para extraer contenedores durante el tiempo de despliegue. Puede descargar el archivo de paquete Helm denominado `ibm-spectrum-protect-plus-prod-1.0.0.tgz` en <https://github.com/IBM/charts/tree/master/repo/entitled>.

Para obtener instrucciones sobre la instalación del diagrama de Helm, consulte el archivo léame del producto en <https://github.com/IBM/charts/tree/master/entitled/ibm-spectrum-protect-plus-prod>.

#### Descargando e instalando el paquete de producto de IBM Passport Advantage Online

El paquete de instalación de IBM Passport Advantage es un paquete más grande pero autocontenido. No se necesita acceso a Internet durante el tiempo de despliegue. En este tema se proporcionan instrucciones para descargar e instalar el paquete.

Complete las tareas siguientes para descargar el paquete de instalación desde IBM Passport Advantage:

- Asegúrese de que el entorno del sistema cumple los requisitos que se describen en [“Requisitos de Soporte de copia de seguridad de Kubernetes”](#) en la página 56 y [“Requisitos previos para Soporte de copia de seguridad de Kubernetes”](#) en la página 153.
- Descargue el archivo de instalación `SPP_V10.1.6_for_Containers.tar.gz` desde Passport Advantage® Online. Para obtener información sobre la descarga de archivos, consulte [Nota técnica 5693313](#).
- Valide el archivo descargado utilizando uno de los métodos siguientes:
  - Verifique la suma de comprobación MD5 del archivo de instalación 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.

- Verifique el archivo firmado asociado con el paquete de instalación emitiendo el mandato siguiente:

```
openssl dgst -sha256 -verify IBMSPSignCertificatePublic -signature ./SPP_V10.1.6_for_Containers.tar.gz.sig ./SPP_V10.1.6_for_Containers.tar.gz
```

### Restricciones:

- La retrotracción a una versión anterior de Soporte de copia de seguridad de Kubernetes no está soportada. En otras palabras, no puede utilizar Soporte de copia de seguridad de Kubernetes V10.1.5 para restaurar datos de los que Soporte de copia de seguridad de Kubernetes V10.1.6 hizo una copia de seguridad.
- No se admite la actualización del producto desde Soporte de copia de seguridad de Kubernetes V10.1.5.
- Debido a los cambios subyacentes en el objeto BaasReq, no puede utilizar Soporte de copia de seguridad de Kubernetes V10.1.6 de los que Soporte de copia de seguridad de Kubernetes V10.1.5 ha hecho copia de seguridad.

### Acerca de esta tarea

Durante el procedimiento de instalación y despliegue, debe actualizar el archivo de configuración `baas_config.cfg` con especificaciones para su entorno y, a continuación, ejecutar el script de instalación `baas_install.sh`. Cuando ejecuta el script de instalación, se llama automáticamente a un diagrama de Helm adecuado para desplegar Soporte de copia de seguridad de Kubernetes en el entorno.

### Procedimiento

Complete los pasos siguientes en la línea de mandatos del entorno de Kubernetes:

1. Inicie sesión en el clúster de destino como usuario con privilegios de `admin-admin`.
2. Desempaquete el paquete de instalación (`SPP_V10.1.6_for_Containers.tar.gz`) especificando el mandato siguiente:

```
tar -xvf SPP_V10.1.6_for_Containers.tar.gz
```

Este mandato extrae una carpeta denominada `installer`.

3. Vaya al directorio `installer` emitiendo el mandato siguiente:

```
cd installer
```

4. Ejecute el mandato siguiente para obtener el método CIDR (Classless Inter-Domain Routing) para el clúster. Los valores se utilizan en el Paso “6” en la página 158.

```
kubectl cluster-info dump | grep -m 1 cluster-cidr
```

El CIDR se proporciona en la salida con el formato siguiente:

```
--cluster-cidr=xxx.yyy.0.0/zz
```

**Consejo:** Si el mandato no devuelve el CIDR, cambie la expresión **grep** para buscar la combinación de "clúster" y "CIDR" y ejecute el mandato de nuevo.

El CIDR es similar al ejemplo siguiente:

```
198.51.0.0/24
```

5. Ejecute el mandato siguiente para obtener el clúster y la dirección IP y el puerto para el servidor de API de clúster. Los valores se utilizan en el Paso “6” en la página 158.

```
kubectl config view|awk '/cluster\:\/\/,server\:\/\/' | grep server\: | awk '{print $2}'
```

El resultado es un URL que se compone de una dirección IP y un número de puerto, tal como se muestra en el ejemplo siguiente:

https://192.0.2.0:6443

donde 192.0.2.0 es la dirección IP del servidor de API de clúster y 6443 es la dirección de puerto.

6. Edite el archivo `baas_config.cfg` con un editor de texto y modifique los parámetros de configuración proporcionando los valores adecuados para el entorno. Encierre los valores entre comillas como se muestra en el ejemplo siguiente.

```
BAAS_ADMIN="sppadmin"
```

La tabla siguiente contiene los parámetros que debe modificar:

Tabla 54. Especificaciones para el archivo de configuración <code>baas_config.cfg</code>	
Parámetro	Descripción
BAAS_ADMIN	ID de usuario del administrador de IBM Spectrum Protect Plus.
BAAS_PASSWORD	La contraseña de IBM Spectrum Protect Plus.  Para mayor seguridad, especifique una serie vacía (" "). Se le solicitará la contraseña al ejecutar el script de despliegue. Si debe especificar una contraseña en el archivo de configuración para despliegues de prueba automatizados, asegúrese de que el archivo esté almacenado en una ubicación segura.
CLUSTER_NAME	El nombre de clúster exclusivo que se utiliza para registrar el host de aplicación en el servidor de IBM Spectrum Protect Plus.
CLUSTER_CIDR	El CIDR para el clúster. Especifique el CIDR que se ha obtenido en el Paso "4" en la <a href="#">página 157</a> .
CLUSTER_API_SERVER_IP_ADDRESS	La dirección IP o el nombre de dominio completo (FQDN) para el servidor de API de clúster. Especifique la dirección IP o FQDN que se ha obtenido en el Paso "5" en la <a href="#">página 157</a> .
CLUSTER_API_SERVER_PORT	La dirección del puerto del servidor de API de clúster. Especifique la dirección del puerto que se ha obtenido en el Paso "5" en la <a href="#">página 157</a> .
LICENSE	<p>La licencia de producto para Soporte de copia de seguridad de Kubernetes. El archivo de licencia en inglés que se ubica en el directorio <code>installer/licenses/LA_</code> en que se incluye en el paquete de instalación. Las versiones de la licencia en otros idiomas se encuentran disponibles en <a href="#">Documentos de Información sobre Licencias</a>.</p> <p>Revise la información de la licencia y especifique <code>ACCEPTED</code> para aceptar la licencia durante la instalación sin que se le solicite.</p> <p>El valor predeterminado es <code>NOTACCEPTED</code>. Si no cambia el valor predeterminado, se le solicitará que acepte la licencia durante la instalación. De lo contrario, la instalación fallará.</p>

Tabla 54. Especificaciones para el archivo de configuración *baas\_config.cfg* (continuación)

Parámetro	Descripción
SPP_AGENT_SERVICE_NODEPORT	<p>El puerto SSH para la conexión desde IBM Spectrum Protect Plus del servicio de contenedor de agentes de Soporte de copia de seguridad de Kubernetes.</p> <p>Si no especifica un valor para este puerto, el servicio NodePort de Kubernetes asigna un puerto aleatorio en el rango NodePort. El rango predeterminado es 30000-32767.</p> <p>Si especifica un valor para este puerto, utilice un número de puerto dentro del rango de NodePort establecido por el administrador de Kubernetes. Asegúrese de que el clúster no esté utilizando el puerto. Si el puerto ya está en uso, el proceso de instalación falla con un error que muestra qué NodePorts ya están en uso.</p>
SPP_IP_ADDRESSES	La dirección IP del servidor de IBM Spectrum Protect Plus o FQDN.
PRODUCT_IMAGE_REGISTRY	La dirección de registro de Docker y el puerto que aloja los contenedores. Especifique la dirección en el formato <i>ip_address:port</i> .
PRODUCT_IMAGE_REGISTRY_NAMESPACE	El espacio de nombres del registro de Docker que aloja los contenedores.
PRODUCT_IMAGE_REGISTRY_SECRET_NAME	<p>El nombre del secreto de extracción de imagen de Kubernetes que contiene las credenciales para el registro. El secreto debe estar en el espacio de nombres especificado por el parámetro <code>PRODUCT_IMAGE_REGISTRY_NAMESPACE</code>.</p> <p>Si está utilizando un registro interno, especifique una serie vacía, ("").</p> <p>Para que se ejecute el contenedor de transportador de datos, el secreto de extracción de imagen debe estar en cada espacio de nombres de cada reclamación de volumen persistente (PVC) para que se realice la copia de seguridad y restauración.</p> <p>Para obtener instrucciones sobre la creación del secreto de extracción de imagen, consulte <a href="#">“Creación de un secreto de extracción de imagen para su uso con un registro externo”</a> en la página 155.</p>
PRODUCT_LOGLEVEL	<p>Los niveles de rastreo para la resolución de problemas con los componentes del gestor de transacción, controlador y planificador de Soporte de copia de seguridad de Kubernetes. Están disponibles los siguientes niveles de rastreo: INFO, WARNING, DEBUG o ERROR.</p> <p>Valor predeterminado: INFO</p>

#### Restricciones:

- Los siguientes parámetros y valores están reservados para Soporte de copia de seguridad de Kubernetes. Manténgalos tal cual.

```
PRODUCT_NAMESPACE="baas"
OPERATOR_NAMESPACE="default"
PRODUCT_TARGET_PLATFORM="K8S"
```

- El valor de `SPP_PORT` especifica el puerto para la interfaz de usuario de IBM Spectrum Protect Plus. No cambie el valor predeterminado de 443.
- Soporte de copia de seguridad de Kubernetes solo está disponible el inglés en IBM Spectrum Protect Plus V10.1.6. Por este motivo, no cambie el valor de `PRODUCT_LOCALIZATION="en_US"`.

Las especificaciones se insertan automáticamente en la ConfigMap (baas - configmap) durante el despliegue.

7. Inicie la instalación y el despliegue emitiendo el mandato siguiente.

```
./baas_install.sh -i
```

Cuando se le solicite, especifique **sí** para continuar.

8. Durante el proceso de instalación, se le solicita la siguiente información:

- Introduzca el ID de administrador y contraseña de IBM Spectrum Protect Plus cuando se le solicite.
- Cuando se le solicite que verifique la conectividad con el servidor IBM Spectrum Protect Plus, escriba **yes** para continuar.

Si especifica **no**, la instalación continúa sin verificar la conectividad con el servidor IBM Spectrum Protect Plus.

Si especifica **yes** y la prueba de conectividad falla, la instalación termina con el siguiente mensaje de error:

```
ERROR: no se ha podido conectar con el servidor de IBM Spectrum Protect Plus con las credenciales proporcionadas.
```

En función de su entorno, el paquete puede tardar varios minutos en cargarse y desplegarse.

9. Para verificar que los componentes de Soporte de copia de seguridad de Kubernetes estén correctamente instalados, emita el siguiente mandato:

```
./baas_install.sh -s
```

Si la instalación falla, los componentes que faltan se listan en la sección **MISSING** de la salida.

**Consejo:** También puede comprobar el estado de la instalación con el mandato **./helm status baas**.

## Resultados

Cuando todos los pods están en ejecución, el despliegue se ha completado. Para verificar que todos los pods están en estado **Running** y que no faltan componentes, emita el mandato siguiente:

```
kubectl get pods -n baas
```

O

```
kubectl describe pod pod_name -n baas
```

La salida es similar a la que se muestra en el ejemplo siguiente:

```
kubcectl get pods -n baas
NAME                                READY   STATUS    RESTARTS   AGE
baas-controller-768869468c-crt4d4   1/1     Running   0           4m24s
baas-kafka-68d7ff8455-m96cc         1/1     Running   0           4m24s
baas-scheduler-656978d87f-thqv2     1/1     Running   1           4m24s
baas-spp-agent-cdb784466-v9tnz      1/1     Running   0           4m24s
baas-transaction-manager-657db7bb8b-6dgqb 1/1     Running   2           4m24s
-----
Todos los pods están en ejecución.
Todos los recursos están instalado correctamente.
La instalación se ha completado.
El release de producto >>baas<< versión 10.1.6 se ha instalado en el espacio de nombres>>baas<<
el miér 20 de mayo 17:58:02 MST 2020.
Script baas_install.sh finished at Wed May 20 17:58:02 MST 2020. Se ha grabado un registro de
esta transacción en /tmp
/baas_installation.sh_20200520-175605.log .
```

Si el contenedor del transportador de datos no está listado en la salida, el contenedor del transportador de datos se despliega en el tiempo de ejecución.

Puede mostrar los servicios de Soporte de copia de seguridad de Kubernetes configurados emitiendo el mandato siguiente:

```
kubectl get services -n baas
```

La salida es similar a la que se muestra en el ejemplo siguiente:

NAME	TYPE	CLUSTER-IP	EXTERNAL-IP	PORT(S)	AGE
baas-kafka-svc	ClusterIP	10.110.116.210	<none>	9092/TCP, 2181/TCP	4m27s
baas-scheduler	ClusterIP	10.96.38.170	<none>	8000/TCP	4m27s
baas-spp-agent	NodePort	10.110.164.151	<none>	22:30412/TCP	4m27s
baas-transaction-manager	ClusterIP	10.108.42.194	<none>	5000/TCP	4m27s

El servicio `baas-datamover` se despliega en el tiempo de ejecución con el tipo `NodePort` en lugar del rango de `ClusterIP` con el protocolo TCP.

Puede mostrar las políticas de red de Soporte de copia de seguridad de Kubernetes que se despliegan emitiendo el mandato siguiente:

```
kubectl get networkpolicies -n baas
```

La salida es similar a la que se muestra en el ejemplo siguiente:

NAME	POD
baas-ctl-networkpolicy	app.kubernetes.io/component=controller,app.kubernetes.io/name=baas,app.kubernetes.io/version=10.1.6
baas-kafka	app.kubernetes.io/component=kafka,app.kubernetes.io/name=baas,app.kubernetes.io/version=10.1.6
baas-scheduler	app.kubernetes.io/component=scheduler,app.kubernetes.io/name=baas,app.kubernetes.io/version=10.1.6
baas-spp-agent	app.kubernetes.io/component=spp-agent,app.kubernetes.io/name=baas,app.kubernetes.io/version=10.1.6
baas-transaction-manager	app.kubernetes.io/component=transaction-manager,app.kubernetes.io/name=baas,app.kubernetes.io/version=10.1.6

La política de red para el transportador de datos se despliega en el tiempo de ejecución con el selector de pod `app.kubernetes.io/name=baas,app.kubernetes.io/component=datamover,version=10.1.6`.

### Qué hacer a continuación

Una vez que se ha completado el despliegue, el host de aplicación para el contenedor de Soporte de copia de seguridad de Kubernetes se registra automáticamente al iniciarse el host de clúster en Kubernetes. Sin embargo, si el registro automático no se ha realizado correctamente, puede registrar el clúster manualmente utilizando la interfaz de usuario de IBM Spectrum Protect Plus. Para obtener instrucciones, consulte [“Registro de un clúster Kubernetes”](#) en la página 335.

Si desea actualizar la configuración existente o actualizar la instalación existente de Soporte de copia de seguridad de Kubernetes, modifique los parámetros en el archivo `baas_config.cfg` según sea necesario para el entorno y emita el siguiente mandato:

```
./baas_install.sh -u
```

### Conceptos relacionados

[“Resolución de problemas de Soporte de copia de seguridad de Kubernetes”](#) en la página 550

Para ayudar a resolver problemas con Soporte de copia de seguridad de Kubernetes, puede recopilar archivos de registro de depuración y ver los registros de rastreo. También puede seguir procedimientos para diagnosticar problemas.

### Tareas relacionadas

[“Establecimiento del nivel de rastreo de los archivos de registro”](#) en la página 551

Puede establecer el nivel de rastreo de los archivos de registro locales para ayudarle a resolver los problemas que puede encontrarse en Soporte de copia de seguridad de Kubernetes.

## Desinstalación de Soporte de copia de seguridad de Kubernetes

Puede desinstalar completamente Soporte de copia de seguridad de Kubernetes para que todos los componente, incluidas todas las configuraciones y copias de seguridad, se eliminen del entorno de Kubernetes.

### Antes de empezar

Lleve a cabo las acciones siguientes antes de iniciar la desinstalación:

- Detenga todas las copias de seguridad planificadas. Para obtener instrucciones, consulte [Interrupción de las copias de seguridad de SLA para una PVC o Modificación de parámetros en un archivo YAML](#).
- Espere a que finalicen todos los trabajos de copia de seguridad y restauración en ejecución.

### Procedimiento

Para desinstalar completamente Soporte de copia de seguridad de Kubernetes del clúster en el que ha iniciado sesión, complete los pasos siguientes en la línea de mandatos:

1. Destruir todas las copias de seguridad de instantánea y de copia con una solicitud **destroy**. Para obtener instrucciones, consulte [“Supresión de copias de seguridad de contenedor” en la página 366](#).
2. Suprima las reclamaciones de volumen persistente (PVC) que se han utilizado para copias de seguridad de copia.

**Consejo:** Puede buscar los nombres de los PVC a los que se ha hecho copia de seguridad.

3. Suprima la definición de recurso personalizado de baas (CRD) emitiendo el siguiente mandato:

```
kubect1 delete crd baasreqs.baas.io
```

Este mandato también suprime todos los objetos de solicitud BaasReq.

4. Desinstale Soporte de copia de seguridad de Kubernetes emitiendo el siguiente mandato desde el directorio `installer`:

```
./baas_install.sh -d
```


Cuando se le solicite, especifique **sí** para continuar.

Este mandato elimina todos los pods de transportador de datos, despliegues y políticas de red. También se elimina el secreto de Kubernetes para Soporte de copia de seguridad de Kubernetes.


5. Opcional: Para verificar el progreso de la desinstalación, escriba el mandato siguiente:

```
kubect1 get pod -n baas
```

6. Anule el registro del clúster Kubernetes utilizando la interfaz de usuario de IBM Spectrum Protect Plus:

- a) En el panel de navegación, haga clic en **Gestionar protección > Contenedores > Kubernetes**.
- b) En la página **Kubernetes**, haga clic en **Gestionar clústeres**.
- c) En la lista de direcciones de host, haga clic en el icono de supresión  junto al clúster para el que desea anular el registro.
- d) En la ventana **Confirmar**, escriba el código de confirmación visualizado y haga clic en **Anular registro**.

7. Elimine la identidad de cuenta que se utiliza para registrar el clúster Kubernetes:

- a) En el panel de navegación, haga clic en **Cuentas > Identidad**.
- b) Haga clic en el icono de supresión  asociado con el clúster.
- c) Pulse **Sí** para suprimir la identidad.

8. Inhabilite la característica **VolumeSnapshotDataSource** si ya no la necesita.



9. Suprima las políticas de acuerdo de nivel de servicio (SLA) y otras personalizaciones suprimiendo el espacio de nombres baas. Emita el mandato siguiente:

```
kubect1 delete namespace baas
```

10. Si ha creado manualmente un secreto de extracción de imágenes para utilizarlo con un registro externo, elimine el secreto con el mandato **kubect1 delete secret** en todos los espacios de nombres en los que existía el secreto.
11. Opcional: Revise la información de instalación y configuración y revierta los pasos de requisitos previos.

### Qué hacer a continuación

Si Soporte de copia de seguridad de Kubernetes no se ha desinstalado de forma limpia, consulte "Soporte de copia de seguridad de Kubernetes no se ha desinstalado de forma limpia" en ["Consulta rápida de resolución de problemas"](#) en la página 554.



## Capítulo 6. 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 copia y 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 [“Storyboard de despliegue para IBM Spectrum Protect Plus”](#) en la [página 1](#) 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* completa las tareas de copia de seguridad y restauración de recursos. No obstante, un solo administrador puede ser responsable de todas las tareas del entorno.

Acción	Propietario	Descripción
<a href="#">Iniciar IBM Spectrum Protect Plus</a>	Administrador de infraestructuras y administrador de aplicaciones	<p>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.</p> <p>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.</p>

Acción	Propietario	Descripción
<a href="#">“Sitios de gestión” en la página 168</a>	Administrador de infraestructuras	<p>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.</p> <p>Los sitios predeterminados se denominan Primario y Secundario, pero también puede crearse y asignarse un sitio personalizado cuando se añade el servidor vSnap.</p> <p>Antes de continuar con las siguientes acciones, revise los sitios disponibles y determine si desea añadir nuevos sitios o modificar los existentes.</p>
<a href="#">Crear políticas de copia de seguridad</a>	Administrador de infraestructuras	<p>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 copiar datos de copia de seguridad en el almacenamiento secundario de copias de seguridad para la protección a más largo plazo.</p> <p>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.</p> <p>Las políticas de copia de seguridad se denominan políticas de SLA en IBM Spectrum Protect Plus.</p>
<a href="#">Crear una cuenta de usuario para el administrador de aplicaciones</a>	Administrador de infraestructuras	<p>Las cuentas de usuario determinan los recursos y las funciones que están disponibles para el usuario.</p>

Acción	Propietario	Descripción
<a href="#">Añadir recursos para proteger</a>	Administrador de aplicaciones	Los recursos son entidades que desea proteger. Después de registrar un recurso, se captura un inventario del recurso y se añade al inventario de IBM Spectrum Protect Plus.
<a href="#">Añadir recursos a una definición de trabajo</a>	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.
<a href="#">Iniciar un trabajo de copia de seguridad</a>	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.
<a href="#">Ejecutar un informe</a>	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-SysXyz`. 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.

Se imponen las reglas siguientes al crear una contraseña nueva:

- La longitud mínima aceptable de la contraseña es de 15 caracteres.
- Debe haber ocho caracteres en la nueva contraseña que no estén presentes en la contraseña anterior.
- La nueva contraseña debe contener al menos un carácter de cada una de las clases (números, letras en mayúscula, letras en minúscula y otros).
- El número máximo de caracteres consecutivos idénticos permitidos en la nueva contraseña es de tres caracteres.
- El número máximo de la clase de caracteres consecutivos idénticos permitidos en la nueva contraseña es de cuatro caracteres.
- 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

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.	<ol style="list-style-type: none"><li>a. Pulse <b>Añadir sitio</b>.</li><li>b. Especifique un nombre de sitio.</li><li>c. Opcional: seleccione <b>Habilitar regulador</b> para gestionar el rendimiento de las operaciones de copia y réplica de sitios tal como se describe en <a href="#">“Adición de un sitio” en la página 213</a>.</li><li>d. Pulse <b>Guardar</b>.</li></ol>

Acción	Procedimiento
Edite un sitio.	<p>a. Pulse <b>Editar sitio</b>.</p> <p>b. Pulse el icono de edición  que está asociado a un sitio.</p> <p>c. Opcional: seleccione <b>Habilitar regulador</b> para gestionar el rendimiento de las operaciones de copia y réplica de sitios tal como se describe en <a href="#">“Edición de un sitio” en la página 214</a>.</p> <p>d. Pulse <b>Guardar</b>.</p>

### Conceptos relacionados

[“Componentes del producto” en la página 6](#)

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 213](#)

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

IBM Spectrum Protect Plus incluye políticas de SLA como se describe en [Capítulo 9, “Gestión de políticas de SLA para operaciones de seguridad”](#), en la página 241. Puede utilizar políticas predeterminada tal como están o bien modificarlas. También puede crear políticas de SLA personalizadas.

Con fines de ejemplo, los pasos siguientes muestran cómo crear una política de SLA para VMware. Esta tarea no incluye instrucciones para habilitar la réplica para servidores vSnap o para copiar datos en el almacenamiento de copia de seguridad secundario, que son características opcionales. Para obtener información sobre cómo configurar estas características en la política de SLA, consulte [“Creación de una política de SLA para hipervisores, bases de datos y sistemas de archivos” en la página 244](#).

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, haga clic en **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. Haga clic en **VMware, Hyper-V, Exchange, Office365, SQL, Oracle, Db2, MongoDB y sistemas de archivos de Windows**.
5. En la sección **Política de copia de seguridad**, 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 que se crean sin una planificación se pueden ejecutar bajo demanda.

### **Frecuencia**

**Restricción:** Los días de la semana para la opción **Semanas** está disponible solo si instala el arreglo temporal de IBM Spectrum Protect Plus 10.1.6 eFix2 o posterior.

Escriba una frecuencia para las operaciones de copia de seguridad. Elija entre **Minutos, Horas, Días, Semanas, Meses** o **Años**. Cuando se selecciona **Semanas**, puede seleccionar uno o más días de la semana. La **Hora de inicio** se aplicará a los días seleccionados de la semana.

### **Hora de inicio**

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

El huso horario se rellena automáticamente con los valores del navegador. Para actualizar el huso horario, haga clic en el campo y seleccione una región y ciudad de la lista, por ejemplo: **Europa/Dublín**. También puede hacer clic en el campo y especificar una región o ciudad en el campo **Buscar** y seleccionar un elemento de los resultados coincidentes.

### **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.

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:



## Policy Overview

### New SLA Policy

Name

☒ VMware, Hyper-V, Exchange, Office365, SQL, Oracle, DB2, MongoDB, Catalog, and Windows File Systems

☐ Kubernetes

☐ Amazon EC2

#### Backup Policy

Retention

☐ Disable Schedule

Frequency

Start Time

Target Site

☐ Only use encrypted disk storage.

#### Replication Policy

☐ Backup Storage Replication

Figura 12. Creación de una política de SLA

6. 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 176.

### Conceptos relacionados

[“Replicar datos de almacenamiento de copia de seguridad”](#) en la página 11

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.

[“Copiar instantáneas en almacenamiento de copias de seguridad secundario”](#) en la página 12

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 copiar instantáneas desde un servidor vSnap en un almacenamiento de copias de seguridad secundario.

[“Gestión de políticas de SLA para operaciones de seguridad”](#) en la página 241

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 para replicar o copiar datos de 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 recursos que se encuentran en su 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 543.

Para crear roles de usuario y grupos de recursos personalizados, consulte [“Creación de un grupo de recursos”](#) en la página 534 y [“Creación de un rol”](#) en la página 539

### 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**.

User

### Add User - User Information and Role

Select the type of user or group you want to add. Individual new user

Username   
Username must not be 'root', 'admin' or 'test'.

Password  [Show](#)  
Password must contain at least 8 characters.

#### ASSIGN ROLE

- ☐ Application Admin
- ☐ Backup Only
- ☐ Restore Only
- ☐ SYSADMIN
- ☐ Self Service
- ☒ VM Admin

#### PERMISSION GROUPS

- [Certificate](#)
- [Cloud](#)

[Cancel](#) [Continue >](#)

Figura 13. Creación de una cuenta de usuario y asignación de un rol

- Pulse **Continuar**.
- 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**.

The screenshot shows the 'Add User - Assign Resources' window. On the left, the user 'vmadmin' is listed with the role 'VM Administrator'. The 'Selected Resources' section on the right shows 'All Resources' with a red minus icon. Below this, there are two checkboxes: 'All Resources' (checked) and 'Hypervisor All Resource Group' (unchecked). An 'Add resources' button is present. At the bottom, there are 'Cancel', '< Back to user role', and 'Create user' buttons.

Figura 14. 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 533](#)

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 entidades 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 tipo de recurso en las secciones siguientes:

- [Capítulo 10, “Protección de sistemas virtualizados”, en la página 257](#)
- [Capítulo 11, “Protección de sistemas de archivos”, en la página 309](#)
- [Capítulo 12, “Protección de contenedores”, en la página 329](#)
- [Capítulo 13, “Protección de datos en sistemas en nube”, en la página 369](#)
- [Capítulo 14, “Protección de bases de datos”, en la página 375](#)

## Procedimiento

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

1. En el panel de navegación, pulse **Gestionar protección > Sistemas virtualizados > 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 15. 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.

### Procedimiento

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

1. En el panel de navegación, pulse **Gestionar protección > Sistemas virtualizados > 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:

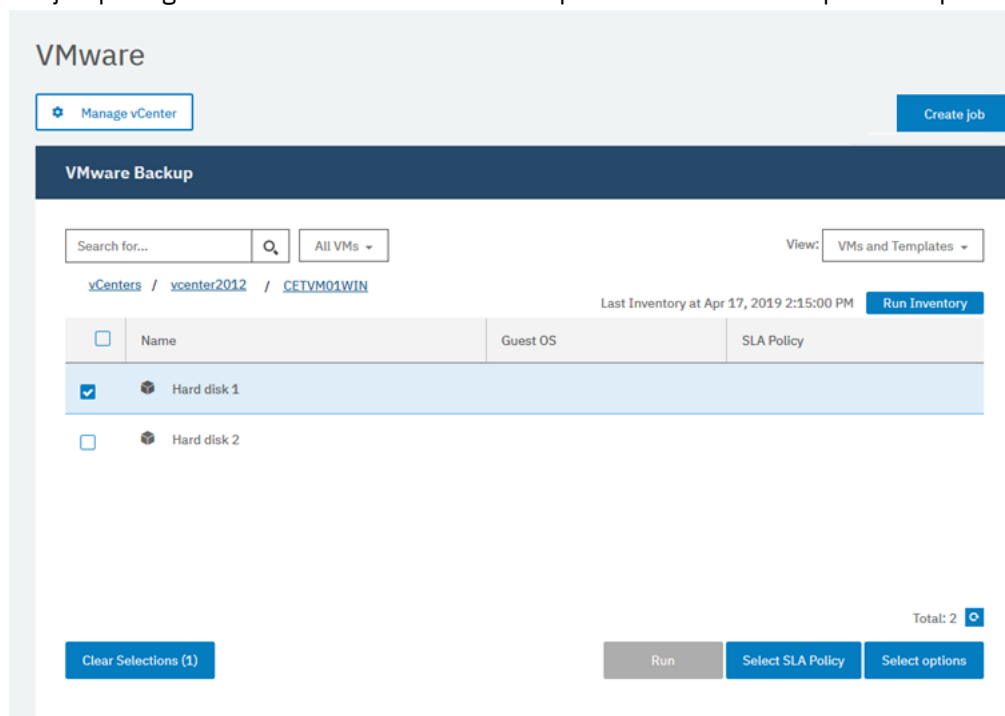


Figura 16. Selección de recursos para copia de seguridad

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:

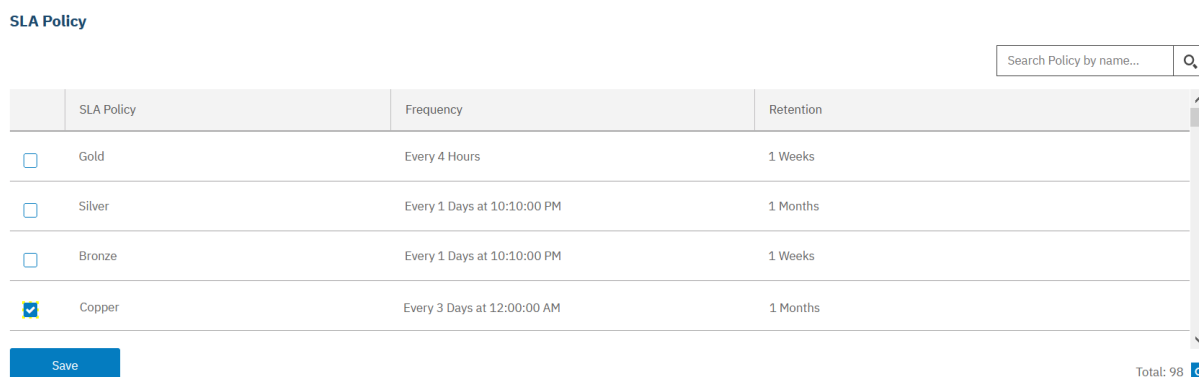


Figura 17. Selección de una política de SLA

4. Para crear la definición de trabajo utilizando las opciones predeterminadas, pulse **Guardar**.  
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. Para este trabajo de ejemplo, se crea el nombre vmware\_Copper.
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 262.
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 266](#).

## 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 178](#).

## Conceptos relacionados

[“Protección de IBM Spectrum Protect Plus”](#) en la [página 505](#)

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 y la información de trabajo en un servidor vSnap definido en la política de SLA asociada.

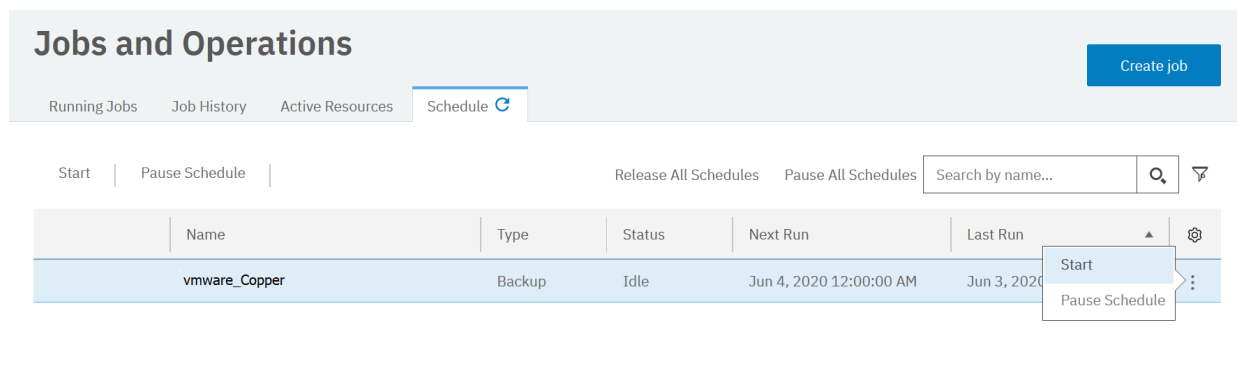
## Iniciar un trabajo de copia de seguridad

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 la acción **Iniciar** como se muestra en el ejemplo siguiente:



*Figura 18. 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

“Gestión de trabajos y operaciones” en la página 509

Puede gestionar y supervisar trabajos en la ventana **Trabajos y operaciones**. También puede configurar scripts para que se ejecuten antes o después de los trabajos.

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. Pulse la pestaña **Informes**.












































Reports			
Reports		Custom Reports	
		Filter by category: All	
	Name (job title)	Category	Schedule
  +	Configuration	System	
  +	Container Persistent Volume Backup History	Protection	
  +	Container Persistent Volume Backup Utilization	Backup Storage Utilization	
  +	Container SLARPO Compliance DisplayName	Protection	
  +	Database Backup History	Protection	
  +	Database Backup Utilization	Backup Storage Utilization	
  +	Database SLA Policy RPO Compliance	Protection	
  +	Job	System	
  +	License	System	
  +	Protected and Unprotected Container Persistent Volumes	Protection	
  +	Protected and Unprotected Databases	Protection	
  +	Protected and Unprotected VMs	Protection	
  +	VM Backup History	Protection	
  +	VM Backup Utilization	Backup Storage Utilization	
  +	VM Datastores	VM Environment	
  +	VM LUNs	VM Environment	
  +	VM SLA Policy RPO Compliance	Protection	
  +	VM Snapshot Sprawl	VM Environment	
  +	VM Sprawl	VM Environment	
  +	VM Storage	VM Environment	
  +	vSnap Storage Utilization	Backup Storage Utilization	

Figura 19. Selección de un informe para ejecutar

- 3. Ejecute el informe haciendo clic en el icono **Ejecutar informe** () junto al informe.
  - Para ejecutar el informe con parámetros personalizados, establezca los parámetros en la ventana **Ejecutar informe** y haga clic en **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 521

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 7. Actualización de componentes de IBM Spectrum Protect Plus

Puede actualizar el dispositivo virtual de IBM Spectrum Protect Plus o 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 5693313](#).

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 505.
- 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.

---

### Gestión de actualizaciones

Un entorno de IBM Spectrum Protect Plus incluye el servidor IBM Spectrum Protect Plus y uno o más servidores vSnap y, opcionalmente, uno o más proxies VADP. Para garantizar que IBM Spectrum Protect Plus funciona con normalidad, todos los componentes del entorno deben estar en el mismo nivel de versión. Revise las instrucciones para planificar y completar cuidadosamente el proceso de actualización.

#### Antes de empezar

Complete los pasos siguientes:

1. Planifique un periodo de mantenimiento y verificación para el proceso de actualización. Puede estimar el tiempo necesario en función del número de componentes del entorno que se deben actualizar.

El proceso de actualización de un entorno de IBM Spectrum Protect Plus depende del número de componentes del entorno y de las velocidades de red de las ubicaciones implicadas. La tabla siguiente contiene los tres componentes de IBM Spectrum Protect Plus y el tiempo promedio, en minutos, que tarda en aplicar la actualización y reiniciar correctamente el sistema.

Tabla 55. Tiempos de actualización y componentes de IBM Spectrum Protect Plus

Componente	Tiempo para actualizar	Tiempo para reiniciar	Total
Servidor de IBM Spectrum Protect Plus	10	15	25
Servidor vSnap	15	10 - 30	25 - 45
Servidor proxy VADP	15	No es necesario.	15

2. Recopile información de la versión para los componentes del entorno y determine los niveles de versión para el proceso de actualización. Determine si los servidores vSnap deben actualizarse como parte del proceso de actualización.

3. Ajuste las horas de inicio de los trabajos de inventario o de mantenimiento planificados para que se ejecuten después de que concluya el periodo de mantenimiento y verificación.

4. Finalice los trabajos de restauración o reutilización, incluidos los trabajos de restauración del almacenamiento de objetos. Si es necesario, planifique estos trabajos después de que se haya completado el periodo de mantenimiento y verificación.

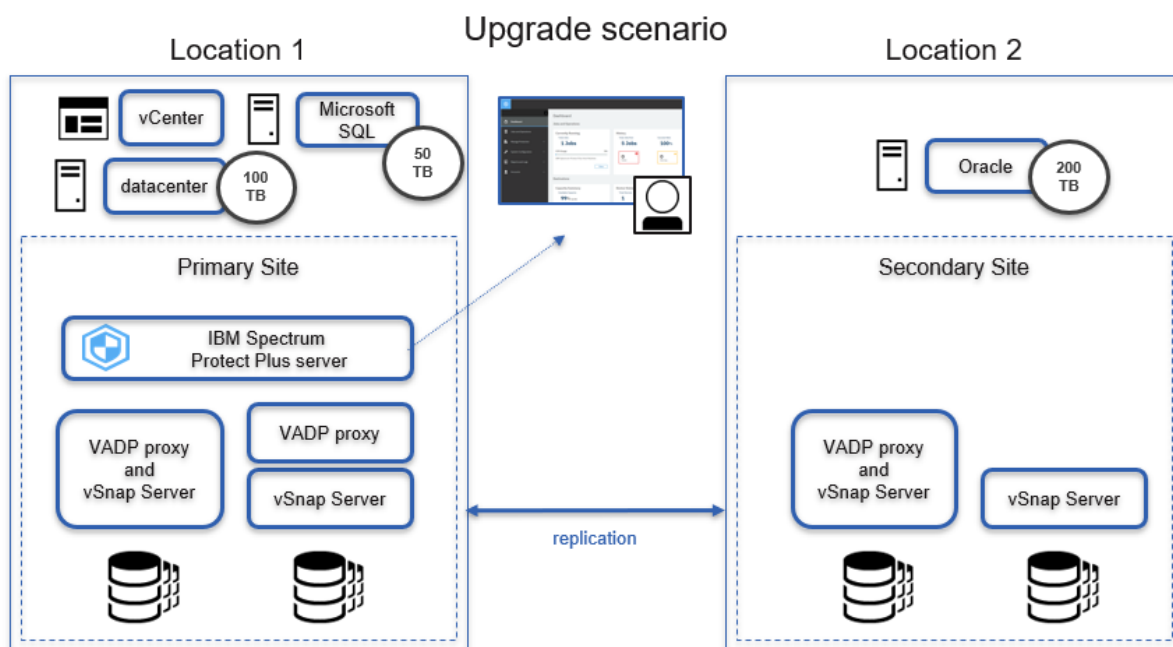
5. Pause los trabajos restantes para que no se ejecuten durante el periodo de mantenimiento y verificación.

#### Acerca de esta tarea

El procedimiento se basa en un entorno de ejemplo, que incluye los siguientes componentes:

- 1 servidor de IBM Spectrum Protect Plus
- 2 servidores incorporados y 2 servidores autónomos, con los 4 servidores teniendo relaciones de duplicación
- 2 proxies VADP co-instalados con dos de los servidores vSnap
- 1 proxy VADP autónomo

En la figura siguiente, los componentes se muestran en sus sitios respectivos, Ubicación 1 y Ubicación 2:



## Procedimiento

1. Para preparar el entorno del sistema para el proceso de actualización, complete los pasos siguientes:
  - a) En el panel de navegación, pulse **Gestionar protección > Visión general de políticas** y, a continuación, haga clic en el botón **Añadir política de SLA**.
  - b) En el panel **Nueva política de SLA**, especifique un nombre de política y pulse el botón de selección que incluye la palabra **Catálogo**. Pulse **Guardar**.
  - c) Seleccione la casilla de verificación **Inhabilitar planificación** y especifique el periodo de retención adecuado. En la lista **Sitio de destino**, seleccione el sitio que contendrá la copia de seguridad del catálogo.
  - d) Opcionalmente, especifique otras opciones para el trabajo de copia de seguridad. Pulse **Guardar**.
  - e) En el panel de navegación, pulse **Gestionar protección > IBM Spectrum Protect Plus > Copia de seguridad**.
  - f) En el panel **Política de SLA**, seleccione la política que ha creado. Pulse **Guardar**.
  - g) La política se visualiza en el panel **Estado de la política de SLA**. Si no aparece automáticamente, pulse el botón de renovación.
  - h) Para iniciar la copia de seguridad del catálogo, pulse **Acciones** y, a continuación, pulse .
  - i) Verifique la finalización del trabajo de copia de seguridad del catálogo. En el panel de navegación, haga clic en **Trabajos y operaciones** para verificar que el trabajo de copia de seguridad del catálogo se ha completado correctamente.
  - j) Ponga en pausa todos los trabajos planificados. En el panel de navegación, pulse **Trabajos y operaciones** y, a continuación, pulse la pestaña **Planificar**. Pulse **Pausar todas las planificaciones**. El estado de todos los trabajos planificados cambiará a **Retenido**.
  - k) Para verificar que no hay trabajos en ejecución, pulse la pestaña **Trabajos en ejecución**. Si hay trabajos en ejecución, permita a los trabajos completar el proceso.
2. Para preparar la actualización de servidores vSnap, revise IBM Spectrum Protect Plus Blueprints en <https://www.ibm.com/support/pages/node/1119489>. Deben actualizarse todos los servidores vSnap de su entorno al mismo nivel de versión de IBM Spectrum Protect Plus. Para actualizar servidores vSnap, complete los pasos siguientes:
  - a) Siga los pasos para actualizar el sistema operativo para servidores vSnap, tal como se describe en [“Actualización del sistema operativo para un servidor vSnap virtual”](#) en la página 185.


**Importante:** Debe cambiar el nombre del archivo ISO descargado como se describe en el procedimiento y moverlo al directorio /tmp en el servidor vSnap si desea actualizar el sistema operativo.
  - b) Complete los pasos para actualizar un servidor vSnap, tal como se describe en [“Actualización de un servidor vSnap”](#) en la página 186.

**Consejo:** Después de actualizar un servidor vSnap, reiniciar el servidor vSnap puede tardar 15 minutos más que en versiones anteriores. Para obtener más información, consulte <https://www.ibm.com/support/pages/node/3531159>.
3. Actualice el servidor de IBM Spectrum Protect Plus completando los pasos siguientes:
  - a) Opcional: Si el servidor de IBM Spectrum Protect Plus se despliega de forma virtual, tome una instantánea del dispositivo en la interfaz de hipervisor adecuada.
  - b) Actualice el servidor de IBM Spectrum Protect Plus. Siga los pasos del 1 al 6 en el tema de [“Actualización del dispositivo virtual de IBM Spectrum Protect Plus”](#) en la página 187. No libere la planificación ni ningún trabajo que se hayan retenido como se indica en los dos últimos pasos.
  - c) Vuelva a iniciar sesión en el servidor de IBM Spectrum Protect Plus.
4. Actualizar proxies VADP. Después de actualizar el servidor de IBM Spectrum Protect Plus, los proxies VADP se actualizan de forma automática. Sin embargo, es posible que los proxies no se actualicen inmediatamente

Para actualizar los proxies VADP inmediatamente, siga los pasos del tema de [“Actualización de proxies VADP”](#) en la página 189.

5. Verifique que todos los componentes se han actualizado correctamente completando los pasos siguientes:
  - a) Utilizando la cuenta `serveradmin`, inicie sesión en la consola de administración de IBM Spectrum Protect Plus. Siga los pasos descritos en el apartado [“Inicio de sesión en la consola de administración”](#) en la página 219.
  - b) Haga clic en **Gestión de productos**. En la tabla, verifique que los elementos siguientes tienen el mismo nivel de versión: `release spp.`, `vsnap`, `vsnap-dist`, `vadp` y `vadp-dist`.
  - c) Finalice la sesión en la consola de administración de IBM Spectrum Protect Plus.
  - d) Cargue la pantalla inicial de IBM Spectrum Protect Plus abriendo un navegador soportado y escribiendo el siguiente URL:

`https://nombre_host/`

donde *hostname* es la dirección IP de la máquina virtual en la que se despliega la aplicación.
  - e) Verifique que la versión y la compilación en la pantalla inicial coincidan con el `spp-release` que se visualiza en la sección **Gestión de productos** de la consola de administración.
  - f) Para verificar que un trabajo de mantenimiento se puede completar correctamente en el entorno actualizado, en el panel de navegación, haga clic en **Trabajos y operaciones > Planificar**. Haga clic en el icono de opciones  junto al trabajo de mantenimiento y seleccione **Iniciar**. Supervise el progreso de trabajo a través del panel **Trabajos y operaciones**.
6. Libere los trabajos planificados y, opcionalmente, elimine la instantánea. Siga los pasos siguientes:
  - a) Libere todas las planificaciones. En el panel de navegación, haga clic en **Trabajos y operaciones > Planificar**. Haga clic en **Liberar todas las planificaciones**.
  - b) Opcional: Si ha tomado una instantánea del dispositivo virtual de IBM Spectrum Protect Plus, puede suprimir la instantánea del servidor de IBM Spectrum Protect Plus utilizando la interfaz de hipervisor. Siga las instrucciones de la documentación del hipervisor.

#### Qué hacer a continuación

Si es necesario, reinicie los trabajos que se han detenido o se han pausado durante el periodo de mantenimiento y verificación.

## 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

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 23.

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 186

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

La actualización del sistema operativo del servidor vSnap con el archivo ISO le proporciona las actualizaciones de seguridad y los parches disponibles más recientes. Si el sistema operativo es CentOS Linux versión 7.4 o anterior, debe actualizar el sistema operativo antes de actualizar el software del servidor vSnap. La actualización del sistema operativo es opcional para las versiones 7.5 o 7.6. Se descarga un archivo ISO y se utiliza para actualizar servidores vSnap virtuales.

### Antes de empezar

Antes de comenzar el proceso de actualización, asegúrese de que ha realizado la copia de seguridad del entorno de IBM Spectrum Protect Plus como se describe en “Copia de seguridad de la aplicación de IBM Spectrum Protect Plus” en la página 505. Para obtener información sobre la obtención del archivo ISO, consulte “Actualización del dispositivo virtual de IBM Spectrum Protect Plus” en la página 187.

**Restricción:** No se debe utilizar ISO si se está actualizando un servidor Red Hat Enterprise Linux físico. Solo se debe utilizar en despliegues de OVA.

### Procedimiento

1. Descargue el archivo ISO `<part_number>.iso`. Mueva el archivo ISO al directorio `/tmp` en el servidor vSnap y cambie el nombre del archivo por `spp_with_os.iso`.

```
$mv <part_number>.iso /tmp/spp_with_os.iso
```

**Importante:** Es fundamental cambiar el nombre del archivo ISO descargado como se describe en este paso y moverlo al directorio `/tmp` en el servidor vSnap si desea actualizar el sistema operativo.

2. Continúe con las instrucciones que se encuentran en el tema de “Actualización de un servidor vSnap” en la página 186. Cuando se ejecuta el archivo `<part_number>.run`, el instalador actualizará opcionalmente el sistema operativo si `/tmp/spp_with_os.iso` está presente.

Se dará uno de los dos escenarios siguientes en función de la presencia del archivo ISO.

- Si el archivo está presente, los paquetes de sistema operativo se actualizan y, a continuación, se actualiza el software de vSnap.
- Si el archivo no está presente, se muestra el mensaje:

```
El archivo /tmp/spp_with_os.iso no está presente, omite la actualización de los paquetes de SO.  
Para actualizar los paquetes del sistema operativo, descargue el archivo ISO en /tmp/  
spp_with_os.iso y vuelva a ejecutar este instalador.
```

Después, se actualiza el software de software.

Una vez que se haya completado el instalador, se puede suprimir `/tmp/spp_with_os.iso`.

### Tareas relacionadas

“Actualización de un servidor vSnap” en la página 186

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 505](#).
2. Descargue el archivo de actualización de vSnap `<part_number>.run` y cópielo en una ubicación temporal en el servidor vSnap. Para obtener información sobre la descarga de archivos, consulte [Nota técnica 5693313](#).

### 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 `<part_number>.run` convierta el archivo en ejecutable emitiendo el mandato siguiente:

```
$ chmod +x <part_number>.run
```

3. Ejecute el instalador emitiendo el siguiente mandato:

```
$ sudo ./<part_number>.run
```

De forma alternativa, las instalaciones no interactivas o las actualizaciones de vSnap se pueden iniciar utilizando la opción `noprompt`. Cuando se utiliza esta opción, el instalador de vSnap omitirá la solicitud de información para respuestas y asume una respuesta de "sí" a las siguientes solicitudes:

- Acuerdo de licencia
- Instalación o actualización de Kernel
- Vuelva a arrancar el final de la instalación o actualización si es necesario

Para utilizar la opción `noprompt`, emita el mandato siguiente. Observe el espacio deliberado antes y después de los guiones dobles:

```
$ sudo ./<part_number>.run -- noprompt
```

Se instalan los paquetes de vSnap.

4. Una vez que se han instalado los paquetes de vSnap, inicie la versión actualizada del servidor vSnap.
5. En el panel de navegación, pulse **Trabajos y operaciones**, a continuación, pulse la pestaña **Planificación**.  
Encuentre los trabajos que ha puesto en pausa.
6. En el menú **Acciones** para los trabajos en pausa, seleccione **Liberar planificación**.



# 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

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 505.
2. Para las actualizaciones fuera de línea, descargue la actualización de IBM Spectrum Protect Plus de requisito previo denominada `<part_number>.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 5693313](#).

## 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 autenticación	Información de inicio de sesión
IBM Spectrum Protect Plus	Para iniciar la sesión como un usuario de IBM Spectrum Protect Plus con privilegios SUPERUSER, 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 la sesión como un usuario del sistema, especifique la contraseña de serveradmin. La contraseña predeterminada es sppDP758-SysXyz. 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)**. Solo puede seleccionar un archivo de actualización cada vez.

**Importante:** Debe haber al menos 4.2 GB de espacio de disco disponible en el directorio /tmp del servidor IBM Spectrum Protect Plus.

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**, 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 184](#)

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.

## Pasos adicionales para actualizar máquinas virtuales en entornos de Hyper-V Replica

A partir de IBM Spectrum Protect Plus versión 10.1.5, puede proteger las máquinas virtuales (VM) habilitadas para usar la característica Hyper-V Replica.

IBM Spectrum Protect Plus procesa los datos en las instancias de origen y replicadas de las MV por separado. Por ejemplo, si una MV denominada VM1 está en el host de Hyper-V denominado Host1 y la MV se replica en Host2, IBM Spectrum Protect Plus asigna los ID VM1@Host1 y VM1@Host2 a las MV. A continuación, puede seleccionar una o ambas MV para la protección de datos.

### Consideraciones para las máquinas virtuales definidas en las políticas de SLA existentes

Si actualiza IBM Spectrum Protect Plus, es posible que tenga que realizar pasos adicionales para garantizar que la protección de datos continúa para las MV incluidas actualmente en las políticas de acuerdo de nivel de servicio (SLA).

Una política de SLA puede incluir *implícitamente* o *explícitamente* una máquina virtual replicada. Es posible que sea necesario actualizar la política de SLA cuando actualice a IBM Spectrum Protect Plus V10.1.5 o posterior.

Un ejemplo de una política de SLA que incluye implícitamente una MV replicada es un escenario en el que la política protege todas las máquinas virtuales en Host1, que contiene las máquinas virtuales VM1. VM1 se replica en Host2. En este escenario, no es necesario un cambio en la política de SLA después de actualizar IBM Spectrum Protect Plus. La política de SLA crea una copia de seguridad completa de la instancia de VM1 en Host2 y crea una copia de seguridad completa nueva de la instancia de VM1 en Host1. Las copias de seguridad existentes de VM1 en Host1 que se crearon antes de la actualización caducarán en base a los valores de retención de políticas de SLA.

Un ejemplo de una política de SLA que incluye explícitamente una máquina virtual replicada es un escenario en el que la política protege a VM1 en Host1 y VM1 se replica en Host2. En este escenario, debe volver a añadir la instancia de la máquina virtual en cada host a la política de SLA después de actualizar IBM Spectrum Protect Plus.

## 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 505](#).



**Nota:** Solo se actualizarán los proxies VADP con IBM Spectrum Protect Plus. Si el proxy VADP no se registra con IBM Spectrum Protect Plus, el componente VADP no se actualizará.

### 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**. Haga clic en el icono de puntos suspensivos **\*\*\*** y seleccione **Editar**. Seleccione **Utilizar usuario existente** y elija una identidad especificada anteriormente en **Seleccionar usuario** 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.	<p>Consulte <a href="#">“Copia de seguridad de datos de VMware”</a> en la página 262.</p> <p>Los proxies se indican en el registro de trabajo con un mensaje de registro similar al texto siguiente:</p> <p>Run remote vmdkbackup of MicroService: http://&lt;proxy nombrenodo, IP:dirección_IP_proxy</p>

### Tareas relacionadas

“Creación de proxies VADP” en la página 268

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 108

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 8. Configuración del entorno del sistema

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.



**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 copiar instantáneas desde un servidor vSnap a un sistema de almacenamiento en la nube o a un servidor de repositorio.

Para obtener más información sobre la copia de datos de instantánea en un almacenamiento secundario, consulte [“Copiar instantáneas en almacenamiento de copias de seguridad secundario”](#) en la página 12.

### Gestión del almacenamiento en la nube

Puede copiar datos de instantánea en el almacenamiento en la nube para una protección de datos más a largo plazo.

#### Configuración para copiar o archivar datos en la nube

Si tiene previsto copiar o archivar datos de IBM Spectrum Protect Plus en el almacenamiento en la nube para una retención a largo tiempo o para el almacenamiento de instantáneas, debe configurar un almacenamiento secundario.

#### Tareas para configurar el almacenamiento en la nube

Debe configurar IBM Spectrum Protect Plus para realizar operaciones de copia de seguridad y restauración en el almacenamiento en la nube como se muestra en la Tabla 1.

Escenario de usuario	Propósito	Pasos
Almacene datos deduplicados y datos no deduplicados en una agrupación de almacenamiento de contenedores en la nube y restaure los datos según sea necesario.	Copie datos en almacenamiento en la nube. En la primera operación de copia, se crea una copia de seguridad completa. Las copias posteriores son incrementales.	<p>Elija uno de los siguientes proveedores:</p> <ul style="list-style-type: none"> <li>• “<a href="#">Adición del almacenamiento de objetos de Amazon S3</a>” en la <a href="#">página 192</a></li> <li>• “<a href="#">Adición de IBM Cloud Object Storage como proveedor de almacenamiento de copias de seguridad</a>” en la <a href="#">página 193</a></li> <li>• “<a href="#">Adición del almacenamiento en la nube de Microsoft Azure como proveedor de almacenamiento de copias de seguridad</a>” en la <a href="#">página 195</a></li> <li>• “<a href="#">Adición del almacenamiento de objetos compatible de S3</a>” en la <a href="#">página 196</a></li> </ul>

### Adición del almacenamiento de objetos de Amazon S3

Puede añadir Amazon Simple Storage Service (S3) como un proveedor de almacenamiento de copias de seguridad a IBM Spectrum Protect Plus para permitir las operaciones de copia en el almacenamiento de Amazon 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 220](#).

Asegúrese de que se crean grupos de almacenamiento en la nube para los datos de IBM Spectrum Protect Plus. Para obtener instrucciones sobre la creación de grupos, consulte [Documentación de Amazon Simple Storage Service](#).

### Procedimiento

Para añadir el almacenamiento en la nube de Amazon S3 como proveedor de almacenamiento de objetos de copia de seguridad, complete los pasos siguientes:

1. En el menú de navegación, haga clic en **Configuración del sistema > Almacenamiento de copias de seguridad > Almacenamiento de objetos**.
2. Pulse **Añadir almacenamiento de objetos**.
3. En la lista **Proveedor**, seleccione **Amazon S3**.
4. Complete los campos en el formulario **Registro de almacenamiento de objetos**:

#### 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 en la consola de gestión de AWS.

### Clave secreta

Especifique la clave secreta de AWS. Las claves secretas se crean en la consola de gestión de AWS.

### Habilitar Deep Archive

Opcionalmente, seleccione esta opción para habilitar la clase de almacenamiento Amazon S3 Glacier Deep Archive.

- Haga clic en **Obtener grupos** para conectar IBM Spectrum Protect Plus a AWS para recuperar la lista de grupos disponibles.
- Seleccione el grupo que tiene planeado utilizar como destino de copia.  
Se visualizan los campos **Grupo de almacenamiento de objetos estándar** y **Grupo de almacenamiento de objetos de archivado**.
- En el campo **Grupo de almacenamiento de objetos estándar**, seleccione un grupo para que sirva de destino de copia.
- Opcional: En el campo **Grupo de almacenamiento de objetos de archivado**, seleccione un recurso de almacenamiento en la nube que sirva 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 [“Copiar instantáneas en almacenamiento de copias de seguridad secundario”](#) en la página 12.
- Seleccione **Deep Archive** para registrar los grupos de Amazon S3 Glacier Deep Archive Buckets para el archivado a largo plazo.
- Pulse **Registrar** para completar la operación.  
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 <a href="#">“Creación de una política de SLA para hipervisores, bases de datos y sistemas de archivos”</a> en la página 244.  Para modificar una política de SLA existente, consulte <a href="#">“Edición de una política de SLA”</a> en la página 255.

### 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 copiar datos en 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 220 y [“Adición de un certificado”](#) en la página 221.

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](#).

Al crear un grupo en IBM Cloud Object Storage (COS), asegúrese de que **Añadir regla de archivado** y **Añadir reglas de caducidad** no están seleccionadas cuando se crean grupos que se van a utilizar para copia o archivado. Esto puede dar como resultado un fallo con el error “el paquete tiene una configuración de ciclo de vida no soportada” cuando el trabajo intenta ejecutarse en IBM Spectrum Protect Plus. La opción **Añadir política de retención** puede establecerse para un grupo que se va a utilizar para copia, pero no debe establecerse para un grupo que se utilizará para archivado.

El grupo de tipo Cold Vault solo debe utilizarse cuando se archiva, ya que es la opción de coste más bajo y se describe como ideal para la retención a largo plazo de datos a los que se accederá mínimamente.

Al añadir IBM Cloud Object Storage (COS), el método para obtener el acceso y la clave de secreto dependerá del modelo de despliegue. Si es local, las claves se pueden obtener de la consola de IBM COS Manager. Para IBM COS IaaS, se crean claves cuando se crea una cuenta de servicio y se puede obtener del portal softlayer. Si utiliza IBM COS (COS como servicio), el acceso y la clave secreta no se crean de forma predeterminada; cuando se crea una cuenta de servicio, compruebe el recuadro **Incluir credencial de HMAC** y añada `{"HMAC": true}` al área de texto **Añadir parámetros de configuración en línea**.

## Procedimiento

Para añadir IBM Cloud Object Storage como un proveedor de almacenamiento de copia de seguridad, complete los pasos siguientes:

1. En el menú de navegación, haga clic en **Configuración del sistema > Almacenamiento de copias de seguridad > Almacenamiento de objetos**.
2. Pulse **Añadir almacenamiento de objetos**.
3. En la lista **Proveedor**, seleccione **IBM Cloud Object Storage**.
4. Complete los campos en el panel **Registro de almacenamiento de objetos**:

### 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 el IBM Cloud Object Storage público.

5. Haga clic en **Obtener grupos**, a continuación, seleccione un grupo que sirva de destino de la copia.

Una vez generados los grupos, se visualizan los campos **Grupo de almacenamiento de objetos estándar** y **Grupo de almacenamiento de objetos de archivado**.



6. En el campo **Grupo de almacenamiento de objetos estándar**, seleccione un grupo para que sirva de destino de copia.
7. Opcional: En el campo **Grupo de almacenamiento de objetos de archivado**, seleccione un recurso de almacenamiento en la nube que sirva 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 [“Copiar instantáneas en almacenamiento de copias de seguridad secundario” en la página 12](#).

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, complete la siguiente acción:

Acción	Cómo
Asocie el almacenamiento en la nube con la política de SLA que se utiliza para el trabajo de copia de seguridad.	<p>Para crear una política de SLA, consulte <a href="#">“Creación de una política de SLA para hipervisores, bases de datos y sistemas de archivos” en la página 244</a>.</p> <p>Para modificar una política de SLA existente, consulte <a href="#">“Edición de una política de SLA” en la página 255</a>.</p>

### Adición del almacenamiento en la nube de Microsoft Azure como proveedor de almacenamiento de copias de seguridad

Añada el almacenamiento en la nube de Microsoft Azure para que IBM Spectrum Protect Plus pueda copiar los datos en el almacenamiento 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, haga clic en **Configuración del sistema > Almacenamiento de copias de seguridad > Almacenamiento de objetos**.
2. Pulse **Añadir almacenamiento de objetos**.
3. En la lista **Proveedor**, seleccione **Almacenamiento de Microsoft Blob Azure**.
4. Complete los campos en el panel **Registro de almacenamiento de objetos**:

#### 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. Haga clic en **Obtener grupos**, a continuación, seleccione un grupo que sirva de destino de la copia. Una vez generados los grupos, se visualizan los campos **Grupo de almacenamiento de objetos estándar** y **Grupo de almacenamiento de objetos de archivado**.
6. En el campo **Grupo de almacenamiento de objetos estándar**, seleccione un grupo para que sirva de destino de copia.
7. Opcional: En el campo **Grupo de almacenamiento de objetos de archivado**, seleccione un recurso de almacenamiento en la nube que sirva 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 [“Copiar instantáneas en almacenamiento de copias de seguridad secundario” en la página 12](#).
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.	<p>Para crear una política de SLA, consulte <a href="#">“Creación de una política de SLA para hipervisores, bases de datos y sistemas de archivos” en la página 244</a>.</p> <p>Para modificar una política de SLA existente, consulte <a href="#">“Edición de una política de SLA” en la página 255</a>.</p>

### Adición del almacenamiento de objetos compatible de S3

Además de realizar copia de seguridad de los datos en Amazon Simple Storage Service (S3) e IBM Cloud Object Storage, es posible que desee realizar una copia de seguridad de los datos en otros proveedores de almacenamiento de objetos compatibles de S3. Antes de hacer una copia de seguridad en un entorno de producción para cualquier otro almacenamiento de objetos de S3 compatible, asegúrese de que el almacenamiento de objetos se ha validado para su uso con IBM Spectrum Protect Plus.

### Antes de empezar

#### Consejo:

Para obtener información sobre proveedores de almacenamiento de objetos compatibles, consulte la [nota técnica 108714](#).

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 220](#).

Asegúrese de que los grupos de almacenamiento en la nube estén disponibles. Para obtener más información sobre los grupos de almacenamiento en la nube, consulte la documentación para el proveedor de almacenamiento de S3 compatible.

### Procedimiento

Para añadir almacenamiento en la nube de S3 compatible como destino de copia de seguridad, complete los pasos siguientes:

1. En el menú de navegación, haga clic en **Configuración del sistema > Almacenamiento de copias de seguridad > Almacenamiento de objetos**.
2. Pulse **Añadir almacenamiento de objetos**.
3. En la lista **Proveedor**, seleccione **Almacenamiento de S3 compatible**.
4. Complete los campos en el panel **Registro de almacenamiento de objetos**:

**Nombre**

Especifique un nombre significativo para ayudar a identificar el almacenamiento en la nube.

**Punto final**

Especifique el punto final del almacenamiento en la nube.

**Utilizar clave de acceso 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 identificar la clave.

**Clave de acceso**

Especifique la clave de acceso compatible de S3. Para obtener instrucciones sobre cómo obtener claves de acceso, consulte la documentación del proveedor de almacenamiento compatible de S3.

**Clave secreta**

Especifique la clave secreta compatible de S3. Para obtener instrucciones sobre cómo obtener claves de acceso, consulte la documentación del proveedor de almacenamiento compatible de S3.

**Certificado**

Seleccione la opción adecuada para añadir un certificado para el almacenamiento compatible de S3:

**Cargar**

Para cargar un certificado, haga clic en **Examinar** para localizar y seleccionar el certificado. Pulse **Cargar**.

**Copiar y pegar**

Especifique un nombre para el certificado y pegue el certificado en el área de texto. Haga clic en **Crear**.

**Utilizar existente**

Si existe un certificado, seleccione el certificado de la lista **Seleccionar un certificado**.

5. Haga clic en **Obtener grupos** y, a continuación, seleccione un grupo para que sirva como destino. Una vez generados los grupos, se visualizan los campos **Grupo de almacenamiento de objetos estándar** y **Grupo de almacenamiento de objetos de archivado**.
6. En el campo **Grupo de almacenamiento de objetos estándar**, seleccione un grupo para que sirva como destino de copia de seguridad.
7. Opcional: En el campo **Grupo de almacenamiento de objetos de archivado**, seleccione un recurso de almacenamiento en la nube que sirva 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 [“Copiar instantáneas en almacenamiento de copias de seguridad secundario” en la página 12](#).
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 S3 compatible, complete la siguiente acción:


Acción	Procedimiento
Asocie el almacenamiento en la nube con la política de SLA que se utiliza para el trabajo de copia de seguridad.	<p>Para crear una política de SLA, consulte <a href="#">“Creación de una política de SLA para hipervisores, bases de datos y sistemas de archivos”</a> en la página 244.</p> <p>Para modificar una política de SLA existente, consulte <a href="#">“Edición de una política de SLA”</a> en la página 255.</p>

### 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, haga clic en **Configuración del sistema > Almacenamiento de copias de seguridad > Almacenamiento de objetos**.
2. Haga clic en el icono de edición  asociado al proveedor de almacenamiento de objetos.  
Se visualiza el panel **Actualizar almacenamiento de objetos**.
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, haga clic en **Configuración del sistema > Almacenamiento de copias de seguridad > Almacenamiento de objetos**.
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 copiar datos en un servidor de repositorio para la protección de datos a más largo plazo. Para el release actual de IBM Spectrum Protect Plus, el servidor de repositorio debe ser un Servidor de IBM Spectrum Protect Versión 8.1.7 o posterior. Para copiar datos en una cinta, se requiere Servidor de IBM Spectrum Protect versión 8.1.8 o posterior.

Puede elegir replicar los datos de IBM Spectrum Protect Plus que se copian en Servidor de IBM Spectrum Protect en un servidor de destino. Sin embargo, IBM Spectrum Protect Plus no es consciente de las operaciones de réplica de Servidor de IBM Spectrum Protect posteriores y no puede restaurar los datos replicados desde el Servidor de IBM Spectrum Protect de destino a IBM Spectrum Protect Plus.

### Configuración para copiar o archivar datos en IBM Spectrum Protect

Si tiene previsto copiar o archivar datos de IBM Spectrum Protect Plus en un Servidor de IBM Spectrum Protect, hay tres configuraciones posibles. La elección de cuál se debe configurar depende de qué escenario se aplica a sus necesidades de protección de datos. Para cada escenario, hay pasos necesarios en los entornos de IBM Spectrum Protect Plus y Servidor de IBM Spectrum Protect para completar la configuración.

### Tareas para configurar IBM Spectrum Protect

Debe configurar Servidor de IBM Spectrum Protect para comunicarse con el servidor de IBM Spectrum Protect Plus y para habilitar las solicitudes de proceso para las operaciones de copia de seguridad y

restauración. El protocolo Amazon Simple Storage Service (S3) permite la comunicación entre los dos servidores.

Escenario de usuario	Propósito	Pasos
Copiar en un almacenamiento de objetos estándar cuando se estén ejecutando copias diarias o menos frecuentes en un almacenamiento de objetos estándar.	Copiar datos en un almacenamiento de objetos estándar. En la primera operación de copia, se crea una copia de seguridad completa. Las copias posteriores son incrementales. La copia de datos en el almacenamiento de objetos estándar 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 en cintas.	Para copiar datos en un almacenamiento de objetos estándar en Servidor de IBM Spectrum Protect, debe crear una agrupación de almacenamiento de contenedor de directorios o de contenedor en la nube, y configurar el componente de agente objeto de IBM Spectrum Protect. La adición del agente objeto es un paso obligatorio. Además de configurar la agrupación de almacenamiento necesaria, siga los pasos del 2 al 4 listados, <a href="#">aquí</a> .
Copiar en cinta cuando se esté creando una copia completa de los datos semanalmente o menos frecuente en el almacenamiento en cintas.  <b>Importante:</b> El archivado de datos en cintas no se puede ejecutar con menos frecuencia que una vez a la semana. Por esta razón, los datos archivados no deben considerarse una copia útil para la recuperación tras desastre.	Cuando copia datos en cintas, se crea una copia de datos completa durante el proceso de copia. La copia de datos en cintas proporciona beneficios de seguridad adicionales. 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. Sin embargo, como la copia 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 copiar datos en cintas, debe crear una agrupación de almacenamiento de contenedor de directorios o de contenedor en la nube para cintas, y una agrupación de almacenamiento de memoria caché de datos fríos Servidor de IBM Spectrum Protect. La adición del agente objeto es un paso obligatorio. Siga los pasos 1-4 listados, <a href="#">aquí</a> .
Combinación del almacenamiento de objetos estándar y de la copia a largo plazo en cintas	Proteja los datos en copias de seguridad incrementales en Servidor de IBM Spectrum Protect, además de retener datos en cintas para una seguridad a más largo plazo.	Esta es una combinación de los casos anteriores: los datos se almacenan en cinta y los datos se almacenan en el almacenamiento de objetos estándar en Servidor de IBM Spectrum Protect. Además de configurar las agrupaciones de almacenamiento de datos necesarias para ambos escenarios, la creación de un agente objeto es obligatoria.

Los cuatro pasos necesarios para establecer y configurar la comunicación de transferencia de datos entre IBM Spectrum Protect Plus y Servidor de IBM Spectrum Protect son los siguientes:

1. Si está configurando agrupaciones de almacenamiento para copiar datos en cinta, siga el Paso 1. Cree agrupaciones de almacenamiento en Servidor de IBM Spectrum Protect utilizando IBM Spectrum Protect Operations Center. Para obtener instrucciones, consulte [“Paso 1: Creación de una agrupación de almacenamiento en cintas y una agrupación de almacenamiento de memoria caché de datos fríos para copiar datos en cintas”](#) en la página 200. Este paso es necesario solo si está configurando IBM Spectrum Protect para el archivado con copias que se ejecutan una vez a la semana o con menos frecuencia.
2. Cree un dominio de políticas que apunte a la agrupación o agrupaciones de almacenamiento. El dominio de políticas define las reglas que controlan los servicios de copia de seguridad para IBM Spectrum Protect Plus. Para obtener instrucciones, consulte [“Paso 2: Configuración de un dominio de políticas de objeto”](#) en la página 202.
3. Si copia datos en una agrupación de almacenamiento estándar o en una cinta, debe añadir el almacenamiento de objetos estándar en Servidor de IBM Spectrum Protect. Para obtener instrucciones, consulte [“Paso 3: Configuración del almacenamiento de objetos estándar”](#) en la página 204.
4. Añada un agente objeto a Servidor de IBM Spectrum Protect. El agente objeto proporciona una pasarela entre el servidor IBM Spectrum Protect Plus y Servidor de IBM Spectrum Protect. Para obtener instrucciones, consulte [“Paso 4: Adición de un agente objeto para copiar datos”](#) en la página 207.
5. Para completar la configuración, debe añadir un cliente objeto a Servidor de IBM Spectrum Protect. El cliente objeto identifica el servidor de IBM Spectrum Protect Plus y le permite almacenar objetos en Servidor de IBM Spectrum Protect. Se utilizan las mismas credenciales que las que ha utilizado para IBM Spectrum Protect Plus para el cliente objeto, que es el cliente objeto que está asociado con el dominio de políticas como se ha configurado en el Paso 2. Para obtener instrucciones para configurar un cliente objeto, consulte [“Paso 5: Adición y configuración de un cliente objeto para copiar datos”](#) en la página 209.

**Consejo:** De forma alternativa, especifique el mandato **DEFINE STGPOOL** para crear una agrupación de almacenamiento tal como se describe en los temas siguientes:

### Qué se debe hacer a continuación

1. Después de completar las tareas necesarias para el almacenamiento de IBM Spectrum Protect, debe añadir Servidor de IBM Spectrum Protect a IBM Spectrum Protect Plus. Para obtener información sobre cómo hacerlo, siga las instrucciones en [“Registro de un servidor de repositorio como proveedor de almacenamiento de copias de seguridad”](#) en la página 210.
2. Cuando está hecho, puede crear una política de SLA que defina Servidor de IBM Spectrum Protect como el destino de almacenamiento de copia de seguridad. Para obtener más información que le ayude a elegir el tipo de política que necesita, consulte [“Configuración para copiar o archivar datos en IBM Spectrum Protect”](#) en la página 198

### **Paso 1: Creación de una agrupación de almacenamiento en cintas y una agrupación de almacenamiento de memoria caché de datos fríos para copiar datos en cintas**

Antes de poder copiar datos desde IBM Spectrum Protect Plus a Servidor de IBM Spectrum Protect para fines de archivado, debe configurar un servicio de agente objeto. Para el archivado de datos a largo plazo, debe configurar una agrupación de almacenamiento de datos fríos. Si no tiene previsto archivar datos en cintas en el Servidor de IBM Spectrum Protect, puede omitir este paso.

### **Acerca de esta tarea**

Antes de empezar asegúrese de que ha cambiado el tamaño de las necesidades de almacenamiento de memoria caché en frío utilizando la herramienta de dimensionamiento y Blueprints. Para obtener más información sobre cómo hacerlo, consulte [Blueprints](#). Para obtener vídeos y enlaces útiles, consulte [“Storyboard de despliegue para IBM Spectrum Protect Plus”](#) en la página 1.

No se accede con frecuencia a los datos de cliente objeto especificados con una clase de almacenamiento S3 Glacier. Para habilitar la copia de estos datos, que a menudo se denominan *datos fríos*, en almacenamiento en cintas, los datos se graban temporalmente en una agrupación de almacenamiento que cumple los requisitos para manejar datos de objeto. A continuación, los datos se mueven al dispositivo de cinta o VTL. Esta agrupación de almacenamiento, denominada *agrupación de almacenamiento de memoria caché de datos fríos*, se asigna a un dominio de políticas para clientes objeto. Solo se pueden grabar datos de clientes objeto a o restaurar desde una agrupación de almacenamiento de memoria caché de datos fríos.

## Procedimiento

Si no está utilizando el Centro de operaciones, puede utilizar el mandato **define stgpool**. El mandato se puede definir de la siguiente manera:

```
define stgpool NAME
stgtype=colddatacache
```

**Nota:** Para configurar agrupaciones estándar para el almacenamiento de objetos, siga estos pasos pero cuando defina el tipo de agrupación de almacenamiento, seleccione Estándar.

Para configurar Servidor de IBM Spectrum Protect para copiar datos de un cliente objeto en un soporte de cinta física o un VTL, complete los pasos de configuración siguientes:

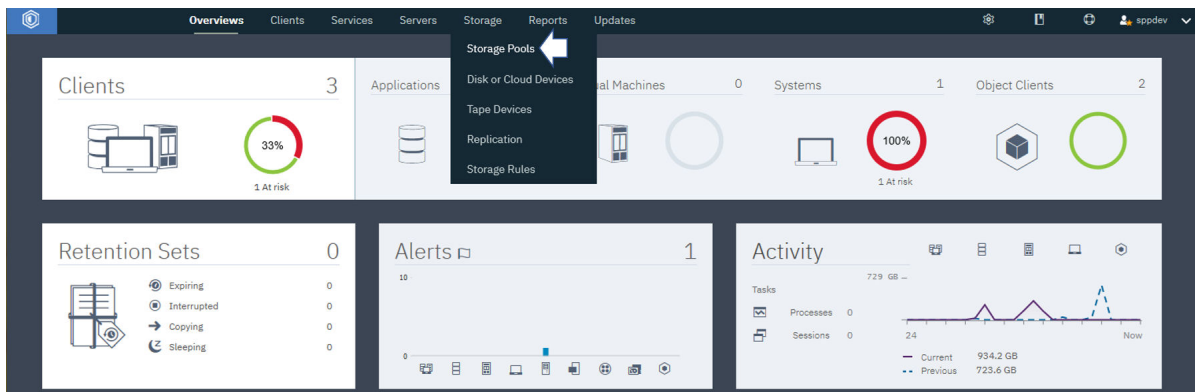
1. En Servidor de IBM Spectrum Protect, configure una agrupación de almacenamiento primaria que representa un dispositivo de cinta o VTL. Esta agrupación de almacenamiento primaria es el destino para los datos de objeto que desea copiar.

Más tarde, cuando define la agrupación de almacenamiento de memoria caché de datos fríos, debe especificar esta agrupación en cintas como la siguiente agrupación de almacenamiento para la agrupación de memoria caché de datos fríos.

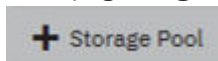
**Restricciones:** Las restricciones siguientes se aplican a la agrupación de almacenamiento de cinta:

- No puede replicar datos de cliente objeto a o desde la agrupación de almacenamiento de cinta.
- La agrupación de almacenamiento de cinta no se puede deduplicar.
- No se puede especificar una agrupación de almacenamiento siguiente para la agrupación de almacenamiento de cinta.

- a) En la barra de menús del Centro de operaciones, pulse **Almacenamiento > Agrupaciones de almacenamiento**.



- b) En la página **Agrupaciones de almacenamiento**, haga clic en **Agrupación de almacenamiento**



- c) En el asistente **Añadir agrupación de almacenamiento**, seleccione **Cliente objeto** para habilitar los clientes objetos para copiar datos en cintas.
2. Paso a través de los pasos del asistente para configurar una agrupación de almacenamiento de memoria caché de datos fríos.



Una agrupación de almacenamiento de memoria caché de datos fríos consta de uno o más directorios del sistema de archivos en el disco. Es una agrupación de almacenamiento intermediario entre el cliente objeto y un dispositivo de cinta o VTL y se enlaza con el almacenamiento de agrupación de acceso secuencial primario que representa el dispositivo de cinta o VTL. Identifique uno o más directorios del sistema de archivos existente para el almacenamiento de disco temporal y la agrupación de almacenamiento de acceso secuencial primaria que representa el dispositivo de cinta o VTL.

3. En la página **Memoria caché de datos fríos**, especifique uno o más directorios del sistema de archivos existentes para el almacenamiento de disco. Especifique un nombre de vía de acceso completo que se ajuste a la sintaxis que utiliza el sistema operativo del servidor.

Por ejemplo, especifique `c:\temp\dir1\` para Microsoft Windows, o `/tmp/dir1/` para UNIX.

Los datos de objeto se almacenan en volúmenes secuenciales en los directorios del sistema de archivos. Un cliente objeto puede copiar datos a los que se accede con poca frecuencia, o datos fríos, a un soporte de cinta física o a un VTL. Cuando un cliente objeto copia datos fríos, los datos se almacenan primero en la memoria caché de datos fríos. A continuación, los datos se migran, sin un retardo en la migración, a la agrupación de almacenamiento en cintas primaria que representa el soporte de cinta física o VTL. Una vez se migran los datos a la cinta, se suprimen de la memoria caché de datos fríos. La memoria caché de datos fríos se utiliza como un área de transferencia para restaurar datos fríos en el cliente objeto. Durante las operaciones de restauración, los datos se copian en la memoria caché de datos fríos. Los datos permanecen en la memoria caché de datos fríos durante un periodo de tiempo especificado por el cliente objeto. Los datos se restauran en el cliente objeto desde la memoria caché de datos fríos y no directamente desde la cinta o VTL.

Si especifica varios directorios para la mejora de rendimiento, asegúrese de que los directorios se corresponden con volúmenes físicos separados. Aunque la memoria caché de datos fríos se utiliza para el almacenamiento temporal, debe ser lo suficientemente grande como para contener los datos que se han copiado del cliente objeto antes de que los datos se migren a cintas. También debe ser lo suficientemente grande para contener datos durante las operaciones de restauración durante el periodo de tiempo especificado por el cliente objeto.

### Qué hacer a continuación

Cuando complete la configuración de la agrupación de almacenamiento de memoria caché de datos fríos, cree el dominio de objetos. Para obtener instrucciones sobre cómo hacerlo, consulte [“Paso 2: Configuración de un dominio de políticas de objeto”](#) en la página 202.

### **Paso 2: Configuración de un dominio de políticas de objeto**

Antes de copiar datos de IBM Spectrum Protect Plus a Servidor de IBM Spectrum Protect, debe crear y configurar un dominio de políticas de objeto. El dominio de políticas define las reglas que controlan los servicios de copia de seguridad para IBM Spectrum Protect Plus. Debe añadir una agrupación de almacenamiento estándar que esté con un almacenamiento basado en contenedores en la nube o directorios, y una agrupación fría si está copiando datos en cintas o archivando datos.

### Procedimiento

1. Verifique los valores del dominio de políticas que tiene previsto utilizar en las operaciones de copia de datos. Los clientes objeto que se definen o actualizan en Servidor de IBM Spectrum Protect V8.1.8 o posterior deben asignarse a dominios de políticas creados con el mandato **DEFINE OBJECTDOMAIN**. Un nodo de cliente objeto se asocia a este dominio de políticas cuando el nodo se registra o se actualiza utilizando los mandatos **REGISTER NODE** o **UPDATE NODE**.

**Restricción:** A partir de Servidor de IBM Spectrum Protect V8.1.8, todos los nodos de cliente objeto nuevos deben asignarse a dominios de políticas de objeto.

En los nodos de cliente objeto que se asignan a dominios de políticas que no son de objeto anteriores a V8.1.8, no tiene que actualizar la asignación después de actualizar el servidor a Servidor de IBM Spectrum Protect V8.1.8. Sin embargo, si se necesita una actualización para el dominio del nodo de cliente objeto, el nodo debe asignarse a un dominio de políticas de objeto.



2. Revise las siguientes consideraciones para especificar los dominios de políticas para operaciones de copia.

- En Servidor de IBM Spectrum Protect, un dominio de políticas puede especificar clases de gestión para agrupaciones de almacenamiento estándar (agrupaciones de almacenamiento de contenedores en la nube o de contenedores de directorio), agrupaciones de almacenamiento de memoria caché de datos fríos o agrupaciones de almacenamiento estándar y de almacenamiento de memoria caché de datos fríos.

Sin embargo, para copiar datos desde IBM Spectrum Protect Plus, debe especificar las siguientes clases de gestión dependiendo de si está copiando datos en una agrupación de almacenamiento de contenedores en la nube o de contenedores de directorio o si está copiando datos en una agrupación de almacenamiento de memoria caché de datos fríos en un soporte de cinta física o en una biblioteca virtual de cintas (VTL):

- Para datos en una agrupación de almacenamiento de contenedores en la nube o de contenedores de directorio, utilice el parámetro **STANDARDPOOL** para definir la agrupación de almacenamiento para el dominio de políticas como se muestra en el ejemplo siguiente:

```
define objectdomain mydomain standardpool=hotpool
```

- Para copiar datos en una agrupación de almacenamiento de memoria caché de datos fríos, debe especificar una agrupación estándar y una agrupación fría para los dominios de políticas. Se necesita una agrupación estándar para almacenar metadatos que se utilizan para operaciones de restauración y otras operaciones de IBM Spectrum Protect Plus. Para definir una agrupación de almacenamiento de memoria caché de datos fríos para un dominio de políticas, utilice el parámetro **COLDPOOL**, tal como se muestra en el ejemplo siguiente:

```
define objectdomain mydomain standardpool=hotpool coldpool=coldpool
```

- Todos los objetos se nombran de forma exclusiva. No hay versiones inactivas de objetos. Cuando define un dominio de políticas, se especifican automáticamente las siguientes políticas de gestión de almacenamiento:
  - El campo `Versions Data Exists` se establece en 1.
  - Los campos `Retain Extra Versions` y `Retain Only Version` se establecen en 0.
- El servidor de IBM Spectrum Protect Plus controla la hora a la que se suprimieron los objetos.

### Ejemplo: visualizar información detallada sobre un dominio de políticas en una operación de copia de IBM Spectrum Protect Plus

Cuando se crea el dominio de políticas, se asignan grupos de copias y clases de gestión. Puede utilizar el mandato **QUERY COPYGROUP** para ver información sobre las agrupaciones de almacenamiento de destino para el dominio de políticas. En el ejemplo siguiente, el nombre de dominio de políticas es XYZ. Las agrupaciones de almacenamiento de destino son HOTPOOL y COLDPOOL.

```
query copygroup xyz standard f=d
```

```

Policy Domain Name: XYZ
Policy Set Name: STANDARD
Mgmt Class Name: COLD
Copy Group Name: STANDARD
Copy Group Type: Backup
Versions Data Exists: 1
Versions Data Deleted: 1
Retain Extra Versions: 0
Retain Only Version: 0
Copy Mode: Modified
Copy Serialization: Shared Static
Copy Frequency: 0
Copy Destination: COLDPOOL
Table of Contents (TOC) Destination:
Last Update by (administrator): SERVER_CONSOLE
Last Update Date/Time: 05/22/20 17:03:46
Managing profile:
Changes Pending: No

Policy Domain Name: XYZ
Policy Set Name: STANDARD
Mgmt Class Name: STANDARD
Copy Group Name: STANDARD
Copy Group Type: Backup
Versions Data Exists: 1
Versions Data Deleted: 1
Retain Extra Versions: 0
Retain Only Version: 0
Copy Mode: Modified
Copy Serialization: Shared Static
Copy Frequency: 0
Copy Destination: HOTPOOL
Table of Contents (TOC) Destination:
Last Update by (administrator): SERVER_CONSOLE
Last Update Date/Time: 03/05/20 22:15:18
Managing profile:
Changes Pending: No

```

### Qué hacer a continuación

Después de crear el dominio de objetos, continúe con el paso siguiente [“Paso 3: Configuración del almacenamiento de objetos estándar”](#) en la página 204.

### *Paso 3: Configuración del almacenamiento de objetos estándar*

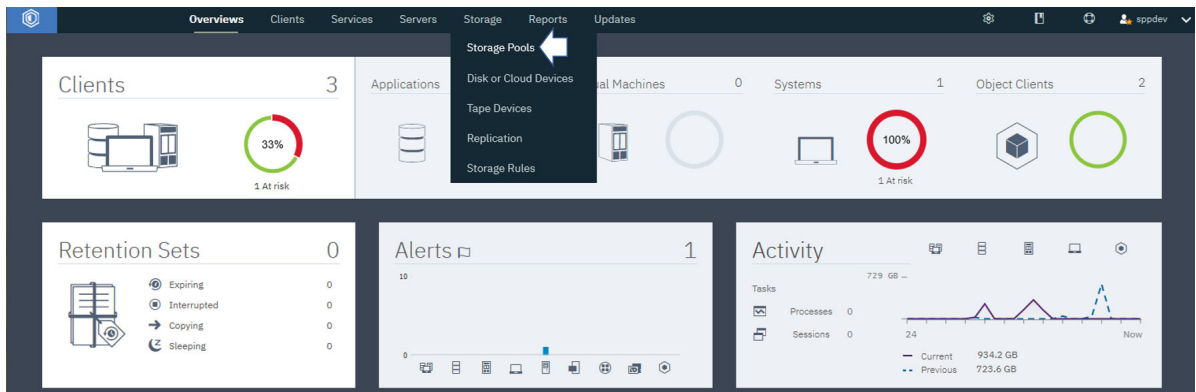
Para configurar el almacenamiento de objetos estándar para copiar datos de IBM Spectrum Protect Plus a Servidor de IBM Spectrum Protect, inicie sesión en el Centro de operaciones y siga el procedimiento para configurar agrupaciones de almacenamiento. Complete el proceso siguiendo los pasos para crear un servicio de agente objeto utilizando el asistente de Centro de operaciones.

### Antes de empezar

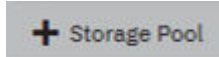
Antes de empezar, debe configurar las agrupaciones de almacenamiento para almacenamiento estándar o para la copia en cintas. Si copia en una cinta, debe configurar la agrupación de almacenamiento de memoria caché de datos fríos y, en el almacenamiento de objetos estándar, debe crear y configurar agrupaciones de almacenamiento según sea necesario. Para obtener instrucciones sobre cómo configurar la agrupación de almacenamiento de memoria caché de datos fríos, consulte [“Paso 1: Creación de una agrupación de almacenamiento en cintas y una agrupación de almacenamiento de memoria caché de datos fríos para copiar datos en cintas”](#) en la página 200.

### Procedimiento

1. Para crear una agrupación de almacenamiento de contenedores de directorios, siga estos pasos:
  - a) En la barra de menús del Centro de operaciones, pulse **Almacenamiento > Agrupaciones de almacenamiento**.



- b) En la página **Agrupaciones de almacenamiento**, haga clic en **Agrupación de almacenamiento**



- c) Realice los pasos del asistente **Añadir agrupación de almacenamiento**.

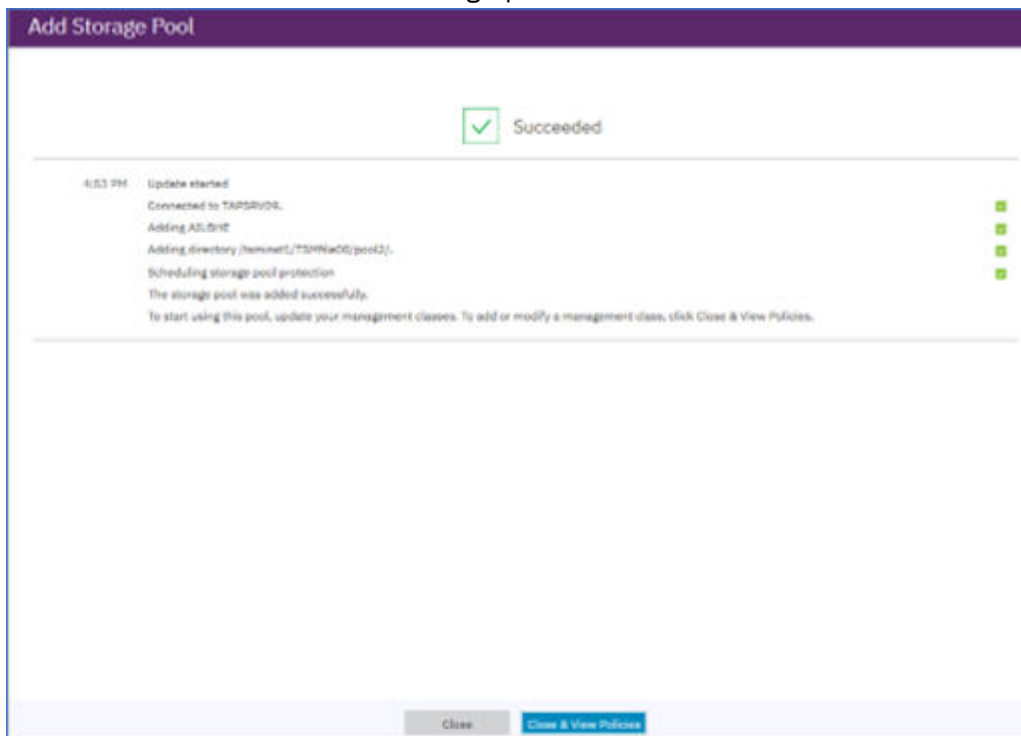
**Consejo:** Seleccione **Directorio** para el tipo de almacenamiento basado en contenedores y añada directorios con el icono +. Pulse **Siguiente** para continuar.

- d) Revise el resumen de **Proteger agrupación** y pulse **Siguiente**.

- e) Especifique una agrupación de desbordamiento que sea necesaria.

- f) Haga clic en **Añadir agrupación de almacenamiento** para completar la creación de la agrupación de almacenamiento.

Si la operación se ha realizado correctamente, verá un icono para indicar que se ha realizado correctamente con un resumen de la agrupación de almacenamiento.




2. En la página **Servicios > Políticas**, seleccione una política y haga clic en **Detalles**.

Policy Domain	Server	Clients	Mgmt Classes	Option Sets	Schedules	Default Mgmt Class	Backup Destination	Archive Destination	Migration
IBM_DEPLOY_CLIENT...	P9B-AIX1	0	1	0	0	IBM_DEPLOY_CLIENT		DEDUPPOOL	
JASON	P9B-AIX1	0	2	0	0	STANDARD	DEDUPPOOL		
P9B-AIX1_DATABA...	P9B-AIX1	0	4	0	1	BACKUP_DISK_KEEP30DAYS	DEDUPPOOL		
P9B-AIX1_DB2	P9B-AIX1	0	1	0	0	BACK_ARCH_DISK	DEDUPPOOL	DEDUPPOOL	

- Puede editar una política de dominio existente siguiendo estos pasos:
    - a) Actualice una o más clases de gestión para utilizar la nueva agrupación editando el campo **Destino de copia de seguridad** de la tabla.
    - b) Pulse **Guardar**.
  - O bien, puede crear un nuevo dominio ejecutando el mandato **define objectdomain**. Para obtener más información, consulte el paso anterior “Paso 2: Configuración de un dominio de políticas de objeto” en la página 202.
3. En la página **Detalles**, haga clic en **Conjunto de políticas**. Haga clic en el conmutador **Configurar** para que los conjuntos de políticas se puedan editar.

Management Class	Default	Backup Destination
COLD		(None)
STANDARD	✓	DEDUPPOOL

4. Cambie el Destino de copia de seguridad para la agrupación de almacenamiento recién creada, o

añada una nueva clase de gestión,  **Management Class** para que apunte a la nueva agrupación de almacenamiento.

5. Haga clic en **Activar**.
- Cambiar el conjunto de políticas activas puede dar como resultado la pérdida de datos. Se muestra un resumen de las diferencias entre el conjunto de políticas activas y el nuevo conjunto de políticas antes de que se realice el cambio.
6. Revise las diferencias entre las clases de gestión correspondientes en los dos conjuntos de políticas y tenga en cuenta las consecuencias en los archivos cliente. Los archivos cliente que están enlazados a las clases de gestión del conjunto de políticas actualmente activo se enlazan, después de la activación, a las clases de gestión con los mismos nombres del nuevo conjunto de políticas.
7. Identifique las clases de gestión del conjunto de políticas actualmente activo que no tiene contrapartidas en el nuevo conjunto de políticas, y tenga en cuenta las consecuencias en los archivos

cliente. Los archivos cliente que están enlazados a estas clases de gestión los gestiona, después de la activación, la clase de gestión predeterminada en el nuevo conjunto de políticas.

8. Si los cambios implementados por el conjunto de políticas son aceptables, seleccione la casilla de verificación **Entiendo que estas actualizaciones pueden causar pérdida de datos** y pulse **Activar**.

### Qué hacer a continuación

Cree y configure un cliente objeto para la agrupación o agrupaciones de almacenamiento que ha creado. Para obtener más información, consulte [“Paso 5: Adición y configuración de un cliente objeto para copiar datos”](#) en la página 209

### Paso 4: Adición de un agente objeto para copiar datos

Antes de copiar datos de IBM Spectrum Protect Plus a Servidor de IBM Spectrum Protect, debe añadir y configurar el agente objeto. Este paso es el cuarto paso en la configuración de IBM Spectrum Protect Plus con Servidor de IBM Spectrum Protect para archivar datos o copiar datos en el almacenamiento de objetos.

### Antes de empezar

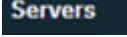
Asegúrese de que los pasos siguientes se han completado antes de empezar a crear el cliente objeto.

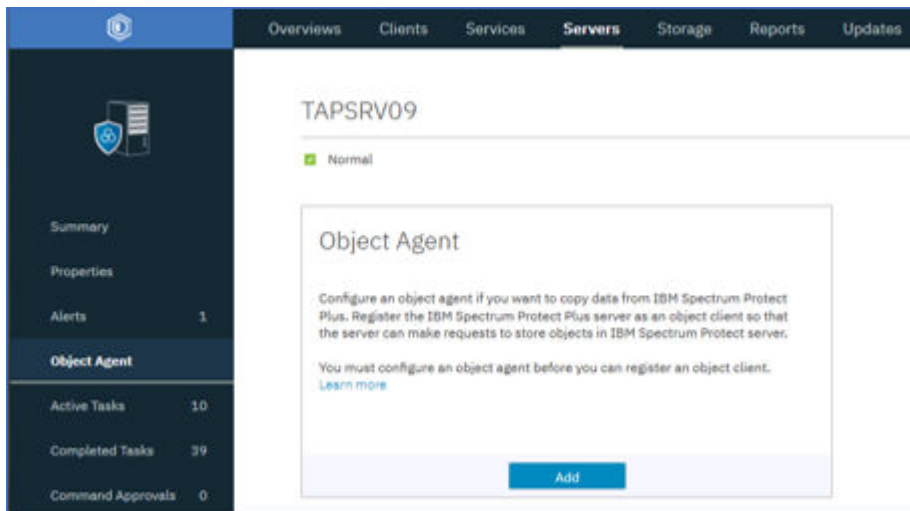
1. Asegúrese de que ha iniciado sesión en Servidor de IBM Spectrum Protect con un ID de usuario de instancia.
2. Asegúrese de que ha configurado las agrupaciones de almacenamiento para el almacenamiento estándar o para la copia en cinta. Para obtener instrucciones, consulte las secciones [“Paso 1: Creación de una agrupación de almacenamiento en cintas y una agrupación de almacenamiento de memoria caché de datos fríos para copiar datos en cintas”](#) en la página 200 o [“Paso 3: Configuración del almacenamiento de objetos estándar”](#) en la página 204.
3. Asegúrese de que ha creado un dominio de objetos.

### Acerca de esta tarea

Este procedimiento se basa en un entorno donde está instalado Servidor de IBM Spectrum Protect en un sistema operativo IBM AIX AIX Versión 7.2 TL 1 y SP 4 o posterior, que se ejecuta en un servidor IBM POWER8 o posterior. (ENLAZAR CON una versión anterior)

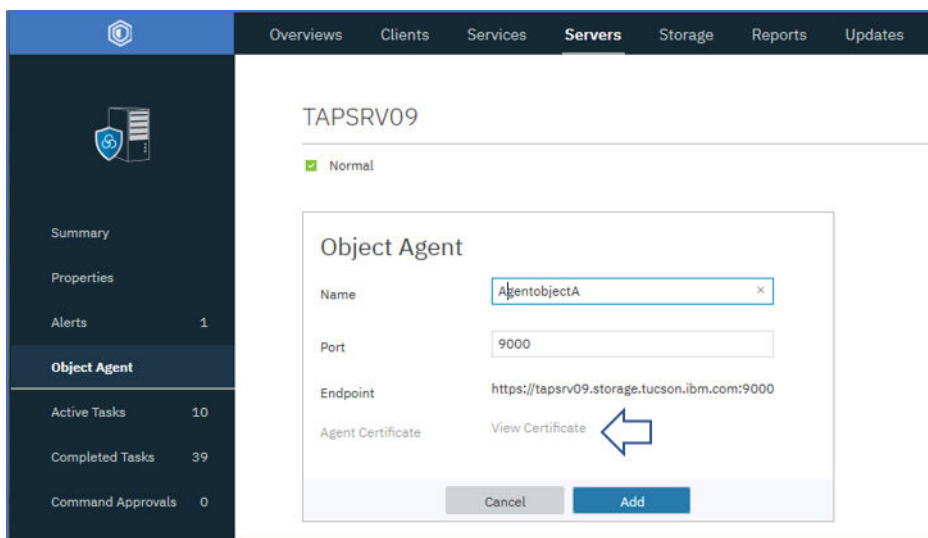
### Procedimiento

1. En la barra de menús del Centro de operaciones, haga clic en **Servidores** .
2. Seleccione un servidor y haga clic en **Detalles**.
3. En el panel de navegación, haga clic en **Agente objeto**; haga clic en **Añadir** para añadir un agente objeto.



**Consejo:** Si utiliza la línea de mandatos, ejecute el mandato **DEFINE SERVER** para crear un agente objeto. Especifique OBJECTAGENT=YES. Siga las instrucciones de la salida del mandato. Cuando se completan estas acciones, el servicio de agente objeto se inicia automáticamente en el sistema que está alojando Servidor de IBM Spectrum Protect.

4. Para autenticarse en el agente objeto, utilice el certificado que se genera.



5. Instale el servicio de agente objeto ejecutando el mandato que se puede copiar desde el asistente como en los ejemplos siguientes:

```
[root@servername-os: /]# /opt/tivoli/tsm/server/bin/spObjectAgent service install
/home/tsminst1/tsminst1/SPP0BJAGENT/spObjectAgent_SPP0BJAGENT_1500.config
2020-03-31 15:50:07.631021 I | Servicio del sistema instalado e iniciado como
nameportnumberobjectagentname
```

He aquí un ejemplo:

```
[root@p9b-aix1: /]# /opt/tivoli/tsm/server/bin/spObjectAgent service install
/home/tsminst1/tsminst1/SPP0BJAGENT/spObjectAgent_SPP0BJAGENT_1500.config
2020-03-31 15:50:07.631021 I | Servicio del sistema instalado e iniciado como
spoa9000SPP0BJAGENT
```

6. Complete la configuración iniciando un servicio de agente objeto ejecutando el mandato **startObjectAgent**. A continuación, se muestra un ejemplo para el agente objeto **AGENTOBJECTA**.

```
"/opt/tivoli/tsm/server/bin/spObjectAgent" service install
"/home/tsminst1/tsminst1/AGENTOBJECTA/spObjectAgent_AGENTOBJECTA_1500.config"
```

7. Configure el servicio de agente objeto para que se inicie automáticamente durante el inicio ejecutando un mandato similar al mandato siguiente para AIX:

```
spobj:2:once:/usr/bin/startsrc -s nameportnumberobjectagentname
```

A continuación se muestra un ejemplo:

```
spobj:2:once:/usr/bin/startsrc -s spoa9000SPPOBJAGENT
```

### Paso 5: Adición y configuración de un cliente objeto para copiar datos

Antes de poder copiar datos de IBM Spectrum Protect Plus a Servidor de IBM Spectrum Protect, debe configurar el cliente objeto. Este paso es el último paso en la configuración de Servidor de IBM Spectrum Protect para archivar y copiar datos con el Centro de operaciones.

#### Antes de empezar

Asegúrese de que los pasos siguientes se han completado antes de empezar a crear el cliente objeto.

1. Asegúrese de que ha iniciado sesión en Servidor de IBM Spectrum Protect con un ID de usuario de instancia.
2. Asegúrese de que las agrupaciones de almacenamiento para el almacenamiento estándar o para la copia en cinta están configuradas y listas. Para obtener instrucciones, consulte las secciones [“Paso 1: Creación de una agrupación de almacenamiento en cintas y una agrupación de almacenamiento de memoria caché de datos fríos para copiar datos en cintas”](#) en la página 200 o [“Paso 3: Configuración del almacenamiento de objetos estándar”](#) en la página 204.
3. Asegúrese de que se han creado un dominio de objetos y un agente objeto antes de empezar.

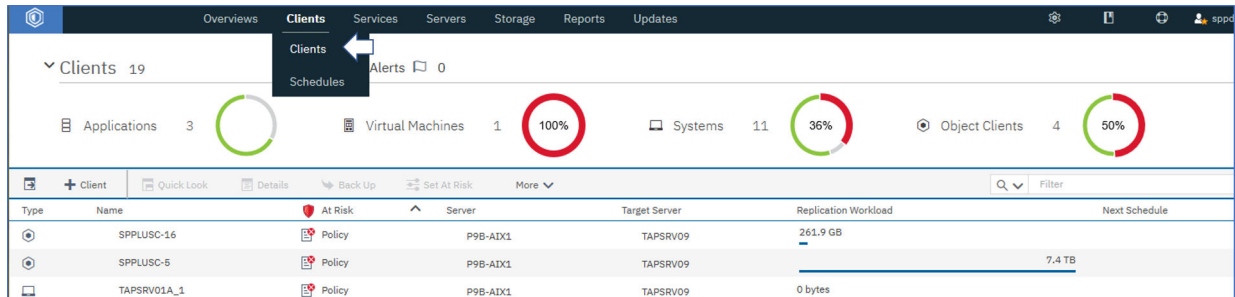
**Consejo:** Si crea un cliente objeto antes de crear el agente objeto correspondiente, el asistente **Añadir cliente** fuerza la creación del agente objeto.

#### Acerca de esta tarea

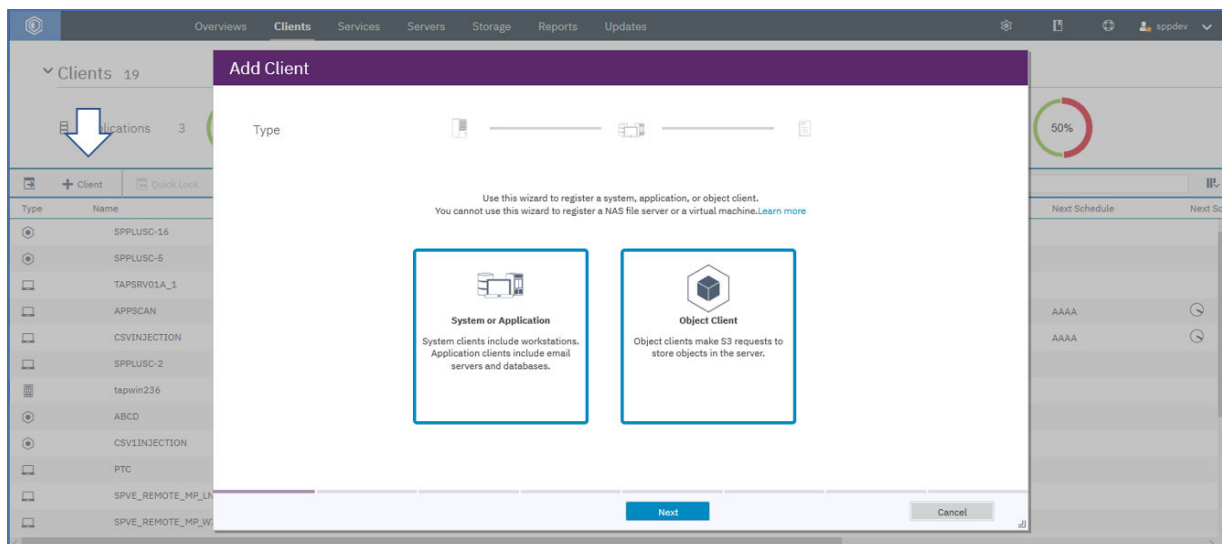
Este procedimiento se basa en un entorno donde está instalado Servidor de IBM Spectrum Protect en un sistema operativo IBM AIX Versión 7.2 TL 1 y SP 4 o posterior, que se ejecuta en un servidor IBM POWER8 o posterior.

#### Procedimiento

1. En la barra de menús del Centro de operaciones, pulse **Cientes**.



2. Haga clic en **Cliente** para añadir un cliente tal como se muestra.



3. Seleccione **Cliente objeto** y haga clic en **Siguiente** para iniciar el asistente **Añadir cliente**.

En las pantallas del asistente, se le pedirá que elija opciones y definiciones para el cliente que está configurando.

- También puede elegir habilitar la réplica para este cliente.
- Debe asignar un nombre de cliente y un nombre de contacto, y una dirección de correo electrónico para los informes que defina en el paso final del asistente.
- Debe asignar el dominio de políticas que ha configurado en el paso 2, [“Paso 2: Configuración de un dominio de políticas de objeto”](#) en la página 202.
- Puede definir los informes de riesgo para el cliente, como enviar un informe una vez al día a la dirección de correo electrónico que ha especificado.

4. Pulse **Añadir cliente**.

**Nota:**

Una vez que finaliza el proceso, se le proporciona el punto final para comunicarse con el agente objeto en el servidor, el ID de la clave de acceso, la clave de acceso secreta y el certificado para comunicarse de forma segura. Cuando IBM Spectrum Protect Plus es un cliente objeto, dirige solicitudes al punto final y utiliza esta información en forma de ID de clave de acceso, clave de acceso secreta y certificado seguro.

**Importante:** Asegúrese de que se guarda una copia de cada credencial en una ubicación segura.

**Consejo:** Si utiliza la línea de mandatos, ejecute el mandato **REGISTER NODE** para crear un cliente objeto. Especifique TYPE=OBJECTCLIENT. El script se ejecuta bajo el ID de usuario de instancia.

**Qué hacer a continuación**

Como paso siguiente, debe registrar el servidor de IBM Spectrum Protect como servidor de repositorio. Para obtener información sobre cómo hacer esto, consulte [“Registro de un servidor de repositorio como proveedor de almacenamiento de copias de seguridad”](#) en la página 210. Una vez que se ha completado, puede crear trabajos de política de SLA para copiar datos en el servidor de IBM Spectrum Protect para almacenamiento estándar o para el archivado en cintas.

**Registro de un servidor de repositorio como proveedor de almacenamiento de copias de seguridad**

Añadir y registrar un servidor de repositorio para permitir que IBM Spectrum Protect Plus copie 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 220 y [“Adición de un certificado”](#) en la página 221.

Para el release actual de IBM Spectrum Protect Plus, el servidor de repositorio debe ser un Servidor de 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 copiados. 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.

Los certificados se pueden obtener en el Centro de operaciones del Servidor de 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 copia se controlan por completo mediante políticas de SLA asociadas en IBM Spectrum Protect Plus. Los valores de retención del grupo de copias de Servidor de IBM Spectrum Protect no se utilizan para las operaciones de copia.

## Procedimiento

Para añadir y registrar un Servidor de 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 objeto 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 <a href="#">“Creación de una política de SLA para hipervisores, bases de datos y sistemas de archivos”</a> en la página 244.  Para modificar una política de SLA existente, consulte <a href="#">“Edición de una política de SLA”</a> en la página 255.

### Conceptos relacionados

[“Configuración para copiar o archivar datos en IBM Spectrum Protect”](#) en la página 198


Si tiene previsto copiar o archivar datos de IBM Spectrum Protect Plus en un Servidor de IBM Spectrum Protect, hay tres configuraciones posibles. La elección de cuál se debe configurar depende de qué escenario se aplica a sus necesidades de protección de datos. Para cada escenario, hay pasos necesarios en los entornos de IBM Spectrum Protect Plus y Servidor de IBM Spectrum Protect para completar la configuración.

### 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 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 réplica y copia 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).

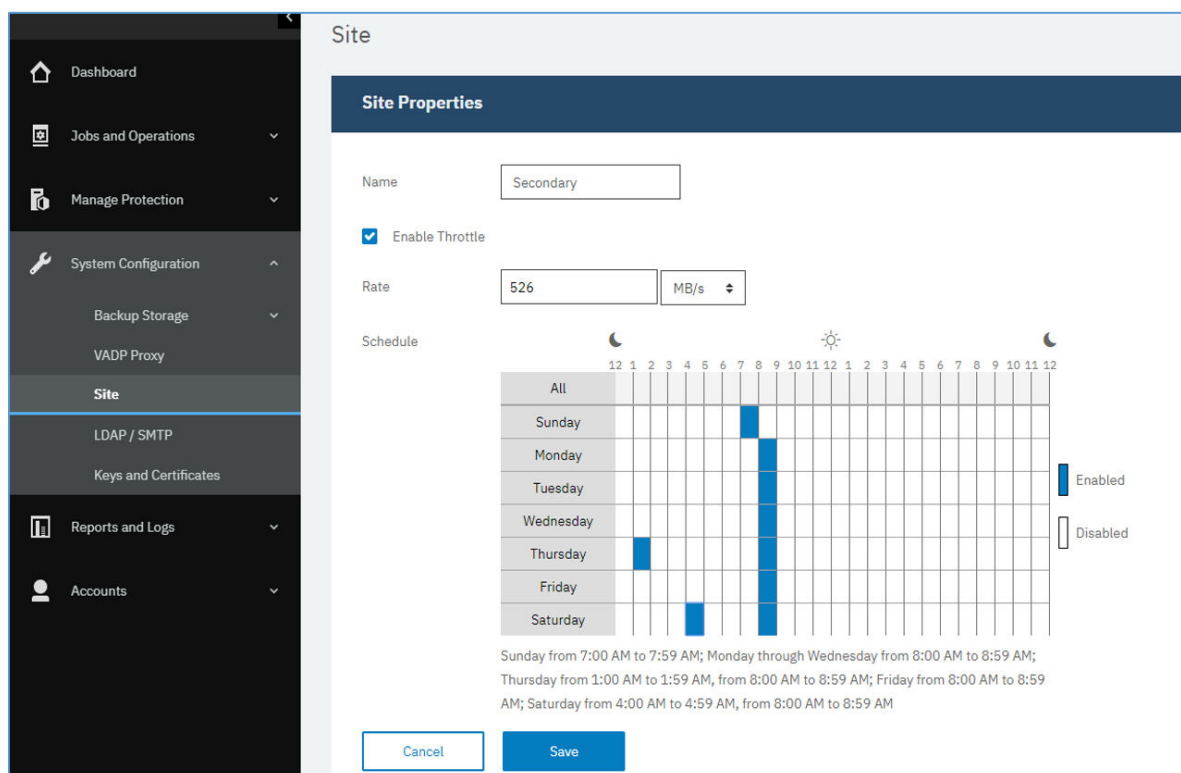


Figura 20. Habilitación de distintos índices de regulación para diferentes horas para mejorar el rendimiento

- 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 réplica y copia 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).

**Site Properties**

Name:

☒ Enable Throttle

Rate:  MB/s

Schedule

	12	1	2	3	4	5	6	7	8	9	10	11	12
All													
Sunday													
Monday													
Tuesday													
Wednesday													
Thursday													
Friday													
Saturday													

Sunday from 7:00 AM to 7:59 AM; Monday through Wednesday from 8:00 AM to 8:59 AM; Thursday from 1:00 AM to 1:59 AM, from 8:00 AM to 8:59 AM; Friday from 8:00 AM to 8:59 AM; Saturday from 4:00 AM to 4:59 AM, from 8:00 AM to 8:59 AM

*Figura 21. 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 543](#)

Con IBM Spectrum Protect Plus, puede utilizar un servidor Lightweight Directory Access Protocol (LDAP) para gestionar usuarios. Cuando crea una cuenta de usuario de LDAP, puede añadir la cuenta de usuario a un grupo de usuarios.

[“Planificación de un informe” en la página 530](#)

Puede planificar informes 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 sAMAccountName 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 543](#)

Con IBM Spectrum Protect Plus, puede utilizar un servidor Lightweight Directory Access Protocol (LDAP) para gestionar usuarios. Cuando crea una cuenta de usuario de LDAP, puede añadir la cuenta de usuario a un grupo de usuarios.

## 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 530](#)


Puede planificar informes 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.

## 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 autenticación	Información de inicio de sesión
<b>IBM Spectrum Protect Plus</b>	Para iniciar sesión como un usuario de IBM Spectrum Protect Plus con privilegios SUPERUSER, 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.
<b>Sistema</b>	Para iniciar la sesión como un usuario del sistema, especifique la contraseña de serveradmin. La contraseña predeterminada es sppDP758-SysXyz. Se le solicitará que cambie esta contraseña durante el primer inicio de sesión. Se imponen ciertas reglas al crear una contraseña nueva. Para obtener más información, consulte las reglas de requisitos de contraseña en <a href="#">“Iniciar IBM Spectrum Protect Plus” en la página 167</a> .

### Qué hacer a continuación

Revise la configuración del dispositivo virtual de IBM Spectrum Protect Plus.

### Conceptos relacionados

[“Requisitos del sistema” en la página 23](#)

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 537](#)

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.

## Gestión de claves y certificados

---

Los recursos de nube y los servidores de repositorio requieren credenciales que sirvan como destinos de copia. 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 copia y permiten que IBM Spectrum Protect Plus acceda a ellos. Algunos destinos de copia 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 copia, 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

Puede añadir una clave SSH para proporcionar credenciales para recursos basados en Linux en máquinas virtuales gestionadas por vCenter y Hyper-V, así como servidores de aplicaciones Oracle, Db2 y MongoDB. Las claves SSH ayudan a proporcionar una conexión segura entre IBM Spectrum Protect Plus y los recursos de destinos para las operaciones de restauración y de indexación de archivos.

### 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.
- La cuenta de usuario en el recurso de destino que se utiliza para generar el par de claves SSH debe tener privilegios **sudo**. Esta cuenta, que se asignará a IBM Spectrum Protect Plus, se conoce como el agente de usuario de IBM Spectrum Protect Plus (sppagent).

- Si el entorno incluye máquinas virtuales gestionadas por vCenter, asegúrese de que están instaladas las últimas herramientas de VMware.

## Procedimiento

Para añadir una clave, complete los pasos siguientes:

1. En el recurso de destino, genere una clave SSH utilizando el mandato `ssh-keygen` con la cuenta de usuario que se asignará a IBM Spectrum Protect Plus. Esta cuenta debe tener privilegios **sudo**. Por ejemplo, en un servidor de Oracle, especifique el siguiente mandato en el terminal y siga las instrucciones:

```
ssh-keygen
```

Si utiliza los valores predeterminados, se crean dos archivos en el directorio especificado: `id_rsa.pub` es la clave pública y `id_rsa` es la clave privada.

2. Cuando se le solicite, especifique el nombre de archivo en el que se guardará la clave, especifique un directorio y un nombre de archivo. Si no especifica un directorio y un nombre de archivo, se utiliza el valor predeterminado:

```
/home/usuario_privilegiado/.ssh/id_rsa
```

donde *usuario\_privilegiado* es la cuenta asignada a IBM Spectrum Protect Plus, `sppagent`. Si ya existe una clave con un nombre predeterminado, esto se indicará con un mensaje siguiente visualizado. Tenga cuidado de no sobrescribir las claves preexistentes si están en uso. Pulse **N** para entrar un archivo distinto en el que guardar la clave.

```
/home/<priveleged user>/.ssh/id_rsa already exists.  
Overwrite (y/n)?
```

Este procedimiento se basa en la asunción de que la clave se guarda en la ubicación predeterminada utilizando el nombre de archivo predeterminado (`id_rsa`). Si el archivo de claves se crea utilizando un nombre de archivo diferente, utilice el nombre de archivo en los pasos siguientes.

3. Proporcione una frase de contraseña y pulse Intro. De lo contrario, pulse simplemente Intro para que no haga frase de contraseña.
4. Si se suministra una frase de contraseña, escríbala de nuevo. Pulse la tecla Intro.
5. Copie el contenido de la clave `id_rsa.pub` en el archivo `authorized_keys`. Si ya existe el archivo, añada la clave pública al archivo `authorized_keys`.

```
cat ~/.ssh/id_rsa.pub >> ~/.ssh/authorized_keys
```

6. Asigne los privilegios necesarios al archivo `authorized_keys` emitiendo el mandato `chmod 600`.

```
chmod 600 ~/.ssh/authorized_keys
```

7. Edite el archivo `/etc/ssh/sshd_config` para establecer el valor `PubkeyAuthentication` en `yes` utilizando un editor de texto. Para asegurarse de que el valor no se ha comentado, elimine el signo de almohadilla (`#`) si aparece al principio de la línea.

```
sudo vi /etc/ssh/sshd_config
```

```
...  
PubkeyAuthentication yes  
...
```

8. Reinicie el servicio SSH en el recurso de destino.

```
systemctl restart sshd
```

9. En el panel de navegación de IBM Spectrum Protect Plus, pulse **Configuración del sistema > Claves y certificados**.

10. En la sección **Claves de acceso**, pulse **Añadir clave SSH**.

## 11. Complete los campos en el panel **Propiedades de clave SSH**:

### Nombre

Especifique un nombre significativo para identificar la clave SSH.

### Usuario

Especifique la cuenta de usuario que está asociada con el recurso de destino y la clave SSH. Esta es la cuenta de usuario utilizada para generar las claves públicas y privadas en los pasos anteriores.

### Cifrado

Seleccione este recuadro si se ha proporcionado una frase de contraseña al generar la clave pública y privada.

### Frase de contraseña

Este recuadro solo se visualiza si se selecciona la casilla de verificación **Cifrado**. Si se ha proporcionado una frase de contraseña al generar la clave pública y privada, proporcione la frase de contraseña en este recuadro.

### Clave privada

Copie y pegue la clave privada en este recuadro. Será la clave contenida en el archivo `id_rsa` en el recurso de destino. El archivo es similar al ejemplo siguiente:

```
cat ~/.ssh/id_rsa
```

```
-----BEGIN OPENSSH PRIVATE KEY-----
ZRYtuinJaHx2mKgW4LnFqz1yAIIq5Amasi/J8/AAAFiFiP4GZYj+BmAAAAB3NzaC1yc2
...
Q5ZqZ1Ec8N7dsAAAANDG9vckBVYnVudHVWQgECAwQFBg==
-----END OPENSSH PRIVATE KEY-----
```

## 12. Pulse **Guardar**.


La clave se muestra en la tabla **Claves SSH** y se puede seleccionar cuando se utiliza una característica que requiere credenciales para acceder a un recurso con 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.

## 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.

### Antes de empezar

Asegúrese de que haya un certificado disponible. Las notas técnicas siguientes proporcionan información introductoria para utilizar certificados con IBM Spectrum Protect Plus:

### HTTPS

Nota técnica 739663 proporciona información sobre el uso de un certificado HTTPS que emite la entidad emisora de certificados de Microsoft. Sin embargo, puede utilizar otra entidad emisora de certificados (CA).

## LDAP

Nota técnica 791677 proporciona información sobre el uso de un certificado LDAP.

En los certificados HTTPS, se admiten los certificados codificados PEM con las extensiones .cer o .crt.

En los certificados LDAP, 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.

## Procedimiento

Para cargar un certificado SSL, complete los pasos siguientes:

1. Desde un navegador soportado, especifique el URL siguiente para la consola de administración:

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

Donde *HOSTNAME* es la dirección IP de la máquina virtual en la que se despliega la consola de administración.

2. En la ventana de inicio de sesión, seleccione uno de los tipos de autenticación siguientes en la lista

### Tipo de autenticación:

Tipo de autenticación	Información de inicio de sesión
<b>IBM Spectrum Protect Plus</b>	Para iniciar la sesión como un usuario de IBM Spectrum Protect Plus con privilegios SUPERUSER, especifique el nombre de usuario y la contraseña del administrador.
<b>Sistema</b>	Para iniciar la sesión como un usuario del sistema, especifique la contraseña de serveradmin. La contraseña predeterminada es sppDP758-SysXyz. Se le solicitará que cambie esta contraseña durante el primer inicio de sesión. Se imponen ciertas reglas al crear una contraseña nueva. Para obtener más información, consulte las reglas de requisitos de contraseña en <a href="#">“Iniciar IBM Spectrum Protect Plus”</a> en la <a href="#">página 167</a> .

3. Pulse **Gestión de certificados**.
4. Haga clic en el tipo de certificado: **HTTP** o **LDAP/Hyper-V**.
5. Pulse **Examinar** y seleccione el certificado que desea cargar.
6. Haga clic en **Cargar certificado SSL para tipo de certificado**.
7. Cuando la carga se haya completado, haga clic en **Gestión del sistema > Reinicie IBM Spectrum Protect Plus**.

## 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 autenticación	Información de inicio de sesión
<b>IBM Spectrum Protect Plus</b>	Para iniciar la sesión como un usuario de IBM Spectrum Protect Plus con privilegios SUPERUSER, especifique el nombre de usuario y la contraseña del administrador.
<b>Sistema</b>	Para iniciar la sesión como un usuario del sistema, escriba la contraseña de <code>serveradmin</code> . La contraseña predeterminada es <code>sppDP758-SysXyz</code> . Se le solicitará que cambie esta contraseña durante el primer inicio de sesión. Se imponen ciertas reglas al crear una contraseña nueva. Para obtener más información, consulte las reglas de requisitos de contraseña en <a href="#">“Iniciar IBM Spectrum Protect Plus”</a> en la <a href="#">página 167</a> .

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. Reinicie el dispositivo IBM Spectrum Protect Plus desde la consola de administración.
6. Una vez reiniciado el dispositivo IBM Spectrum Protect Plus, vea el huso horario actual. Seleccione **Información sobre el producto** desde la página principal de la consola de administración y verifique el huso horario actualizado.

## 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-SysXyz`. Se le solicitará que cambie esta contraseña durante el primer inicio de sesión. Se imponen ciertas reglas al crear una contraseña nueva. Para obtener más información, consulte las reglas de requisitos de contraseña en [“Iniciar IBM Spectrum Protect Plus”](#) en la [página 167](#).

### 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-SysXYZ`. Se le solicitará que cambie esta contraseña durante el primer inicio de sesión. Se imponen ciertas reglas al crear una contraseña nueva. Para obtener más información, consulte las reglas de requisitos de contraseña en [“Iniciar IBM Spectrum Protect Plus” en la página 167](#).

### 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 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 sesión en el dispositivo virtual de IBM Spectrum Protect Plus utilizando el ID de usuario `serveradmin` y acceda a la línea de mandatos. Ejecute el siguiente mandato:

```
# sudo bash
```

2. Abra el puerto 9000 en el cortafuegos ejecutando 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 se va a probar, complete 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 **Ejecutar**.

Si no se puede establecer una conexión, se visualiza la condición de error, junto con las posibles causas y acciones.

8. Detenga la herramienta ejecutando el mandato siguiente en la línea de mandatos:

```
ctl-c
```

9. Proteja el entorno de almacenamiento reconfigurando el cortafuegos. Ejecute 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 del cortafuegos con iptables** aquí: [https://www.ibm.com/support/knowledgecenter/en/STXKQY\\_5.0.3/com.ibm.spectrum.scale.v5r03.doc/bl1adv\\_firewallportopenexamples.htm](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 **pvdisk** 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-SysXyz`. Se le solicitará que cambie esta contraseña durante el primer inicio de sesión. Se imponen ciertas reglas al crear una contraseña nueva. Para obtener más información, consulte las reglas de requisitos de contraseña en [“Iniciar IBM Spectrum Protect Plus”](#) en la página 167.

### 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 IBM Spectrum Protect Plus, emita los siguientes mandatos:

```
sudo bash
```

Pulse la tecla Intro.

```
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-SysXYZ`. Se le solicitará que cambie esta contraseña durante el primer inicio de sesión. Se imponen ciertas reglas al crear una contraseña nueva. Para obtener más información, consulte las reglas de requisitos de contraseña en [“Iniciar IBM Spectrum Protect Plus” en la página 167](#).

### 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 -l**.
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 **pvccreate /dev/sdd1**.
5. Para ver el nuevo volumen físico de /dev/sdd1, emita el mandato **pvddisplay**.
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
```

## Configuración de las preferencias globales

Como administrador, puede configurar preferencias que se aplican a todas las operaciones de IBM Spectrum Protect Plus en el panel **Preferencias globales**.

### Antes de empezar

Debe tener credenciales de administrador para configurar las preferencias globales.

Puede cambiar la preferencia en la categoría **Integraciones con otros productos de almacenamiento** en cualquier momento.



**Atención:** Aunque puede modificar la preferencia en la categoría **Integraciones con otros productos de almacenamiento**, modifique todas las preferencias solo si es absolutamente necesario y solo en la dirección de soporte de IBM. La modificación de preferencias globales puede afectar al entorno de almacenamiento. Las preferencias que requieren consulta con el soporte de IBM están en las siguientes categorías: **Aplicación, General, Trabajo, Registro, Protección y Seguridad**.

### Acerca de esta tarea

Todos los cambios que realice en los valores predeterminados del parámetro se aplican a todas las operaciones de IBM Spectrum Protect Plus al guardar los cambios.

### Procedimiento


Para editar los valores para cualquier parámetro y aplicarlos globalmente, complete los pasos siguientes:

1. En el panel de navegación, pulse **Configuración del sistema > Preferencias globales**.
2. Para habilitar el acceso a IBM Spectrum Protect Operations Center desde IBM Spectrum Protect Plus, edite la preferencia en la categoría **Integraciones con otros productos de almacenamiento**. El valor predeterminado de la preferencia se muestra en la figura siguiente:

Puede editar la preferencia siguiente:

#### URL del Centro de operaciones de IBM Spectrum Protect

La dirección IP de IBM Spectrum Protect Operations Center. El Centro de operaciones ofrece acceso a web y a móvil a la información de estado sobre el entorno de IBM Spectrum Protect.

Cuando se establece esta preferencia, el icono IBM Spectrum Protect  está activo en la barra de menús de IBM Spectrum Protect Plus. Cuando se establece inicialmente el URL para esta preferencia o si lo cambia, debe cerrar sesión y volver a iniciar sesión para que la preferencia entre en vigor en la interfaz de usuario.

El URL se crea durante el proceso de instalación de Centro de operaciones. Para obtener el URL de Centro de operaciones, póngase en contacto con el administrador del sistema de IBM Spectrum Protect.

3. Para aplicar las preferencias de la aplicación global, edite los valores en la categoría **Aplicación**. Los valores predeterminados de las preferencias se muestran en la figura siguiente:

## Application

Enable SQL Server databases restored in test mode eligible for backup

☐

Maximum volume size for backup target LUNs on Windows (TB)

Maximum backup retries(k8s)

Maximum concurrent servers running backups

Allow SQL database backup when transaction log backup chain is broken

☐

Rename SQL data and log files when database is restored in production mode with new name

☐

Puede editar las preferencias de aplicación siguientes:

### **Habilitar las bases de datos de SQL Server restauradas en la modalidad de prueba elegibles para la copia de seguridad**

Copia de seguridad de las bases de datos de SQL Server que se restauraron en modalidad de prueba. Cuando se selecciona esta opción, las bases de datos de SQL Server que se restauraron en la modalidad de prueba están disponibles para la selección en el panel Copia de seguridad de SQL o el asistente de copia de seguridad ad hoc.

### **Tamaño de volumen máximo para los LUN de destino de copia de seguridad en Windows (TB)**

El tamaño máximo del almacenamiento para un destino de copia de seguridad.

### **Número máximo de reintentos de copia de seguridad (k8)**

El número máximo de veces que IBM Spectrum Protect Plus reintenta las sesiones de copia de seguridad para un trabajo de copia de seguridad de copia que contiene varias reclamaciones de volumen persistente (PVC).

Cuando hay varias PVC implicadas en el mismo trabajo de copia de seguridad de copia, IBM Spectrum Protect Plus ejecuta las operaciones de copia de seguridad como trabajos paralelos. Para ayudar a impedir que las sesiones de copia de seguridad superen el tiempo de espera debido a problemas de conexión, especifique el número máximo de veces que IBM Spectrum Protect Plus reintenta las conexiones.

Si se alcanza el número máximo de reintentos y siguen existiendo errores de conexión, solo se informará de las copias de seguridad de PVC que formaban parte de las sesiones con errores.

### **Número máximo de servidores ejecutando copias de seguridad simultáneamente**

El número máximo de servidores de aplicaciones simultáneos por sesión de copia de seguridad.

### **Permitir la copia de seguridad de base de datos SQL cuando se rompe la cadena de copia de seguridad del registro de transacciones**

Ejecute un trabajo de copia de seguridad de base de datos cuando IBM Spectrum Protect Plus detecta una interrupción en la cadena de copia de seguridad del registro para una base de datos.

### **Cambiar el nombre de los archivos de registro y datos de SQL cuando se restaura la base de datos en modalidad de producción con un nombre nuevo**

Cambie el nombre de los archivos de registro y datos de la base de datos SQL asociada durante un trabajo de restauración de producción o de prueba. Este campo solo se aplica cuando se

proporciona un nombre de base de datos nuevo durante un trabajo de restauración de base de datos SQL.

4. Para aplicar preferencias generales, edite los valores de la categoría **General**. Los valores predeterminados de las preferencias se muestran en la figura siguiente:

General	
Access log retention (days)	<input type="text" value="30"/>
Tools working folder on Linux guest	<input type="text" value="/tmp"/>
Tools working folder on Windows guest	<input type="text" value="c:\ProgramData"/>
Linux/AIX Clients Port (SSH) used for application and file indexing	<input type="text" value="22"/>
Windows Clients Port (WinRM) used for application and file indexing	<input type="text" value="5985"/>
IBM Spectrum Protect Plus Server IP Address	<input type="text"/>

Puede editar las siguientes preferencias generales:

**Retención del registro de acceso (días)**

Especifique el número de días que debe retenerse el registro de acceso.

**Carpeta de trabajo Herramientas en el invitado de Linux**

La carpeta de trabajo para herramientas en los invitados de máquina virtual de Linux.

**Carpeta de trabajo Herramientas en el invitado de Windows**

La carpeta de trabajo para herramientas en los invitados de máquina virtual de Windows.

**Puerto de clientes Linux/AIX (SSH) utilizado para la indexación de archivos y aplicaciones**

El puerto SSH que se utiliza para la indexación de archivos y aplicaciones en clientes de Linux y AIX.

**Puerto de clientes de Windows (WinRM) utilizado para la indexación de archivos y aplicaciones**

El puerto Windows Remote Management (WinRM) que se utiliza para la indexación de archivos y aplicaciones en clientes de Windows.

**Dirección IP del servidor IBM Spectrum Protect Plus**

La lista de direcciones IP disponibles para el servidor IBM Spectrum Protect Plus. Las direcciones IP se utilizan para la comunicación entre los proxies VADP y el servidor IBM Spectrum Protect Plus. Las direcciones también se utilizan para la comunicación de agente remoto.

5. Para aplicar preferencias de trabajo o de registro, edite los valores en las categorías **Trabajo** o **Registro**. Los valores predeterminados de las preferencias se muestran en la figura siguiente:



**Job**

Job log retention (days)

60

Job notification status

failed

**Logging**

Enable logging IBM Spectrum Protect Plus alerts to the system

☐

log

Puede editar las siguientes preferencias de trabajo y de registro:

**Retención de registro de trabajo (días)**

El número de días que se deben retener los registros de trabajo antes de que se supriman los registros.

**Estado de notificación de trabajo**

El nivel de estado para enviar alertas. Las alertas se envían cuando se completa un trabajo con el estado especificado. Por ejemplo, si el estado de la notificación de trabajo es **fallido**, cuando se notifica el estado fallido para un trabajo, se envía una alerta.

**Habilite el registro de alertas de IBM Spectrum Protect Plus en el registro del sistema**

Incluya las alertas generadas por IBM Spectrum Protect Plus en el registro del sistema. Después de habilitar esta característica, puede buscar en el registro del sistema para encontrar alertas.

6. Para aplicar preferencias de protección, edite los valores en la categoría **Protección**. Los valores predeterminados de las preferencias se muestran en la figura siguiente:

Protection	
Number of seconds to wait before checking connection	1000
Number of times to check for valid connection	0
Temporary folder for file index zip files	/data2/filecatalog
Temporary folder for file indexing on Windows server	
Group VMs by	Count
Number of VMs in group	1
Force the removal of replication relationship for last remaining snapshot	<input type="checkbox"/>
Target free space error (percentage)	20
Target free space warning (percentage)	30
Catalog object update count	50
Virtual machine backup status update interval (seconds)	300
VADP proxy uses only HotAdd transport mode	<input type="checkbox"/>
VM group size (GB)	5120
vSnap auto disable deduplication when DDT size reaches resource limit	<input checked="" type="checkbox"/>
vSnap DDT size limit as percentage of total memory cache	80
vSnap DDT size limit in GB	50
Used space threshold on datastore or a volume before backup cannot take snapshots of a VM (percentage)	95
Backup wait timeout (seconds)	600
VMware communication timeout (seconds)	300

Puede editar las preferencias de protección siguientes:

#### Número de segundos a esperar hasta comprobar la conexión

La cantidad de tiempo que IBM Spectrum Protect Plus espera antes de comprobar la conexión con un objeto en la nube.

#### Número de veces que hay que comprobar si hay una conexión válida

El número de veces que IBM Spectrum Protect Plus comprueba una conexión disponible.

#### Carpeta temporal para archivos zip de índice de archivo

La carpeta temporal para almacenar los archivos comprimidos (.zip) que contienen los metadatos para la indexación. Cuando se completa la indexación, se suprimen los archivos.

#### Carpeta temporal para la indexación de archivos en el servidor Windows

La carpeta temporal para almacenar los archivos comprimidos (.zip) que contienen los metadatos para la indexación del servidor Windows. Cuando se completa la indexación, se suprime la carpeta.

#### Agrupar las MV por

Las máquinas virtuales se pueden agrupar juntas. El grupo se puede definir mediante un recuento de las máquinas virtuales incluidas en el grupo o el tamaño de las máquinas virtuales incluidas en el grupo.

#### Número de MV en el grupo

Para la agrupación de máquinas virtuales, hay cuatro grupos de máquinas virtuales disponibles y cada grupo de máquinas virtuales puede tener un máximo de cinco máquinas virtuales. Cada grupo corresponde a un volumen de destino (secuencia de datos). Se puede agrupar un máximo de 20 MV (cuatro secuencias de datos) a la vez en función de los cálculos de tamaño.

#### Forzar la eliminación de la relación de réplica para la última instantánea restante

Elimine una relación de réplica existente para la última instantánea restante que está configurada para que caduque y se bloquee.

### **Error de espacio libre en destino (porcentaje)**

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.

### **Aviso de espacio libre en destino (porcentaje)**

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.

### **Recuento de actualizaciones de objetos de catálogo**

El recuento que puede establecer para limitar el número de objetos que se consultan y se actualizan en el catálogo. Por ejemplo, si el catálogo incluye 100 objetos y el recuento de actualizaciones es 20, IBM Spectrum Protect Plus actualiza el catálogo en cinco iteraciones.

### **Intervalo de actualizaciones de estado de copia de seguridad de máquina virtual (segundos)**

La frecuencia con la que se actualizan los mensajes sobre el progreso de la transferencia de datos en el registro de trabajo.

### **El proxy VADP solo utiliza la modalidad de transporte HotAdd**

Utilice el método de transporte de disco virtual HotAdd para conectar el dispositivo virtual VMware IBM Spectrum Protect Plus con proxies VADP. Si esta opción está habilitada, los proxies VADP solo utilizarán HotAdd sin retroceder a una modalidad de transporte alternativa.

### **Tamaño de grupo de máquinas virtuales (GB)**

El tamaño, en gigabytes (GB), de grupos de máquinas virtuales.

### **vSnap inhabilita automáticamente la deduplicación cuando el tamaño de DDT alcanza el límite de recursos**

La tabla de deduplicación (DDT) está habilitada de forma predeterminada. Cuando se supera cualquiera de los límites de umbral definidos por el espacio de disco (gigabytes) o el porcentaje, se inhabilita la deduplicación de datos y se visualiza una alerta.

### **Límite de tamaño de DDT de vSnap DDT como porcentaje de la memoria caché total**

El umbral como porcentaje de la tabla de deduplicación de (DDT) vSnap comparado con la memoria caché total. La DDT se inhabilita cuando la opción de inhabilitación automática de vSnap está seleccionada y se excede el umbral definido.

### **Límite de tamaño de DDT de vSnap en GB**

El umbral, en gigabytes (GB), de la DDT de vSnap. La DDT se inhabilita cuando la opción de inhabilitación automática de vSnap está seleccionada y se excede el umbral definido.

### **El umbral de espacio utilizado en el almacén de datos o un volumen antes de la copia de seguridad no puede tomar instantáneas de una máquina virtual (porcentaje)**

El porcentaje de espacio utilizado en un almacén de datos o un volumen que es el umbral antes de que se tomen las instantáneas de una máquina virtual para la copia de seguridad.

### **Tiempo de espera de copia de seguridad (segundos)**

La cantidad de tiempo que IBM Spectrum Protect Plus espera a que finalice un trabajo de copia de seguridad antes de iniciar otro trabajo de copia de seguridad. Si el trabajo de copia de seguridad no finaliza en el periodo de espera, el trabajo supera el tiempo de espera y se inicia el siguiente trabajo.

### **Tiempo de espera de conexión de VMware (segundos)**

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 solo a hipervisores de VMware.

7. Para aplicar una preferencia de seguridad, edite el valor en la categoría **Seguridad**. El valor predeterminado de la preferencia se muestra en la figura siguiente:

Set Minimum Password Length (characters)

8

Puede editar la preferencia de seguridad siguiente:

### Establecer longitud mínima de contraseña (caracteres)

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.

## Eliminación del entorno de demostración

El dispositivo IBM Spectrum Protect Plus incluye un servidor vSnap incorporado que se denomina localhost, un sitio para fines de demostración denominado Demo y una política de SLA asociada también llamada Demo. Para entornos de producción más grandes, no utilice el servidor vSnap incorporado. En su lugar, utilice uno o más servidores vSnap autónomos. La política de SLA de Demo, el sitio Demo y el servidor vSnap incorporado, colectivamente como entorno Demo, se pueden eliminar de forma segura para conservar espacio de disco.

### Antes de empezar

Para los dispositivos IBM Spectrum Protect Plus que están en producción, haga una copia de seguridad de la aplicación de IBM Spectrum Protect Plus. Para obtener instrucciones, consulte [“Copia de seguridad de la aplicación de IBM Spectrum Protect Plus”](#) en la [página 505](#). Para los nuevos despliegues, no es necesario hacer copia de seguridad de la aplicación.

Verifique que los datos del servidor vSnap de localhost no son necesarios.


Asegúrese de que se despliega al menos un servidor vSnap autónomo como destino de copia de seguridad.






### Acerca de esta tarea

Cuando se despliega, un dispositivo IBM Spectrum Protect Plus tiene seis discos duros virtuales. Cuando elimina la configuración de Demo y el servidor vSnap de localhost del dispositivo IBM Spectrum Protect Plus, puede eliminar almacenamiento mediante la eliminación de dos de los discos duros virtuales asociados.

Debe seguirse el procedimiento de este tema para eliminar el entorno de Demo de IBM Spectrum Protect Plus.

### Procedimiento

1. Inhabilite las políticas de SLA que se asignan al entorno de Demo completando los pasos siguientes:
  - a) En un navegador soportado, inicie sesión en la interfaz de usuario de IBM Spectrum Protect Plus.
  - b) Vea los trabajos que se han asignado al SLA de demostración. En el panel de navegación, pulse **Trabajos y operaciones**, a continuación, pulse la pestaña **Planificación**. Localice los trabajos que siguen la pauta de nomenclatura *Nombre\_Trabajo\_Demo*, donde *Nombre\_Trabajo* es el nombre del trabajo. Esta pauta de nomenclatura indica que se utiliza el SLA de demostración.
  - c) Ponga en pausa la planificación para todos los trabajos de demostración. Haga clic en el icono del menú de acciones  y seleccione **Pausar planificación** para todos los trabajos que finalicen en *\_Demo*.
2. Suprima el SLA de demostración completando los pasos siguientes:

- a) En el panel de navegación, haga clic en **Gestionar protección > Descripción general de política**. Desplácese hasta la tabla en el panel Políticas de SLA y localice la política Demo.
  - b) Pulse el icono Suprimir  junto al SLA de Demo.
  - c) Especifique el código en el cuadro de diálogo **Confirmar** y haga clic en **Aceptar**.
3. Suprima el almacenamiento de disco vSnap de localhost completando los pasos siguientes:
- a) En el panel de navegación, haga clic en **Configuración del sistema > Almacenamiento de copias de seguridad > Disco**. Localice el almacenamiento de vSnap de localhost que se ha asignado al sitio de demostración.
  - b) Pulse el icono Suprimir  junto al almacenamiento de vSnap de localhost.
  - c) Especifique el código en el cuadro de diálogo **Confirmar** y haga clic en **SUPRIMIR**.
4. Suprima el sitio de demostración completando los pasos siguientes:
- a) En el panel de navegación, pulse **Configuración del sistema > Sitio**. Localice el sitio que se denomina Demo.
  - b) Pulse el icono Suprimir  junto al sitio de demostración.
  - c) Pulse **Sí** en el cuadro de diálogo **Confirmar** para completar la eliminación del sitio de demostración.
5. Elimine la identidad LocalvSnapAdmin completando los pasos siguientes:
- a) En el panel de navegación, pulse **Cuentas > Identidad**.
  - b) Pulse el icono Suprimir  junto a la identidad LocalvSnapAdmin.
  - c) Pulse **Sí** en el cuadro de diálogo **Confirmar** para eliminar la identidad.
6. Limpie las configuraciones del sistema de archivos y LVM completando los pasos siguientes:
- a) Inicie sesión en IBM Spectrum Protect Plus mediante el protocolo Secure Shell (SSH) o mediante la consola de hipervisor utilizando la cuenta serveradmin.
  - b) Obtenga el ID de la agrupación de almacenamiento de vSnap de localhost. Emita el mandato siguiente:
- ```
$ vsnap pool show
```
- 

**Atención:** Para asegurarse de que no se han perdido datos, verifique que el ID obtenido es el ID de la agrupación de almacenamiento de vSnap de localhost.
- c) Suprima la agrupación de almacenamiento de vSnap de localhost. Emita el mandato siguiente donde <ID> es el ID obtenido en el paso anterior:
- ```
$ vsnap pool delete --id <ID>
```
- d) Desmonte la memoria caché de la nube del almacenamiento de vSnap de localhost. Emita el mandato siguiente:
- ```
$ sudo umount -f /opt/vsnap-data
```
- e) Edite el archivo fstab para inhabilitar el inicio de la memoria caché de la nube. Utilizando sudo y un editor de texto, comente la línea que empieza por /dev/mapper/vsnapdata-vsnapdata1v.
  - f) Desactive el grupo de volúmenes de LVM que está asociado con la memoria caché de la nube. Emita el mandato siguiente:
- ```
$ sudo vgchange -an vsnapdata
```
7. Utilizando vSphere o Hyper-V Manager, desconecte los discos duros virtuales que ya no son necesarios del dispositivo IBM Spectrum Protect Plus. Continúe con precaución para asegurarse de que se han desconectado los discos correctos. El servidor vSnap de localhost tiene dos discos duros virtuales asociados, que tienen un tamaño de 100 GB y 128 GB. Para obtener instrucciones detalladas

sobre la desconexión o eliminación de discos duros virtuales, consulte la documentación del hipervisor adecuada. A continuación se proporciona un procedimiento general para cada hipervisor.



**Atención:** Apague el dispositivo IBM Spectrum Protect Plus antes de desconectar los discos duros virtuales. No suprima los discos duros virtuales hasta que se haya confirmado la correcta funcionalidad después de encender el dispositivo y de ejecutar un trabajo de mantenimiento.

Elimine los discos duros virtuales asociados de la máquina virtual completando los pasos siguientes:

a) Para entornos de VMware, abra vSphere y complete los pasos siguientes:

- 1) Pulse **MV y plantillas**.
- 2) Expanda el host que contiene el dispositivo IBM Spectrum Protect Plus.
- 3) Seleccione la máquina virtual IBM Spectrum Protect Plus.
- 4) Apague el dispositivo IBM Spectrum Protect Plus.
- 5) En el menú **Acciones**, haga clic en **Editar valores**.
- 6) Localice los discos duros virtuales que ya no son necesarios. Los tamaños junto a los discos que se pueden eliminar son 100 GB y 128 GB.
- 7) Seleccione uno de los discos identificados y pulse el botón Eliminar.

**Importante:** No seleccione la casilla de verificación **Suprimir archivos del almacén de datos** de ningún disco. Suprima los discos solo después de verificar su correcta funcionalidad.

- 8) Seleccione el disco identificado restante y pulse el botón Eliminar.
- 9) Pulse en **Aceptar**.

10) Encienda IBM Spectrum Protect Plus.

b) Para entornos Hyper-V, abra Hyper-V Manager y complete los pasos siguientes:

- 1) Seleccione el nodo al que pertenece la máquina virtual de IBM Spectrum Protect Plus.
- 2) Seleccione la máquina virtual de IBM Spectrum Protect Plus en el panel **Máquinas virtuales**.
- 3) Apague el dispositivo IBM Spectrum Protect Plus.
- 4) Pulse **Valores** para la máquina virtual.
- 5) Localice los discos duros virtuales que ya no son necesarios. En cada uno de los discos duros virtuales, haga clic en Inspeccionar. Los valores de **Tamaño máximo de disco** de la ventana **Propiedades de disco duro virtual** deben ser de 100 GB y 128 GB.
- 6) Seleccione uno de los discos identificados y pulse **Eliminar**.
- 7) Seleccione el disco identificado restante y pulse **Eliminar**.
- 8) Pulse en **Aceptar**.
- 9) Encienda IBM Spectrum Protect Plus.

8. Vuelva a explorar el bus de SCSI e inhabilite el servicio de vSnap completando los pasos siguientes:

a) Inicie sesión en IBM Spectrum Protect Plus mediante el protocolo Secure Shell (SSH) o mediante la consola de hipervisor utilizando la cuenta `serveradmin`.

b) Vuelva a explorar el bus de SCSI emitiendo el siguiente mandato:

```
$ sudo rescan-scsi-bus.sh
```

c) Detenga el servicio de vSnap emitiendo el siguiente mandato:

```
$ sudo systemctl stop vsnap
```

d) Inhabilite el servicio de vSnap emitiendo el siguiente mandato:

```
$ sudo systemctl disable vsnap
```

---

## Capítulo 9. Gestión de políticas de SLA para operaciones 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 para replicar o copiar datos de 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 periodo de retención de 1 semana. Para todos los recursos soportados excepto para contenedores e instancias de Amazon EC2.

### Plata

Esta política se ejecuta diariamente con un periodo de retención de 1 mes. Para todos los recursos soportados excepto para los datos de contenedores e instancias de Amazon EC2.

### Bronce

Esta política se ejecuta diariamente con un periodo de retención de 1 semana. Para todos los recursos soportados excepto para los datos de contenedores e instancias de Amazon EC2.

### EC2

Para proteger instancias de Amazon EC2, esta política ejecuta diariamente copias de seguridad de instantáneas con un periodo de retención de 31 días.

### Contenedor

Para proteger los datos de contenedor, esta política ejecuta las operaciones siguientes:

- Copias de seguridad de instantánea cada 6 horas con un periodo de retención de 1 día
- Copias de seguridad diarias con un periodo de retención de 31 días.

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 copia de almacenamiento de objetos estándar, el tipo de destino o las opciones del servidor de destino, los trabajos asociados iniciarán una copia de seguridad de base de datos completa, no una copia de seguridad incremental, durante la siguiente ejecución del trabajo.

Para las instalaciones de IBM Spectrum Protect Plus, 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.

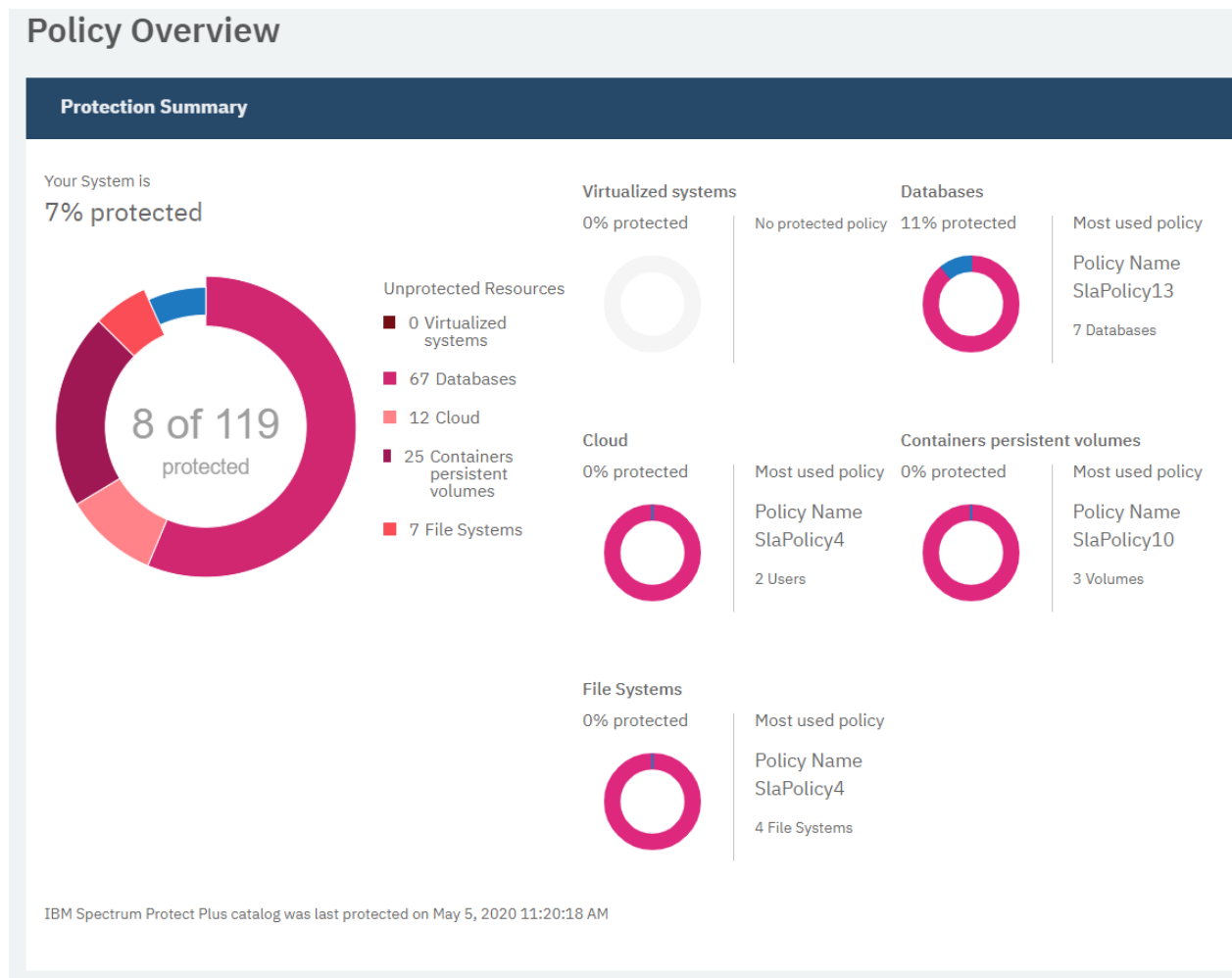
---

## Resumen de protección

Puede ver el estado de protección de los recursos del sistema en el panel **Resumen de protección**.

El panel **Resumen de protección** consta de diagramas de anillo que representan el número de recursos protegidos frente al número de recursos no protegidos. Para cada tipo de recurso, puede ver el porcentaje del recurso que está protegido y la política de acuerdo de nivel de servicio (SLA) que se utiliza con más frecuencia para dicho recurso.

Para ver el panel **Resumen de protección**, desde el panel de navegación, haga clic en **Gestionar protección > Visión general de políticas**.



## Sistema

El gráfico **Su sistema** muestra el porcentaje total de recursos del sistema que están protegidos por IBM Spectrum Protect Plus.

### % protegido

Muestra el porcentaje de recursos protegidos por IBM Spectrum Protect Plus. En el diagrama de anillo, los recursos protegidos están representados por la línea azul. Al pasar el cursor por encima de las distintas partes del anillo, puede ver los números de los recursos protegidos y no protegidos.

### Recursos no protegidos

Muestra la leyenda de los recursos no protegidos. En la lista, los datos se muestran solo para los tipos de recursos que gestiona su instancia de IBM Spectrum Protect Plus. Si IBM Spectrum Protect Plus no gestiona un tipo de recurso, el recuento es 0.

### Sistemas virtualizados

El gráfico **Sistemas virtualizados** muestra el porcentaje de sistemas virtualizados protegidos por IBM Spectrum Protect Plus.



### **% protegido**

Muestra el porcentaje de sistemas virtualizados que están protegidos. Al pasar el cursor por encima de las distintas partes del anillo, puede ver los números de los sistemas virtualizados protegidos y no protegidos.

Si IBM Spectrum Protect Plus no gestiona sistemas virtualizados, el porcentaje es 0.

### **La política más utilizada**

Muestra el nombre de la política de SLA utilizada con más frecuencia y el número de sistemas virtualizados que utilizan esta política. Si IBM Spectrum Protect Plus no gestiona sistemas virtualizados, no se visualiza este campo.

### **Política no protegida**

Este mensaje se muestra solo cuando IBM Spectrum Protect Plus no gestiona sistemas virtualizados.

## **Bases de datos**

El gráfico **Bases de datos** muestra el porcentaje de bases de datos protegidas por IBM Spectrum Protect Plus.

### **% protegido**

Muestra el porcentaje de bases de datos que están protegidas. Al pasar el cursor por encima de las distintas partes del anillo, puede ver los números de bases de datos protegidas y no protegidas.

Si IBM Spectrum Protect Plus no gestiona bases de datos de aplicaciones, el porcentaje es 0.

### **La política más utilizada**

Muestra el nombre de la política de SLA utilizada con más frecuencia y el número de bases de datos que utilizan esta política. Si IBM Spectrum Protect Plus no gestiona bases de datos, este campo no se visualiza.

### **Política no protegida**

Este mensaje se muestra solo cuando IBM Spectrum Protect Plus no gestiona bases de datos.

## **Nube**

El gráfico **Nube** muestra el porcentaje de cuentas basadas en la nube, como los arrendatarios de Microsoft Office 365, que están protegidos por IBM Spectrum Protect Plus.

### **% protegido**

Muestra el porcentaje de cuentas basadas en la nube que están protegidas. Al pasar el cursor por encima de las distintas partes del anillo, puede ver los números de cuentas protegidas y no protegidas.

Si IBM Spectrum Protect Plus no gestiona cuentas basadas en la nube, el porcentaje es 0.

### **La política más utilizada**

Muestra el nombre de la política de SLA utilizada con más frecuencia y el número de cuentas que utilizan esta política. Si IBM Spectrum Protect Plus no gestiona cuentas basadas en la nube, no se visualiza este campo.

### **Política no protegida**

Este mensaje se muestra solo cuando IBM Spectrum Protect Plus no gestiona cuentas basadas en la nube.

## **Volúmenes persistentes de contenedores**

Muestra el porcentaje de volúmenes persistentes que están protegidos por IBM Spectrum Protect Plus.

### **% protegido**

Muestra el porcentaje de volúmenes persistentes que están protegidos. Al pasar el cursor por encima de las distintas partes del anillo, puede ver los números de volúmenes persistentes protegidos y no protegidos.

Si IBM Spectrum Protect Plus no gestiona volúmenes persistentes, el porcentaje es 0.

### **La política más utilizada**

Muestra el nombre de la política de SLA utilizada con más frecuencia y el número de volúmenes persistentes que utilizan esta política. Si IBM Spectrum Protect Plus no gestiona volúmenes persistentes, este campo no se visualiza.

### **Política no protegida**

Este mensaje se muestra solo cuando IBM Spectrum Protect Plus no gestiona volúmenes persistentes.

### **Sistemas de archivos**

Muestra el porcentaje de sistemas de archivos protegidos por IBM Spectrum Protect Plus.

#### **% protegido**

Muestra el porcentaje de sistemas de archivos que están protegidos. Al pasar el cursor por encima de las distintas partes del anillo, puede ver los números de los sistemas de archivos protegidos y no protegidos.

Si IBM Spectrum Protect Plus no gestiona ningún sistema de archivos, el porcentaje es 0.

### **La política más utilizada**

Muestra el nombre de la política de SLA utilizada con más frecuencia y el número de sistemas de archivos que utilizan esta política. Si IBM Spectrum Protect Plus no gestiona ningún sistema de archivos, este campo no se visualiza.

### **Política no protegida**

Este mensaje se muestra solo cuando IBM Spectrum Protect Plus no gestiona sistemas de archivos.

## **Creación de una política de SLA para hipervisores, bases de datos y sistemas de archivos**

Puede crear políticas de acuerdo de nivel de servicio (SLA) personalizadas para definir políticas de frecuencia de copia de seguridad, de retención, de réplica y de copia 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.

Cuando se copian datos de un servidor vSnap en un almacenamiento en la nube, se copiará la instantánea completada correctamente más reciente.

### **Procedimiento**

Para crear una política de SLA para hipervisores, bases de datos y sistemas de archivos, complete los pasos siguientes:

1. En el panel de navegación, haga clic en **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. Haga clic en **VMware, Hyper-V, Exchange, Office365, SQL, Oracle, Db2, MongoDB y sistemas de archivos de Windows**.
5. En la sección **Política de copia de seguridad**, 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 que se crean sin una planificación se pueden ejecutar bajo demanda.

## Frecuencia

**Restricción:** Los días de la semana para la opción **Semanas** está disponible solo si instala el arreglo temporal de IBM Spectrum Protect Plus 10.1.6 eFix2 o posterior.

Escriba una frecuencia para las operaciones de copia de seguridad. Elija entre **Minutos, Horas, Días, Semanas, Meses** o **Años**. Cuando se selecciona **Semanas**, puede seleccionar uno o más días de la semana. La **Hora de inicio** se aplicará a los días seleccionados de la semana.

## Hora de inicio

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

El huso horario se rellena automáticamente con los valores del navegador. Para actualizar el huso horario, haga clic en el campo y seleccione una región y ciudad de la lista, por ejemplo: **Europa/Dublín**. También puede hacer clic en el campo y especificar una región o ciudad en el campo **Buscar** y seleccionar un elemento de los resultados coincidentes.

## 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.

6. 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 [“Configuración de socios de almacenamiento de copias de seguridad”](#) en la página 122.

## 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

**Restricción:** Los días de la semana para la opción **Semanas** está disponible solo si instala el arreglo temporal de IBM Spectrum Protect Plus 10.1.6 eFix2 o posterior.

Escriba una frecuencia para las operaciones de réplica. Elija entre **Minutos, Horas, Días, Semanas, Meses** o **Años**. Cuando se selecciona **Semanas**, puede seleccionar uno o más días de la semana. La **Hora de inicio** se aplicará a los días seleccionados de la semana.

## Hora de inicio

Escriba la fecha y la hora de inicio deseadas para la operación de réplica.

El huso horario se rellena automáticamente con los valores del navegador. Para actualizar el huso horario, haga clic en el campo y seleccione una región y ciudad de la lista, por ejemplo: **Europa/Dublín**. También puede hacer clic en el campo y especificar una región o ciudad en el campo **Buscar** y seleccionar un elemento de los resultados coincidentes.

#### **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.

7. En la sección **Copias adicionales**, establezca las opciones siguientes para copiar datos en el almacenamiento de objetos estándar o el almacenamiento de objetos de archivado.

#### **Almacenamiento de objetos estándar (copia incremental)**

Seleccione esta opción para copiar datos en el almacenamiento en la nube o en un servidor de repositorio.

Se realiza una copia de seguridad de los datos en el servidor vSnap para la protección a corto plazo y, a continuación, se copian en el almacenamiento en la nube o en un servidor de repositorio seleccionado para la protección a largo plazo. Durante la primera copia de un volumen de copia de seguridad, se realiza una copia de seguridad de toda la instantánea. Una vez completada la primera copia 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 carga sin definir una frecuencia o una hora de inicio.

#### **Frecuencia**

**Restricción:** Los días de la semana para la opción **Semanas** está disponible solo si instala el arreglo temporal de IBM Spectrum Protect Plus 10.1.6 eFix2 o posterior.

Especifique una frecuencia para las operaciones de copia. Elija entre **Minutos**, **Horas**, **Días**, **Semanas**, **Meses** o **Años**. Cuando se selecciona **Semanas**, puede seleccionar uno o más días de la semana. La **Hora de inicio** se aplicará a los días seleccionados de la semana.

#### **Hora de inicio**

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

El huso horario se rellena automáticamente con los valores del navegador. Para actualizar el huso horario, haga clic en el campo y seleccione una región y ciudad de la lista, por ejemplo: **Europa/Dublín**. También puede hacer clic en el campo y especificar una región o ciudad en el campo **Buscar** y seleccionar un elemento de los resultados coincidentes.

#### **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.

**Restricción:** Las opciones de retención de copia se inhabilitan si un servidor que utiliza la retención Grabar una vez leer varias (WORM) aparece seleccionado en el campo **Destino**.

#### Origen

Pulse el origen de la operación de copia:

##### Destino de política principal

El origen de la operación de copia es el sitio de destino definido en la sección **Política principal**.

##### Destino de política de réplica

El origen de la operación de copia 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 **Servicios en la nube** o **Servidores de repositorio**.

#### Objetivo

Pulse el sistema de almacenamiento en la nube o el servidor de repositorio donde desea copiar 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 191](#) 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.

#### Almacenamiento de objetos de archivado (copia completa)

Seleccione esta opción para archivar datos en un almacenamiento en la nube o en un servidor de repositorio para la protección a largo plazo.

Esta operación proporciona una copia 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

**Restricción:** Los días de la semana para la opción **Semanas** está disponible solo si instala el arreglo temporal de IBM Spectrum Protect Plus 10.1.6 eFix2 o posterior.

Especifique una frecuencia para las operaciones de archivado. Elija entre **Minutos**, **Horas**, **Días**, **Semanas**, **Meses** o **Años**. Cuando se selecciona **Semanas**, puede seleccionar uno o más días de la semana. La **Hora de inicio** se aplicará a los días seleccionados de la semana.

#### Hora de inicio

Especifique la fecha y la hora en que desea que se inicie la operación de archivado.

El huso horario se rellena automáticamente con los valores del navegador. Para actualizar el huso horario, haga clic en el campo y seleccione una región y ciudad de la lista, por ejemplo: **Europa/Dublín**. También puede hacer clic en el campo y especificar una región o ciudad en el campo **Buscar** y seleccionar un elemento de los resultados coincidentes.

#### 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 **Servicios en la 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 191.

8. 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 <a href="#">“Creación de un rol”</a> en la página 539
Cree una definición de trabajo de copia de seguridad que utilice la política de SLA.	Consulte los temas de copia de seguridad en <a href="#">Capítulo 10, “Protección de sistemas virtualizados”</a> , en la página 257, <a href="#">Capítulo 14, “Protección de bases de datos”</a> , en la página 375 y <a href="#">Capítulo 11, “Protección de sistemas de archivos”</a> , en la página 309.

### Conceptos relacionados

[“Replicar datos de almacenamiento de copia de seguridad”](#) en la página 11

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.

[“Copiar instantáneas en almacenamiento de copias de seguridad secundario”](#) en la página 12

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 copiar instantáneas desde un servidor vSnap en un almacenamiento de copias de seguridad secundario.

### Tareas relacionadas

[“Creación de una política de SLA para instancias de Amazon EC2”](#) en la página 248

Puede crear políticas de acuerdo de nivel de servicio (SLA) personalizadas para definir las políticas de frecuencia y retención de instantáneas que son específicas de las instancias de Amazon EC2.

[“Creación de una política de SLA para clústeres Kubernetes”](#) en la página 250

Puede crear políticas de acuerdo de nivel de servicio (SLA) personalizadas para los volúmenes persistentes que están conectados a un clúster Kubernetes. Puede definir la frecuencia de las operaciones de copia de seguridad y de instantánea y especificar políticas para los trabajos de retención, réplica y copia.

## Creación de una política de SLA para instancias de Amazon EC2

Puede crear políticas de acuerdo de nivel de servicio (SLA) personalizadas para definir las políticas de frecuencia y retención de instantáneas que son específicas de las instancias de Amazon EC2.

## Acerca de esta tarea

Cuando se ejecuta un trabajo de copia de seguridad planificado, se crea una instantánea de la instancia con la frecuencia que se define en la política de instantáneas.

Si una instancia está asociada con varias políticas de SLA, asegúrese de que las políticas que crea no están planificadas 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.

## Procedimiento

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

1. En el panel de navegación, haga clic en **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. Pulse **Amazon EC2**.  
Se muestran las opciones de política de SLA para instancias de EC2.
5. En la sección **Protección de instantáneas**, establezca las siguientes opciones para las operaciones de instantánea:

### Retención

Especifique el periodo de retención para las instantáneas.

### Deshabilitar planificación

Seleccione esta casilla de verificación para crear la política de instantáneas sin definir una frecuencia u hora de inicio. Las políticas que se crean sin una planificación se pueden ejecutar bajo demanda. Este campo es opcional.

### Frecuencia

**Restricción:** Los días de la semana para la opción **Semanas** está disponible solo si instala el arreglo temporal de IBM Spectrum Protect Plus 10.1.6 eFix2 o posterior.

Especifique una frecuencia para las operaciones de instantánea. Elija entre **Minutos**, **Horas**, **Días**, **Semanas**, **Meses** o **Años**. Cuando se selecciona **Semanas**, puede seleccionar uno o más días de la semana. La **Hora de inicio** se aplicará a los días seleccionados de la semana.

### Hora de inicio

Especifique la fecha y hora en que desea que se inicie la operación de instantánea.

El huso horario se rellena automáticamente con los valores del navegador. Para actualizar el huso horario, haga clic en el campo y seleccione una región y ciudad de la lista, por ejemplo: **Europa/Dublín**. También puede hacer clic en el campo y especificar una región o ciudad en el campo **Buscar** y seleccionar un elemento de los resultados coincidentes.

### Prefijo de instantánea

Escriba un prefijo para añadirlo al principio de los nombres de instantánea. Los prefijos pueden ayudarle a organizar e identificar fácilmente instantáneas. Este campo es opcional.

Por ejemplo, si ha especificado el prefijo "daily\_", todos los nombres de instantánea que se crean con esta política de SLA comenzará con "daily\_".

6. Pulse **Guardar**.

La política de SLA que ha creado se muestra en la tabla del panel Políticas de SLA.

## Qué hacer a continuación

Después de crear una política de SLA, realice las acciones siguientes:

- Asigne permisos de usuario a la política de SLA. Para obtener instrucciones, consulte [“Creación de un rol” en la página 539](#).
- Cree una definición de trabajo de copia de seguridad que utilice la política de SLA. Para obtener instrucciones, consulte [“Copia de seguridad de datos de Amazon EC2” en la página 300](#).

## Tareas relacionadas

[“Edición de una política de SLA” en la página 255](#)

Edite las opciones de una política de SLA para que refleje los cambios en el entorno de IBM Spectrum Protect Plus.

[“Supresión de una política de SLA” en la página 255](#)

Suprima una política de SLA cuando está obsoleta.

## Creación de una política de SLA para clústeres Kubernetes

Puede crear políticas de acuerdo de nivel de servicio (SLA) personalizadas para los volúmenes persistentes que están conectados a un clúster Kubernetes. Puede definir la frecuencia de las operaciones de copia de seguridad y de instantánea y especificar políticas para los trabajos de retención, réplica y copia.

### Antes de empezar

Si tiene previsto copiar datos en un almacenamiento secundario o archivar datos en un sistema de almacenamiento en la nube, realice las acciones siguientes:

- Si tiene previsto copiar datos en un almacenamiento secundario, como un sistema de almacenamiento en la nube o un servidor de repositorio, asegúrese de que se ha configurado el almacenamiento secundario. Para obtener información sobre los sistemas de almacenamiento secundario soportados y para obtener instrucciones de configuración, consulte [“Gestión del almacenamiento de copia de seguridad secundario” en la página 191](#)
- Si tiene previsto archivar datos en un sistema de almacenamiento en la nube, el destino de la nube debe tener 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 191](#).

### Acerca de esta tarea

Puede crear políticas de SLA personalizadas si no desea utilizar la política de **Contenedor** predefinida. La política **Contenedor** ejecuta las siguientes operaciones:

- Copias de seguridad de instantánea cada 6 horas con un periodo de retención de 1 día
- Copias de seguridad de copia diarias con un periodo de retención de 31 días

Se necesita una instantánea en una operación de copia de seguridad de Kubernetes. Cuando se ejecuta un trabajo de copia de seguridad planificada, se crea una instantánea de la reclamación de volumen persistente (PVC) en el sistema de almacenamiento Ceph con la frecuencia definida por la política de instantánea. Puede especificar valores de política adicionales para copiar la instantánea en el servidor vSnap de IBM Spectrum Protect Plus, replicar el servidor vSnap o copiar los datos en el almacenamiento de objetos en la nube o en un servidor de repositorio.

Si una PVC está asociada con varias políticas de SLA, asegúrese de que las políticas que crea no están planificadas 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.

### Procedimiento

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

1. En el panel de navegación, haga clic en **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. Haga clic en **Kubernetes**.

Se muestran las opciones de política de SLA para clústeres Kubernetes.



5. En la sección **Protección de instantáneas**, establezca las siguientes opciones para las operaciones de instantánea.
- Retención**  
Especifique el periodo de retención para las instantáneas.
- Deshabilitar planificación**  
Seleccione esta casilla de verificación para crear la política de instantáneas sin definir una frecuencia u hora de inicio. Las políticas que se crean sin una planificación se pueden ejecutar bajo demanda. Este campo es opcional.
- Si tiene previsto habilitar las secciones de política para las operaciones de copia de seguridad de copia, réplica o copia adicional, asegúrese de que esta casilla de verificación no está seleccionada. De lo contrario, no habrá instantáneas disponibles para copiarlas en el servidor vSnap.
- Frecuencia**
- Restricción:** Los días de la semana para la opción **Semanas** está disponible solo si instala el arreglo temporal de IBM Spectrum Protect Plus 10.1.6 eFix2 o posterior.
- Especifique una frecuencia para las operaciones de instantánea. Elija entre **Minutos, Horas, Días, Semanas, Meses** o **Años**. Cuando se selecciona **Semanas**, puede seleccionar uno o más días de la semana. La **Hora de inicio** se aplicará a los días seleccionados de la semana.
- Hora de inicio**  
Especifique la fecha y hora en que desea que se inicie la operación de instantánea.
- El huso horario se rellena automáticamente con los valores del navegador. Para actualizar el huso horario, haga clic en el campo y seleccione una región y ciudad de la lista, por ejemplo: **Europa/ Dublín**. También puede hacer clic en el campo y especificar una región o ciudad en el campo **Buscar** y seleccionar un elemento de los resultados coincidentes.
- Prefijo de instantánea**  
Escriba un prefijo para añadirlo al principio de los nombres de instantánea. Puede añadir un prefijo a los nombres de instantánea para ayudarle a organizar e identificar fácilmente instantáneas. Este campo es opcional.
- Puede especificar hasta 32 caracteres para el prefijo.
- Por ejemplo, si ha especificado el prefijo "daily", todos los nombres de instantánea que se crean con esta política de SLA comenzará con "daily".
6. Opcional: En la sección **Política de copia de seguridad**, establezca las opciones siguientes para las operaciones de copia de seguridad de copia en el servidor vSnap:
- Almacenamiento de copias de seguridad**  
Seleccione esta casilla de verificación para habilitar las operaciones de copia de seguridad de copia en el servidor vSnap. 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 para las copias de seguridad de copia en el servidor vSnap.
- Deshabilitar planificación**  
Seleccione esta casilla de verificación para crear la política de copia de seguridad sin definir una frecuencia o una hora de inicio. Las políticas que se crean sin una planificación se pueden ejecutar bajo demanda. Este campo es opcional.
- Frecuencia**
- Restricción:** Los días de la semana para la opción **Semanas** está disponible solo si instala el arreglo temporal de IBM Spectrum Protect Plus 10.1.6 eFix2 o posterior.
- Especifique una frecuencia para las operaciones de copia de seguridad de copia. Elija entre **Minutos, Horas, Días, Semanas, Meses** o **Años**. Cuando se selecciona **Semanas**, puede seleccionar uno o más días de la semana. La **Hora de inicio** se aplicará a los días seleccionados de la semana.

### **Hora de inicio**

Especifique la fecha y hora en que desea que se inicie la operación de copia de seguridad de copia.

**Consejo:** Asigne una hora para que la copia de seguridad de instantánea se complete antes de iniciar la operación de copia de seguridad de copia. Por ejemplo, si la operación de instantánea comienza a medianoche (0:00), establezca la operación de copia de seguridad de copia para que comience 15 minutos después, a las 00:15.

El huso horario se rellena automáticamente con los valores del navegador. Para actualizar el huso horario, haga clic en el campo y seleccione una región y ciudad de la lista, por ejemplo: **Europa/Dublín**. También puede hacer clic en el campo y especificar una región o ciudad en el campo **Buscar** y seleccionar un elemento de los resultados coincidentes.

### **Sitio de destino**

Seleccione el sitio de destino para las copias de seguridad.

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 colocación de los datos en los servidores vSnap.

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

### **Utilizar únicamente el almacenamiento de disco cifrado**

Si el entorno incluye servidores cifrados y sin cifrar, seleccione esta casilla de verificación para realizar una copia de seguridad de los datos en servidores vSnap cifrados.

**Restricción:** Si se selecciona esta opción, pero no hay disponibles servidores vSnap cifrados, el trabajo asociado falla.

7. Opcional: 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 [“Configuración de socios de almacenamiento de copias de seguridad”](#) en la página 122.

### **Réplica del almacenamiento de copias de seguridad**

Seleccione esta opción para habilitar la réplica.

Esta opción se habilita solo cuando está seleccionada la **Política de copia de seguridad**.

### **Deshabilitar planificación**

Seleccione esta casilla de verificación para crear la relación de duplicación sin definir una frecuencia o una hora de inicio. Este campo es opcional.

### **Frecuencia**

**Restricción:** Los días de la semana para la opción **Semanas** está disponible solo si instala el arreglo temporal de IBM Spectrum Protect Plus 10.1.6 eFix2 o posterior.

Escriba una frecuencia para las operaciones de réplica. Elija entre **Minutos**, **Horas**, **Días**, **Semanas**, **Meses** o **Años**. Cuando se selecciona **Semanas**, puede seleccionar uno o más días de la semana. La **Hora de inicio** se aplicará a los días seleccionados de la semana.

### **Hora de inicio**

Escriba la fecha y la hora de inicio deseadas para la operación de réplica.

El huso horario se rellena automáticamente con los valores del navegador. Para actualizar el huso horario, haga clic en el campo y seleccione una región y ciudad de la lista, por ejemplo: **Europa/Dublín**. También puede hacer clic en el campo y especificar una región o ciudad en el campo **Buscar** y seleccionar un elemento de los resultados coincidentes.

### **Sitio de destino**

Seleccione el sitio de destino para replicar 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 colocación de los datos en los servidores vSnap.

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

#### **Utilizar únicamente el almacenamiento de disco cifrado**

Seleccione esta opción para replicar datos en servidores vSnap cifrados si el entorno incluye servidores cifrados y no cifrados.

**Restricción:** Si se selecciona esta opción, pero no hay disponibles servidores vSnap cifrados, el trabajo asociado falla.

#### **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, deselectione esta opción y establezca una política distinta.

8. Opcional: En la sección **Copias adicionales**, establezca las opciones para copiar datos en el almacenamiento de objetos estándar o el almacenamiento de objetos de archivado.

Cuando se copian datos de un servidor vSnap en un almacenamiento en la nube, se copiará la instantánea completada correctamente más reciente.

#### **Almacenamiento de objetos estándar (copia incremental)**

Seleccione esta opción para copiar datos en el almacenamiento en la nube o en un servidor de repositorio. Esta opción se habilita solo cuando está seleccionada la **Política de copia de seguridad**.

Se realiza una copia de seguridad de los datos en el servidor vSnap para una protección a corto plazo y, a continuación, se copian en el almacenamiento en la nube o en un servidor de repositorio seleccionado para una protección a más largo plazo. Durante la primera copia de un volumen de copia de seguridad, se realiza una copia de seguridad de toda la instantánea. Una vez completada la primera copia 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 repositorio o en la nube se puede realizar desde cualquier servidor vSnap.

#### **Deshabilitar planificación**

Seleccione esta casilla de verificación para crear la relación de copia sin definir una frecuencia o una hora de inicio. Este campo es opcional.

#### **Frecuencia**

**Restricción:** Los días de la semana para la opción **Semanas** está disponible solo si instala el arreglo temporal de IBM Spectrum Protect Plus 10.1.6 eFix2 o posterior.

Especifique una frecuencia para las operaciones de copia. Elija entre **Minutos, Horas, Días, Semanas, Meses o Años**. Cuando se selecciona **Semanas**, puede seleccionar uno o más días de la semana. La **Hora de inicio** se aplicará a los días seleccionados de la semana.

#### **Hora de inicio**

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

El huso horario se rellena automáticamente con los valores del navegador. Para actualizar el huso horario, haga clic en el campo y seleccione una región y ciudad de la lista, por ejemplo: **Europa/Dublín**. También puede hacer clic en el campo y especificar una región o ciudad en el campo **Buscar** y seleccionar un elemento de los resultados coincidentes.

#### **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, deselectione esta opción y establezca una política distinta.

**Restricción:** Las opciones de retención de copia se inhabilitan si un servidor que utiliza la retención Grabar una vez leer varias (WORM) aparece seleccionado en el campo **Destino**.

### Origen

Pulse el origen de la operación de copia:

#### Destino de política de copia de seguridad

El origen de la operación de copia es el sitio de destino que aparece definido en la sección **Política de copia de seguridad**.

#### Destino de política de réplica

El origen de la operación de copia es el sitio de destino que aparece definido en la sección **Política de réplica**.

Esta opción se habilita solo cuando está seleccionada la **Réplica de almacenamiento de copia de seguridad**.

### Destino

Pulse **Servicios en la nube** o **Servidores de repositorio**.

### Objetivo

Pulse el sistema de almacenamiento en la nube o el servidor de repositorio donde desea copiar los datos.

Esta lista contiene los sistemas de almacenamiento secundario que se han añadido a IBM Spectrum Protect Plus.

### Almacenamiento de objetos de archivado (copia completa)

Seleccione esta opción para archivar datos en un almacenamiento en la nube o en un servidor de repositorio para la protección a largo plazo. Esta opción se habilita solo cuando está seleccionada la **Política de copia de seguridad**.

Esta operación proporciona una copia de imagen completa en el almacenamiento de archivos seleccionado.

### Deshabilitar planificación

Seleccione esta casilla de verificación para crear una relación de archivado sin definir una frecuencia o una hora de inicio. Este campo es opcional.

### Frecuencia

**Restricción:** Los días de la semana para la opción **Semanas** está disponible solo si instala el arreglo temporal de IBM Spectrum Protect Plus 10.1.6 eFix2 o posterior.

Especifique una frecuencia para las operaciones de archivado. Elija entre **Minutos**, **Horas**, **Días**, **Semanas**, **Meses** o **Años**. Cuando se selecciona **Semanas**, puede seleccionar uno o más días de la semana. La **Hora de inicio** se aplicará a los días seleccionados de la semana.

### Hora de inicio

Especifique la fecha y la hora en que desea que se inicie la operación de archivado.

El huso horario se rellena automáticamente con los valores del navegador. Para actualizar el huso horario, haga clic en el campo y seleccione una región y ciudad de la lista, por ejemplo: **Europa/Dublín**. También puede hacer clic en el campo y especificar una región o ciudad en el campo **Buscar** y seleccionar un elemento de los resultados coincidentes.

### 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 de copia de seguridad

El origen de la operación de archivado es el sitio de destino que aparece definido en la sección **Política de copia de seguridad**.

#### 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 se habilita solo cuando está seleccionada la **Réplica de almacenamiento de copia de seguridad**.

#### **Destino**

Pulse **Servicios en la 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.

#### 9. Pulse **Guardar**.

La política de SLA que ha creado se muestra en la tabla del panel **Políticas de SLA**.

### **Qué hacer a continuación**

Después de crear una política de SLA, realice las acciones siguientes:

- Asigne permisos de usuario a la política de SLA. Para obtener instrucciones, consulte [“Creación de un rol”](#) en la página 539.
- Cree una definición de trabajo de copia de seguridad que utilice la política de SLA. Para obtener instrucciones, consulte [“Definición de copias de seguridad del acuerdo de nivel de servicio de volúmenes persistentes”](#) en la página 338.

### **Tareas relacionadas**

[“Edición de una política de SLA”](#) en la página 255

Edite las opciones de una política de SLA para que refleje los cambios en el entorno de IBM Spectrum Protect Plus.

[“Supresión de una política de SLA”](#) en la página 255

Suprima una política de SLA cuando está obsoleta.


## **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 Suprimir  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**.

---

## Capítulo 10. Protección de sistemas virtualizados

Debe registrar los sistemas virtualizados que desee proteger en IBM Spectrum Protect Plus y, a continuación, crear trabajos para realizar copias de seguridad y restauración de los recursos asociados con los sistemas.

Los sistemas virtualizados hacen referencia a los hipervisores de VMware y Microsoft Hyper-V y a instancias de Amazon EC2.

---

### 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.

Asegúrese de que el entorno de VMware cumple los requisitos del sistema en “Requisitos de copia de seguridad y restauración de hipervisor (Microsoft Hyper-V y VMware) e instancia en la nube (Amazon EC2)” en la página 41.

#### 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 en 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 realizar copia de seguridad de las máquinas virtuales cifradas y se pueden restaurar a nivel de máquina virtual en su ubicación original. Si está restaurando una máquina virtual en una ubicación alternativa, la máquina virtual cifrada se restaura sin cifrado y se debe cifrar manualmente utilizando vCenter Server después de que se haya completado la operación de restauración.

Se precisan los privilegios de vCenter Server siguientes para habilitar operaciones para máquinas virtuales cifradas:

- Cryptographer.Access
- Cryptographer.AddDisk
- Cryptographer.Clone

**Nota:** Se puede montar un volumen NFS en cualquier número de centro de datos que pertenezcan al mismo vCenter. Si el volumen NFS se monta en más de un centro de datos, vCenter trata el mismo volumen como dos almacenes de datos diferentes. IBM Spectrum Protect Plus lo trata como un único almacén de datos y combina todas las VM y VMDK que residen en el almacén de datos de todos los centros de datos en los que se monta el almacén de datos. Cualquier selección de SLA en este almacén de datos hará que se realicen copias de datos de todas las máquinas virtuales de los diferentes centros de datos o que se restauren en IBM Spectrum Protect Plus.

#### 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 ejecutar informes.

## Procedimiento

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

1. En el panel de navegación, pulse **Gestionar protección > Sistemas virtualizados > 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 <a href="#">“Creación de un rol”</a> en la página 539.

## Conceptos relacionados

[“Gestión de identidades”](#) en la página 544

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 262

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 273

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 el 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	<ul style="list-style-type: none"><li>• Alarma reconocida</li><li>• Establecer estado de alarma</li></ul>
Operaciones criptográficas (6.5 y 6.7)	<ul style="list-style-type: none"><li>• Añadir disco</li><li>• Acceso directo</li><li>• Cifrar</li><li>• Cifrar nuevo</li><li>• Gestionar políticas de cifrado</li></ul>
Almacén de datos	<ul style="list-style-type: none"><li>• Asignar espacio</li><li>• Examinar almacén de datos</li><li>• Operaciones de archivo de bajo nivel</li><li>• Eliminar almacén de datos</li><li>• Eliminar archivo</li><li>• Actualizar archivos de máquina virtual</li></ul>
Conmutador distribuido	<ul style="list-style-type: none"><li>• Operación de configuración de puerto</li><li>• Operación de parámetro de puerto</li></ul>
Carpeta	<ul style="list-style-type: none"><li>• Crear carpeta</li></ul>
Global	<ul style="list-style-type: none"><li>• Cancelar tarea</li></ul>
Host > Configuración	<ul style="list-style-type: none"><li>• Configuración de partición de almacenamiento</li></ul>
Servicio de inventario > Descodificación (6.0) Descodificación de vSphere (6.5, 6.7 y 7.0)	<ul style="list-style-type: none"><li>• Asignar o desasignar código vSphere</li><li>• Asignar o desasignar código vSphere en objeto (7.0)</li><li>• Crear código vSphere</li><li>• Crear categoría de código vSphere</li><li>• Campo Modificar UsedBy para categoría</li><li>• Campo Modificar UsedBy para código</li></ul>
Red	<ul style="list-style-type: none"><li>• Asignar una red</li></ul>

Objeto de vCenter Server	Privilegios necesarios
Recurso	<ul style="list-style-type: none"> <li>• Aplicar recomendación</li> <li>• Asignar una vApp a la agrupación de recursos</li> <li>• Asignar máquina virtual a agrupación de recursos</li> <li>• Migrar máquina virtual desactivada</li> <li>• Migrar máquina virtual activada</li> <li>• Consultar vMotion</li> </ul>
Máquina virtual > Configuración	<ul style="list-style-type: none"> <li>• Añadir disco existente</li> <li>• Añadir nuevo disco</li> <li>• Añadir o eliminar dispositivo</li> <li>• Avanzada (6.0 y 6.5)</li> <li>• Configuración avanzada (6.7 y 7.0)</li> <li>• Cambiar recuento de CPU</li> <li>• Cambiar memoria (6.7 y 7.0)</li> <li>• Cambiar valores (7.0)</li> <li>• Configurar dispositivo en bruto (6.7 y 7.0)</li> <li>• Seguimiento de cambios de disco (6.0 y 6.5)</li> <li>• Memoria (6.0 y 6.5)</li> <li>• Modificar valores de dispositivo</li> <li>• Dispositivo en bruto (6.0 y 6.5)</li> <li>• Recargar desde vía de acceso</li> <li>• Eliminar disco</li> <li>• Renombrar</li> <li>• Valores (6.0, 6.5 y 6.7)</li> <li>• Alternar seguimiento de cambios de disco (6.7 y 7.0)</li> </ul>
Máquina virtual > Operaciones de invitado	<ul style="list-style-type: none"> <li>• Modificaciones de operaciones de invitado</li> <li>• Ejecución del programa de operaciones de invitado</li> <li>• Consultas de operaciones de invitado</li> </ul>
Máquina virtual > Interacción	<ul style="list-style-type: none"> <li>• Operación de copia de seguridad en máquina virtual</li> <li>• Apagar</li> <li>• Encender</li> </ul>
Máquina virtual > Inventario	<ul style="list-style-type: none"> <li>• Registrar</li> <li>• Eliminar</li> <li>• Anular registro</li> </ul>

Objeto de vCenter Server	Privilegios necesarios
Máquina virtual > Suministro	<ul style="list-style-type: none"> <li>• Permitir acceso a disco</li> <li>• Permitir acceso a disco de solo lectura</li> <li>• Permitir descarga de la máquina virtual</li> <li>• Permitir carga de archivos de máquina virtual</li> <li>• Marcar como plantilla</li> <li>• Marcar como máquina virtual</li> </ul>
Máquina virtual > Gestión de instantáneas	<ul style="list-style-type: none"> <li>• Crear instantánea</li> <li>• Eliminar instantánea</li> <li>• Revertir instantánea</li> </ul>
vApp	<ul style="list-style-type: none"> <li>• Añadir máquina virtual</li> <li>• Asignar agrupación de recursos</li> <li>• Asignar vApp</li> <li>• Crear</li> <li>• Suprimir</li> <li>• Apagar</li> <li>• Encender</li> <li>• Renombrar</li> <li>• Anular registro</li> <li>• Configuración de recursos de vApp</li> </ul>

### 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 > Sistemas virtualizados > 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 Plus y la máquina virtual.

### Procedimiento

Para probar la conexión, complete los pasos siguientes:

1. En el panel de navegación, pulse **Gestionar protección > Sistemas virtualizados > 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 definir un 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 257.
- Configure las políticas de SLA. Para obtener más instrucciones, consulte [“Crear políticas de copia de seguridad”](#) en la página 169.
- 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 18, “Gestión del acceso de usuarios”](#), en la página 533.
- 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.
- Asegúrese de que la versión más reciente de Herramientas de VMware esté instalada en máquinas virtuales de VMware.

### Acerca de esta tarea

- Al hacer copia de seguridad de máquinas virtuales de VMware, IBM Spectrum Protect Plus descarga archivos .vmx, .vmxf y .nvram si es necesario y, a continuación, transfiere esos archivos al servidor 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. Cuando el dispositivo se comunica 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.
- Si una operación vMotion migra una máquina virtual existente, IBM Spectrum Protect Plus realizará una operación de cambio de base si es necesario.

**Restricción:** 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 de SO de 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 realizando 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.

## Procedimiento

Para definir un trabajo de copia de seguridad de VMware, complete los pasos siguientes:

1. En el panel de navegación, pulse **Gestionar protección > Sistemas virtualizados > 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 ejecutará según lo definido por las políticas de SLA que ha seleccionado. Para ejecutar el trabajo inmediatamente, haga clic en **Trabajos y operaciones > Planificar**. Seleccione el trabajo y pulse **Acciones > Iniciar**.

**Consejo:** Cuando se ejecuta un trabajo para la política de SLA seleccionada, todos los recursos asociados con esa política de SLA se incluyen en la operación de copia de seguridad. Para hacer copia de seguridad únicamente de los recursos seleccionados, puede ejecutar un trabajo bajo demanda. Un trabajo bajo demanda ejecuta inmediatamente la operación de copia de seguridad.

- Para ejecutar un trabajo de copia de seguridad bajo demanda para un único recurso, seleccione el recurso y haga clic en **Ejecutar**. Si el recurso no está asociado con una política de SLA, el botón **Ejecutar** no está disponible.
- Para ejecutar un trabajo de copia de seguridad bajo demanda para uno o más recursos, haga clic en **Crear trabajo**, seleccione **Copia de seguridad ad hoc** y siga las instrucciones en [“Ejecución de un trabajo de copia de seguridad ad hoc”](#) en la página 517.

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 266.

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. Si no se ha establecido un valor de prioridad, se establece una prioridad de 5 de forma predeterminada.

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 de SO de invitado y Contraseña de SO de 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 en el 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 que se copiaron 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 de SO de 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.

**Restricción:** Las claves SSH no son un mecanismo de autorización válido en las plataformas Windows.

#### **Excluir archivos**


Especifique los directorios que se deben omitir durante 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 de SO de 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 recurso y, a continuación, haga clic en **Probar**.
7. Pulse **Guardar**.
8. Para configurar opciones adicionales, pulse el icono de portapapeles **Opciones de política**  que está asociado al trabajo en la sección **Estado de política de SLA**. Establezca las opciones de política adicionales siguientes:

#### **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 de base de datos 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 <a href="#">“Creación de proxies VADP”</a> en la página 268.
Cree una definición de trabajo de restauración de VMware.	Consulte <a href="#">“Restauración de datos de VMware”</a> en la página 273.

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](#).

## Conceptos relacionados

[“Configuración de scripts para las operaciones de copia de seguridad y restauración”](#) en la página 518

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 bajo demanda”](#) en la página 512

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.

## Antes de empezar

Exclusión de uno o más VMDK de una operación de seguridad puede afectar al éxito de la recuperación. Tenga en cuenta los siguientes escenarios antes de excluir un disco de la operación de copia de seguridad de máquina virtual.

- Para la restauración de disco instantánea, si se selecciona un VMDK para una operación de restauración, se elige una máquina virtual existente como destino. IBM Spectrum Protect Plus monta el disco restaurado en la máquina virtual de destino elegida.



- Para la restauración de MV instantánea, si el VMDK que se ha excluido durante una copia de seguridad contiene datos que son necesarios para arrancar la máquina virtual, es posible que la máquina virtual restaurada no arranque.
- Para las máquinas virtuales con invitados basados en Windows, es posible que la máquina virtual restaurada no arranque si el disco en el que está instalado el sistema operativo principal, normalmente la unidad C :, se ha excluido durante la operación de copia de seguridad.
- Para máquinas virtuales con invitados basados en Linux, la máquina virtual restaurada puede fallar:
  - Si se ha excluido un disco que contiene la partición raíz o de arranque durante la copia de seguridad.
  - Si se ha excluido un disco que contiene una partición de datos (no raíz) durante la copia de seguridad y el volumen de datos no tiene la opción 'nofail' especificada en /etc/fstab, la VM restaurada puede fallar.

## Procedimiento

Para excluir los VMDK de la política de SLA:

1. En el panel de navegación, pulse **Gestionar protección > Sistemas virtualizados > 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 copia de seguridad de una máquina virtual de VMware incluye los archivos siguientes:

- VMDKs que corresponden a todos los disco. La copia de seguridad de base de datos 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 solo los bloques cambiados desde la última copia de seguridad satisfactoria.
- Plantillas de máquina virtual.
- 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. Las tareas libres se determinan mediante el número de núcleos de CPU disponibles o mediante la opción **Límite de tarea Softcap**.

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 se prefiere en un entorno de almacenamiento directo porque esta modalidad es rápida y fiable.
- Se prefiere la modalidad de transporte HotAdd si el proxy VADP está virtualizado. Esta modalidad da soporte a todos los tipos de almacenamiento de vSphere.

**Nota:** Para utilizar solo la modalidad de transporte HotAdd sin volver a las modalidades de transporte alternativas, seleccione **El proxy VADP utiliza solo la modalidad de transporte HotAdd en Preferencias globales**. Para obtener más información, consulte el apartado [“Configuración de las preferencias globales”](#) en la página 232.

- 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

Revise los requisitos del sistema IBM Spectrum Protect Plus en [“Requisitos del proxy VADP”](#) en la página 34.

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 539.

**Restricción:** Para ejecutar los pasos para crear proxies VADP, asegúrese de tener un ID de usuario con el rol SYSADMIN asignado. Para obtener más información sobre los roles, consulte [“Gestión de roles”](#) en la página 537.

**Consejo:** 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**.
5. Pulse **Sí** en la pantalla de confirmación.
6. Repita los pasos anteriores para cada proxy que desee crear.

## Resultados

El proxy se añade a la tabla **Proxy VADP**. Puede suspender, desinstalar, anular el registro o editar un servidor proxy pulsando el icono de puntos suspensivos **\*\*\*** para abrir el menú de 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, haga clic en el icono de puntos suspensivos **\*\*\*** para abrir el menú de acciones y haga clic en **Reanudar**. Después de que se cree correctamente, se inicia el vadp de servicio en la máquina proxy. Se genera un archivo de registro, vadp.log, en el directorio /opt/IBM/SPP/logs.

La conexión entre el dispositivo virtual de IBM Spectrum Protect Plus y un proxy 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 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. Emita el mandato siguiente: `ping <vdp_ip>`, donde `<vdp_ip>` es la dirección IP que se puede resolver 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 siguiente procedimiento:

1. Conéctese a la línea de mandatos del proxy VADP utilizando el protocolo de red Secure Shell (SSH).
2. Emita el mandato siguiente: `ping <spectrum_protect_plus_ip>`, donde `<spectrum_protect_plus_ip>` es la dirección IP que se puede resolver del dispositivo virtual 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, puede completar la acción siguiente:

Acción	Cómo
Ejecute el trabajo de copia de seguridad de VMware.	<p>Consulte <a href="#">“Copia de seguridad de datos de VMware”</a> en la <a href="#">página 262</a>.</p> <p>Los proxies se indican en el registro de trabajo con un mensaje de registro similar al texto siguiente:</p> <pre>Run remote vmdkbackup of MicroService: http://&lt;proxy&gt; nombrenodo, IP:dirección_IP_proxy</pre>

### Tareas relacionadas

[“Establecimiento de opciones para proxies VADP”](#) en la [página 271](#)

Al crear proxies VADP en IBM Spectrum Protect Plus, puede configurar varias opciones para cada proxy VADP.

### Registro de un proxy VADP en un servidor vSnap

Puede instalar y registrar un proxy VADP en un servidor vSnap físico o virtual. Cuando instala y registra un proxy VADP en un servidor vSnap, puede ayudar a optimizar el movimiento de datos eliminando un montaje NFS porque los dos sistemas están en la misma máquina.

### Antes de empezar

Se deben desplegar y configurar correctamente uno o más servidores vSnap autónomos en su entorno y se deben añadir a los proveedores de almacenamiento de copias de seguridad de IBM Spectrum Protect Plus. Para obtener instrucciones, consulte [“Registro de un servidor vSnap como proveedor de almacenamiento de copias de seguridad”](#) en la [página 117](#).


Para los requisitos del sistema combinados de un servidor vSnap y el proxy VADP, consulte [Requisitos del proxy VADP en el servidor vSnap](#).

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 539.

La identidad asociada a un servidor vSnap es la cuenta que se utiliza para registrar el proxy VADP en el servidor vSnap. Cuando registra un proxy VADP en un servidor vSnap, se impulsa un instalador y requiere privilegios sudo para instalar correctamente el software de proxy VADP. La identidad asociada a un servidor vSnap debe tener privilegios sudo.

**Consejo:** Utilice el ID de usuario `serveradmin` al añadir un servidor vSnap a IBM Spectrum Protect Plus. Cuando despliega un proxy VADP en un servidor vSnap, se utiliza esta cuenta que ya tiene todos los privilegios necesarios.

### Procedimiento

1. En el panel de navegación, en **Configuración del sistema** > **Almacenamiento de copias de seguridad** > **Disco**. Los servidores vSnap disponibles se muestran en la tabla del panel Almacenamiento de disco.
2. Seleccione el servidor vSnap en el que se va a instalar y registrar el proxy VADP.
3. Haga clic en el icono del menú de acciones . Seleccione **Registrar como proxy VADP**.
4. En el cuadro de diálogo Confirmar, pulse **Sí**.

### Resultados

Una vez que se completa el proceso, aparecerá una marca de verificación verde en la columna **Proxy VADP** de la tabla del panel Almacenamiento de disco.

### Establecimiento de opciones para proxies VADP


Al crear proxies VADP en IBM Spectrum Protect Plus, puede configurar varias opciones para cada proxy VADP.

### Antes de empezar

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 539.

### 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. Haga clic en el proxy VADP que desea configurar, que muestra la información en el panel de detalles adyacente.
3. En el panel de detalles del proxy VADP, haga clic en el icono de puntos suspensivos  y, a continuación, seleccione **Opciones de proxy**.
4. 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.

#### Modalidades de transporte (lista ordenada)

Establezca las modalidades de transporte que debe utilizar el proxy. El orden en el que se selecciona cada modalidad determinará el orden en que se utilizan las modalidades de transporte. Para eliminar una modalidad de transporte, haga clic en el icono Suprimir junto a la modalidad de transporte. 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. Los tipos de compresión disponibles incluyen **libz**, **fastlz** y **skipz**.

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 establecer las opciones de proxy VADP, puede completar las acciones siguientes:

Acción	Cómo
Ejecute el trabajo de copia de seguridad de VMware.	Consulte <a href="#">“Copia de seguridad de datos de VMware”</a> en la página 262.
Desinstale los proxies cuando deje de ejecutar los trabajos de copia de seguridad de VMware.	Consulte <a href="#">“Desinstalación de proxies VADP”</a> en la página 272.

## Tareas relacionadas

[“Creación de proxies VADP”](#) en la página 268

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:

**Nota:** Este procedimiento solo se aplica a los proxies VADP que se han instalado en el entorno. No se aplica al proxy VADP que se despliega con el dispositivo de IBM Spectrum Protect Plus.

1. En el panel de navegación, haga clic en **Configuración del sistema > Proxy VADP**.
2. Haga clic en el proxy VADP que desea desinstalar, que muestra la información en el panel de detalles adyacente.
3. Haga clic en el icono de puntos suspensivos **...** en el panel de detalles y seleccione **Desinstalar**.

## 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 262.
- Asegúrese de que se asignan los roles adecuados a los usuarios de IBM Spectrum Protect Plus para que puedan completar las operaciones de copia de seguridad y restauración. Otorgue a los usuarios acceso a los hipervisores y a las operaciones de copia de seguridad y restauración mediante el panel **Cuentas**. Para obtener más información, consulte [Capítulo 18, “Gestión del acceso de usuarios”](#), en la página 533 y [“Gestión de cuentas de usuario”](#) en la página 542.
- 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.
- Al restaurar una máquina virtual utilizando la modalidad de clonación y utilizando la configuración IP original, asegúrese de que se establecen las credenciales a través de las opciones **Nombre de usuario de SO invitado** y **Contraseña de SO invitado** dentro de la definición de trabajo de copia de seguridad.

### 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 280.

#### 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.

El tamaño de una máquina virtual restaurada desde una copia 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 operación de copia. El tamaño completo de los datos se debe transferir incluso si no están asignados en la máquina virtual de origen.

Al restaurar los datos de VMware desde un archivado de IBM Spectrum Protect, los archivos se migran inicialmente desde la cinta a una agrupación de transferencia. En función del tamaño de la operación de restauración, este proceso podría tardar varias horas.

**Restricción:** No se da soporte a la indexación de archivos y a la restauración de archivos de Windows en volúmenes que residen en discos dinámicos.

## Procedimiento

Para definir un trabajo de restauración de VMware, realice los pasos siguientes:


1. En el panel de navegación, haga clic en **Gestionar protección > Sistemas virtualizados > VMware > Crear trabajo** y, a continuación, seleccione **Restaurar** para abrir el asistente **Restaurar**.


### Sugerencias:

- También puede abrir el asistente pulsando **Trabajos y operaciones > Crear trabajo > Restaurar > VMware**.
  - Para obtener un resumen en ejecución de las selecciones en el asistente, pulse **Vista previa de restauración** en el panel de navegación del asistente.
  - El asistente se abre en la modalidad de configuración predeterminada. Para ejecutar el asistente en modalidad de configuración avanzada, seleccione **Configuración avanzada**. Con la modalidad de configuración avanzada, puede establecer más opciones para el trabajo de restauración.
2. En la página **Seleccionar origen**, realice 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**, seleccione el tipo de trabajo de restauración que desea crear:

### Bajo demanda

Ejecuta una operación de restauración puntual. 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.

4. Complete los campos de la página **Instantánea de origen** y pulse **Siguiente** para continuar.

Los campos que se muestran dependen del número de elementos seleccionados en la página **Seleccionar origen** y en el tipo de restauración. Algunos campos tampoco se muestran hasta que se selecciona un campo relacionado.



### Campos que se muestran para una restauración de recursos única y bajo demanda

Opción	Descripción
<b>Rango de fechas</b>	Especifique un rango de fechas para mostrar las instantáneas disponibles dentro de ese intervalo.
<b>Tipo de almacenamiento de copias de seguridad</b>	<p>Todas las copias de seguridad del rango de fechas seleccionado se listan en filas que muestran la hora a la que se ha realizado la operación de copia de seguridad y la política de acuerdo de nivel de servicio (SLA) para la copia de seguridad. Seleccione la fila que contiene la hora de la copia de seguridad y la política de SLA que desea y, a continuación, realice una de las siguientes acciones:</p> <ul style="list-style-type: none"> <li>Haga clic en el tipo de almacenamiento de copia de seguridad desde el que desea restaurar. Los tipos de almacenamiento que se muestran dependen de los tipos disponibles en el entorno y se muestran en el orden siguiente: <ul style="list-style-type: none"> <li><b>Copia de seguridad</b> Restaura los datos de los que se ha hecho copia de seguridad en un servidor vSnap.</li> <li><b>Réplica</b> Restaura datos que se replican en un servidor vSnap.</li> <li><b>Almacenamiento de objetos</b> Restaura los datos que se copian en un servicio en la nube o en un servidor de repositorio.</li> <li><b>Archivado</b> Restaura los datos que se copian en un archivo de servicio en la nube o en un archivo de servidor de repositorio (cinta).</li> </ul> </li> <li>Haga clic en cualquier sitio en la fila. El primer tipo de copia de seguridad que se muestra secuencialmente desde la izquierda de la fila se selecciona de forma predeterminada. Por ejemplo, si se muestran los tipos de almacenamiento <b>Copia de seguridad</b>, <b>Réplica</b> y <b>Archivado</b>, <b>Copia de seguridad</b> se selecciona de forma predeterminada.</li> </ul>
<b>Utilizar el servidor vSnap alternativo para el trabajo de restauración</b>	<p>Si restaura datos desde un servicio en la nube o un servidor de repositorio, seleccione este recuadro para especificar un servidor vSnap alternativo y, a continuación, seleccione un servidor desde el menú <b>Seleccionar vSnap alternativo</b>.</p> <p>Cuando restaura datos desde un punto de restauración que se ha copiado en 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 copia. Para reducir la carga en el servidor vSnap, puede seleccionar un servidor vSnap alternativo para que sirva como pasarela.</p>

### Campos que se muestran para una instantánea bajo demanda, una restauración de varios recursos o una restauración recurrente

Opción	Descripción
<b>Tipo de ubicación de restauración</b>	<p>Seleccione un tipo de ubicación desde donde se restauran los datos:</p> <p><b>Sitio</b> El sitio en que se ha realizado la copia de seguridad de instantáneas. El sitio se define en el panel <b>Configuración del sistema &gt; Sitio</b>.</p>

Opción	Descripción
	<p><b>Servicio en la nube</b> El servicio en la nube en el que se han copiado las instantáneas. El servicio en la nube se define en el panel <b>Configuración del sistema</b> &gt; <b>Almacenamiento de copias de seguridad</b> &gt; <b>Almacenamiento de objetos</b>.</p> <p><b>Servidor de repositorio</b> El servidor de repositorio en el que se han copiado las instantáneas. El servidor de repositorio se define en el panel <b>Configuración del sistema</b> &gt; <b>Almacenamiento de copias de seguridad</b> &gt; <b>Servidor de repositorio</b>.</p> <p><b>Archivado de servicio en la nube</b> El servicio de archivado en la nube en el que se copiaron las instantáneas. El servicio en la nube se define en el panel <b>Configuración del sistema</b> &gt; <b>Almacenamiento de copias de seguridad</b> &gt; <b>Almacenamiento de objetos</b>.</p> <p><b>Archivado de servidor de repositorio</b> El servidor de repositorio en el que se han copiado las instantáneas en cintas. El servidor de repositorio se define en el panel <b>Configuración del sistema</b> &gt; <b>Almacenamiento de copias de seguridad</b> &gt; <b>Servidor de repositorio</b>.</p>
<b>Seleccionar una ubicación</b>	<p>Si está restaurando datos desde un sitio, seleccione una de las siguientes ubicaciones de restauración:</p> <p><b>Demo</b> El sitio de demostración desde el que se restauran las instantáneas.</p> <p><b>Primario</b> El sitio primario desde el que se restauran las instantáneas.</p> <p><b>Secundario</b> El sitio secundario desde el que se restauran las instantáneas.</p> <p>Si está restaurando datos desde un servidor de nube o de repositorio, seleccione un servidor en el menú <b>Seleccionar una ubicación</b>.</p>
<b>Selector de fecha</b>	Para las operaciones de restauración bajo demanda, especifique un rango de fechas para mostrar las instantáneas disponibles dentro de ese rango.
<b>Punto de restauración</b>	Para las operaciones de restauración bajo demanda, seleccione una instantánea en la lista de instantáneas disponibles en el rango de fechas seleccionado.
<b>Utilizar el servidor vSnap alternativo para el trabajo de restauración</b>	<p>Si restaura datos desde un servicio en la nube o un servidor de repositorio, seleccione este recuadro para especificar un servidor vSnap alternativo y, a continuación, seleccione un servidor desde el menú <b>Seleccionar vSnap alternativo</b>.</p> <p>Cuando restaura datos desde un punto de restauración que se ha copiado en un servicio en la nube o un servidor de repositorio, se utiliza un servidor vSnap como pasarela para completar esta 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 copia. Para reducir la carga en el servidor vSnap, puede seleccionar un servidor vSnap alternativo para que sirva como pasarela.</p>

5. En la página **Establecer destino**, especifique la instancia que desea restaurar para cada origen elegido y pulse **Siguiente**:

**Host o clúster original**

Seleccione esta opción para restaurar los datos en el host o clúster original.

### Host o clúster 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 ESXi si vCenter está inactivo

Seleccione esta opción para omitir vCenter Server y para restaurar los datos directamente en un host ESXi. En otros escenarios de restauración, las acciones se completan a través de vCenter Server. Si vCenter Server no está disponible, esta opción restaura la máquina virtual o máquinas virtuales que contienen los componentes de los que depende vCenter Server.

Cuando selecciona un host ESXi, debe especificar el usuario de host. Puede seleccionar un usuario existente para el host o crear uno nuevo.

Para crear un usuario, especifique un nombre de usuario, el ID de usuario y la contraseña de usuario.

Si el host ESXi está conectado a un dominio, el ID de usuario sigue el formato predeterminado de *dominio\nombre*. Si el usuario es un administrador local, utilice el formato *local\_administrator*.

Para restaurar datos en un host ESXi, el host debe tener un conmutador estándar o un conmutador distribuido con un enlace efímero. Revise la información en [“Restauración de datos cuando no se puede acceder a vCenter Server u otras MV de gestión” en la página 282](#) para asegurarse de que configurado el entorno correcto para utilizar esta opción.

6. En la página **Establecer almacén de datos**, lleve a cabo las acciones siguientes:

- Si está restaurando datos en un clúster o host ESXi alternativo, seleccione el almacén de datos de destino y haga clic en **Siguiente**.
- Si está restaurando datos en el host o clúster ESXi original, esta página no se muestra.

7. 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 ESXi original, especifique los siguientes valores de red:

### 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 datos en el host o clúster original utilizando la configuración de 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 ESXi 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.

**Nota:** Cuando se añade una correlación, debe especificarse la dirección IP de origen en el campo mediante el botón **+**. La información de IP de destino debe especificarse en los campos **Subred / Dirección IP**, **Máscara de subred** y **Pasarela**. El redireccionamiento solo se puede realizar en máquinas con las Herramientas de VMware instaladas antes de ejecutar el trabajo de copia de seguridad que se va a restaurar.

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.

8. En la página **Restaurar métodos**, seleccione el método de restauración que se va a utilizar para la selección de origen. Establezca el trabajo de restauración 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.
9. Si está ejecutando el trabajo de restauración en modalidad avanzada, puede establecer opciones adicionales como se indica a continuación:

#### **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.

**Restaurar etiquetas de MV**

Habilite esta opción para restaurar las etiquetas aplicadas a máquinas virtuales a través de vSphere.

**Habilitar la restauración de streaming (VADP)**

El streaming paralelo para las operaciones de restauración de máquina virtual está establecido de forma predeterminada. Puede deseleccionar esta opción para las operaciones de restauración de la máquina virtual.

**Consejo:** Cuando está restaurando máquinas virtuales gestionadas por VMware Cloud (VMC) en el Software-Defined Data Center (SDDC) de AWS, esta opción debe estar habilitada siempre para permitir la transmisión de datos.

**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.

10. 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.

11. 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**.

12. 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 257](#)

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 ejecutar informes.

#### 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 273](#).

#### Procedimiento

Para crear una red delimitada, complete los pasos siguientes:

1. En el panel de navegación, pulse **Gestionar protección > Sistemas virtualizados > 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 257](#)

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 ejecutar informes.

## Restauración de datos cuando no se puede acceder a vCenter Server u otras MV de gestión

IBM Spectrum Protect Plus proporciona una opción para restaurar datos automáticamente utilizando un host de ESXi si no se puede acceder a vCenter Server o a uno de los componentes que utiliza. Esta opción restaura las máquinas virtuales que contienen los componentes que utiliza vCenter Server.

## Antes de empezar

Para completar este procedimiento, debe estar familiarizado con las interfaces de usuario de ESXi y vCenter Server.

## Acerca de esta tarea

vCenter Server utiliza los siguientes componentes:

- Platform Services Controller (PSC)
- Software-Defined Data Center (SDDC)
- Active Directory (AD)
- Servidores de Sistema de nombres de dominio (DNS)

Para utilizar la opción **Host ESX si vCenter está inactivo**, el host ESXi debe tener un conmutador estándar o un conmutador distribuido. El conmutador distribuido debe tener un enlace efímero. Si uno o ambos conmutadores están disponibles, puede ejecutar una operación de restauración en IBM Spectrum Protect Plus con la opción habilitada, como se describe en [“Restauración de datos de VMware” en la página 273](#) y no es necesaria ninguna configuración manual adicional.

Si ninguno de estos conmutadores está disponible, debe completar los pasos siguientes antes de poder utilizar la opción **Host ESX si vCenter está inactivo**.

## Procedimiento

1. Conéctese a la interfaz de usuario del host ESXi de destino y cree un conmutador virtual estándar.  
El nuevo conmutador no tiene grupos de puertos ni enlaces ascendentes.
2. Utilice el protocolo Secure Shell (SSH) para conectarse al host ESXi.
3. Enumere los conmutadores distribuidos que se configuran en el host ESXi emitiendo el mandato siguiente:

```
#esxcli network vswitch dvs vmware list
```

4. Identifique la tarjeta de interfaz de red física (NIC) y el grupo de puertos del conmutador distribuido que desea utilizar para la operación de restauración.



5. Elimine el NIC físico y el grupo de puertos del conmutador distribuido emitiendo el siguiente mandato:

```
#esxcfg-vswitch -Q unic_físico -V grupo_puertos nombre_conmutador
```

6. Añada el NIC físico y el grupo de puertos al nuevo conmutador estándar emitiendo el siguiente mandato:

```
#esxcli network vswitch standard uplink add --uplink-name=unic_físico --vswitch-name=new_standard_vswitch
```

7. En la interfaz de usuario del host ESXi, añada un grupo de puertos temporal y seleccione el conmutador estándar que ha creado en el paso “1” en la página 282.

El conmutador estándar tiene un grupo de puertos y un enlace ascendente.

8. Ejecute una operación de restauración en IBM Spectrum Protect Plus con la opción **Host ESX si vCenter está inactivo** habilitada.

Para obtener instrucciones sobre la ejecución de una operación de restauración, consulte “Restauración de datos de VMware” en la página 273.

9. En la interfaz de usuario del host ESXi para el host ESXi, encienda las máquinas virtuales que se han restaurado.
10. Inicie sesión en la interfaz de usuario de vCenter Server e inicie la migración de las máquinas virtuales de gestión del grupo de puertos temporal creado en el paso “7” en la página 283 al grupo de puertos distribuidos disponible.
11. Después de que todas las máquinas virtuales se hayan migrado al grupo de puertos original, vuelva a incorporar el NIC físico y el grupo de puertos en el conmutador distribuido original realizando las acciones siguientes. Con fines de ejemplo, los mandatos siguientes hacen referencia a una Tarjeta de interfaz de red virtualizada (VNIC) denominada *vmnic0* que es parte del grupo de puertos 64.
- a. Elimine las tarjetas de red (conocidas como *vmnics*) de un conmutador estándar emitiendo el siguiente mandato:

```
#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 al conmutador distribuido emitiendo el siguiente mandato:

```
#esxcfg-vswitch -P vmnic -V unused_distributed_switch_port_ID distributed_switch
```

Por ejemplo:

```
#esxcfg-vswitch -P vmnic0 -V 64 SDDC-Dswitch-Private
```

12. Suprime el grupo de puertos temporal y el conmutador estándar de la interfaz de usuario del host ESXi.
13. Una vez que las máquinas virtuales se han migrado y se puede acceder a ellas, utilice la interfaz de usuario del host ESXi para anular el registro, pero sin suprimir las máquinas virtuales antiguas 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**. Esta opción anula el registro de una máquina virtual del catálogo de vCenter Server, pero deja los archivos VMDK en el almacén de datos donde los archivos consumen espacio de almacenamiento. Una vez que haya recuperado completamente la MV 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 de copia de seguridad y restauración de hipervisor \(Microsoft Hyper-V y VMware\) e instancia en la nube \(Amazon EC2\)”](#) en la página 41.

### 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 ejecutar informes.

#### 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 > Sistemas virtualizados > 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.

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 285.

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 <a href="#">“Creación de un rol”</a> en la página 539.

**Tareas relacionadas**

[“Copia de seguridad de datos de Hyper-V”](#) en la página 286

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 290

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 > Sistemas virtualizados > 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 Plus y la máquina virtual.

## Procedimiento

Para probar la conexión, complete los pasos siguientes:

1. En el panel de navegación, pulse **Gestionar protección > Sistemas virtualizados > 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

Revise los procedimientos y las consideraciones siguientes antes de definir un 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 284.
- Configure las políticas de SLA. Para obtener instrucciones, consulte [“Crear políticas de copia de seguridad”](#) en la página 169.
- 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 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 18, “Gestión del acceso de usuarios”](#), en la página 533.

- 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 IBM Spectrum Protect Plus se cambia después de crear una copia de seguridad de base de datos 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.

## Acerca de esta tarea

**Restricción:** 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 de SO de 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 realizando 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.

## 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 > Sistemas virtualizados > 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**.

**Consejo:** Cuando se ejecuta un trabajo para la política de SLA seleccionada, todos los recursos asociados con esa política de SLA se incluyen en la operación de copia de seguridad. Para hacer copia de seguridad únicamente de los recursos seleccionados, puede ejecutar un trabajo bajo demanda. Un trabajo bajo demanda ejecuta inmediatamente la operación de copia de seguridad.

- Para ejecutar un trabajo de copia de seguridad bajo demanda par un único recurso, seleccione el recurso y haga clic en **Ejecutar**. Si el recurso no está asociado con una política de SLA, el botón **Ejecutar** no está disponible.
- Para ejecutar un trabajo de copia de seguridad bajo demanda para uno o más recursos, haga clic en **Crear trabajo**, seleccione **Copia de seguridad ad hoc** y siga las instrucciones en [“Ejecución de un trabajo de copia de seguridad ad hoc”](#) en la página 517.

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 Hyper-V** 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. Si no se ha establecido un valor de prioridad, se establece una prioridad de 5 de forma predeterminada.

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 en el 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 copiados 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 de SO de 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 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 recurso y, a continuación, haga clic en **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 de base de datos 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 <a href="#">“Restauración de datos de Hyper-V”</a> en la <a href="#">página 290</a> .

### Conceptos relacionados

[“Configuración de scripts para las operaciones de copia de seguridad y restauración”](#) en la [página 518](#)

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 bajo demanda”](#) en la [página 512](#)

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 286](#).
- 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, consulte [Sistemas 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 18, “Gestión del acceso de usuarios”](#), en la página 533 y [“Gestión de cuentas de usuario”](#) en la página 542.
- 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.
- Al restaurar una máquina virtual utilizando la modalidad de clonación y utilizando la configuración IP original, asegúrese de que se establecen las credenciales a través de las opciones **Nombre de usuario de SO invitado** y **Contraseña de SO invitado** dentro de la definición de trabajo de copia de seguridad.

### 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, haga clic en **Gestionar protección > Sistemas virtualizados > Hyper-V > Crear trabajo** y, a continuación, seleccione **Restaurar** para abrir el asistente **Restaurar**.


### Sugerencias:


- También puede abrir el asistente pulsando **Trabajos y operaciones > Crear trabajo > Restaurar > Hyper-V**.
- Para obtener un resumen en ejecución de las selecciones en el asistente, pulse **Vista previa de restauración** en el panel de navegación del asistente.
- El asistente se abre en la modalidad de configuración predeterminada. Para ejecutar el asistente en modalidad de configuración avanzada, seleccione **Configuración avanzada**. Con la modalidad de configuración avanzada, puede establecer más opciones para el trabajo de restauración.

2. En la página **Seleccionar origen**, realice 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**, seleccione el tipo de trabajo de restauración que desea crear:

### Bajo demanda

Ejecuta una operación de restauración puntual. 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.

4. Complete los campos de la página **Instantánea de origen** y pulse **Siguiente** para continuar.

Los campos que se muestran dependen del número de elementos seleccionados en la página **Seleccionar origen** y en el tipo de restauración. Algunos campos tampoco se muestran hasta que se selecciona un campo relacionado.

### Campos que se muestran para una restauración de recursos única y bajo demanda

Opción	Descripción
<b>Rango de fechas</b>	Especifique un rango de fechas para mostrar las instantáneas disponibles dentro de ese intervalo.
<b>Tipo de almacenamiento de copias de seguridad</b>	Todas las copias de seguridad del rango de fechas seleccionado se listan en filas que muestran la hora a la que se ha realizado la operación de copia de seguridad y la política de acuerdo de nivel de servicio (SLA) para la copia de seguridad. Seleccione la fila que contiene la hora de la copia de seguridad y la política de SLA que desea y, a continuación, realice una de las siguientes acciones:

Opción	Descripción
	<ul style="list-style-type: none"> <li>Haga clic en el tipo de almacenamiento de copia de seguridad desde el que desea restaurar. Los tipos de almacenamiento que se muestran dependen de los tipos disponibles en el entorno y se muestran en el orden siguiente: <ul style="list-style-type: none"> <li><b>Copia de seguridad</b> Restaura los datos de los que se ha hecho copia de seguridad en un servidor vSnap.</li> <li><b>Réplica</b> Restaura datos que se replican en un servidor vSnap.</li> <li><b>Almacenamiento de objetos</b> Restaura los datos que se copian en un servicio en la nube o en un servidor de repositorio.</li> <li><b>Archivado</b> Restaura los datos que se copian en un archivo de servicio en la nube o en un archivo de servidor de repositorio (cinta).</li> </ul> </li> <li>Haga clic en cualquier sitio en la fila. El primer tipo de copia de seguridad que se muestra secuencialmente desde la izquierda de la fila se selecciona de forma predeterminada. Por ejemplo, si se muestran los tipos de almacenamiento <b>Copia de seguridad</b>, <b>Réplica</b> y <b>Archivado</b>, <b>Copia de seguridad</b> se selecciona de forma predeterminada.</li> </ul>
<b>Utilizar el servidor vSnap alternativo para el trabajo de restauración</b>	<p>Si restaura datos desde un servicio en la nube o un servidor de repositorio, seleccione este recuadro para especificar un servidor vSnap alternativo y, a continuación, seleccione un servidor desde el menú <b>Seleccionar vSnap alternativo</b>.</p> <p>Cuando restaura datos desde un punto de restauración que se ha copiado en 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 copia. Para reducir la carga en el servidor vSnap, puede seleccionar un servidor vSnap alternativo para que sirva como pasarela.</p>

**Campos que se muestran para una instantánea bajo demanda, una restauración de varios recursos o una restauración recurrente**

Opción	Descripción
<b>Tipo de ubicación de restauración</b>	<p>Seleccione un tipo de ubicación desde donde se restauran los datos:</p> <p><b>Sitio</b> El sitio en que se ha realizado la copia de seguridad de instantáneas. El sitio se define en el panel <b>Configuración del sistema &gt; Sitio</b>.</p> <p><b>Servicio en la nube</b> El servicio en la nube en el que se han copiado las instantáneas. El servicio en la nube se define en el panel <b>Configuración del sistema &gt; Almacenamiento de copias de seguridad &gt; Almacenamiento de objetos</b>.</p> <p><b>Servidor de repositorio</b> El servidor de repositorio en el que se han copiado las instantáneas. El servidor de repositorio se define en el panel <b>Configuración del sistema &gt; Almacenamiento de copias de seguridad &gt; Servidor de repositorio</b>.</p>

Opción	Descripción
	<p><b>Archivado de servicio en la nube</b> El servicio de archivado en la nube en el que se copiaron las instantáneas. El servicio en la nube se define en el panel <b>Configuración del sistema &gt; Almacenamiento de copias de seguridad &gt; Almacenamiento de objetos.</b></p> <p><b>Archivado de servidor de repositorio</b> El servidor de repositorio en el que se han copiado las instantáneas en cintas. El servidor de repositorio se define en el panel <b>Configuración del sistema &gt; Almacenamiento de copias de seguridad &gt; Servidor de repositorio.</b></p>
<b>Seleccionar una ubicación</b>	<p>Si está restaurando datos desde un sitio, seleccione una de las siguientes ubicaciones de restauración:</p> <p><b>Demo</b> El sitio de demostración desde el que se restauran las instantáneas.</p> <p><b>Primario</b> El sitio primario desde el que se restauran las instantáneas.</p> <p><b>Secundario</b> El sitio secundario desde el que se restauran las instantáneas.</p> <p>Si está restaurando datos desde un servidor de nube o de repositorio, seleccione un servidor en el menú <b>Seleccionar una ubicación.</b></p>
<b>Selector de fecha</b>	Para las operaciones de restauración bajo demanda, especifique un rango de fechas para mostrar las instantáneas disponibles dentro de ese rango.
<b>Punto de restauración</b>	Para las operaciones de restauración bajo demanda, seleccione una instantánea en la lista de instantáneas disponibles en el rango de fechas seleccionado.
<b>Utilizar el servidor vSnap alternativo para el trabajo de restauración</b>	<p>Si restaura datos desde un servicio en la nube o un servidor de repositorio, seleccione este recuadro para especificar un servidor vSnap alternativo y, a continuación, seleccione un servidor desde el menú <b>Seleccionar vSnap alternativo.</b></p> <p>Cuando restaura datos desde un punto de restauración que se ha copiado en un servicio en la nube o un servidor de repositorio, se utiliza un servidor vSnap como pasarela para completar esta 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 copia. Para reducir la carga en el servidor vSnap, puede seleccionar un servidor vSnap alternativo para que sirva como pasarela.</p>

5. En la página **Establecer destino**, elija la instancia que se va a restaurar para el origen seleccionado y pulse **Siguiente**:

**Host o clúster original**

Seleccione esta opción para restaurar los datos en el host o clúster original.

**Host o clúster 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.

6. 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 de Hyper-V original, esta página no se visualiza.
7. 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.

**Nota:** Cuando se añade una correlación, debe especificarse la dirección IP de origen en el campo mediante el botón **+**. La información de IP de destino debe especificarse en los campos **Subred / Dirección IP**, **Máscara de subred** y **Pasarela**. El redireccionamiento solo se puede realizar en máquinas con las Herramientas de VMware instaladas antes de ejecutar el trabajo de copia de seguridad que se va a restaurar.

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.

8. 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.
9. 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.

10. 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.
11. 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**.
12. 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 286](#)

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 284](#)

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 ejecutar informes.

## Copia de seguridad y restauración de datos de Amazon EC2

Para proteger datos de Amazon EC2, primero añada una cuenta para las instancias de EC2 en IBM Spectrum Protect Plus y, a continuación, cree trabajos para las operaciones de copia de seguridad y restauración para dichas instancias.

Para añadir una cuenta de EC2 a IBM Spectrum Protect Plus, se necesitan claves de acceso. Las claves de acceso son credenciales a largo plazo para un usuario de gestión de identidad y acceso (IAM) o el usuario root de la cuenta de Amazon Web Services (AWS).

Para obtener información sobre cómo crear un usuario de IAM con claves de acceso y los permisos necesarios para IBM Spectrum Protect Plus, consulte [“Creación de un usuario de IAM de AWS” en la página 298](#).

Para mayor seguridad, se recomienda que el usuario root de la cuenta AWS no se utilice para IBM Spectrum Protect Plus. Para obtener más información sobre el usuario root, consulte [Guía de usuario de gestión de gestión de identidad y acceso de AWS](#).

Los datos de EC2 se almacenan en instantáneas en el Elastic Block Store (EBS) de Amazon Web Services (AWS) en lugar de en el servidor vSnap. IBM Spectrum Protect Plus gestiona estas instantáneas para las operaciones de copia de seguridad y restauración.

Asegúrese de que el entorno de EC2 cumple los requisitos del sistema en [“Requisitos de copia de seguridad y restauración de hipervisor \(Microsoft Hyper-V y VMware\) e instancia en la nube \(Amazon EC2\)”](#) en la página 41.

## Creación de un usuario de IAM de AWS

Para completar las tareas en la interfaz de usuario de IBM Spectrum Protect Plus, los usuarios de IAM deben tener claves de acceso y los permisos necesarios.

### Acerca de esta tarea

Puede utilizar la consola de gestión de AWS para crear un usuario de IAM mediante los pasos siguientes. Estos pasos se resumen de los pasos documentados en [Guía de usuario de gestión de gestión de identidad y acceso de AWS](#) para mostrar los valores necesarios para IBM Spectrum Protect Plus. Para obtener los pasos completos y detallados para crear un usuario de IAM, consulte esta guía.

Para crear un usuario, debe tener los permisos administrativos de IAM.

### Procedimiento

1. Inicie sesión en [Consola de gestión de AWS](#) y haga clic en **Servicios > IAM** para abrir la consola de gestión de IAM.
2. En el panel de navegación de la consola, haga clic en **Usuarios > Añadir usuario**.
3. Escriba el nombre de usuario para el usuario nuevo.
4. Seleccione **Acceso programático** para el tipo de acceso AWS.  
Se necesita este tipo de acceso para crear una clave de acceso que requiere IBM Spectrum Protect Plus. IBM Spectrum Protect Plus no requiere el tipo de acceso **Consola de gestión de AWS**.

5. Pulse **Siguiente: Permisos**.

6. Haga clic en **Adjuntar políticas existentes directamente** y, a continuación, haga clic en **Crear política**.

Se abre la página **Crear política** en una ventana de navegador nueva.

7. Haga clic en la pestaña **JSON** y especifique las acciones siguientes:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "ec2:DetachVolume",
        "ec2:AttachVolume",
        "ec2:DeregisterImage",
        "ec2:DeleteSnapshot",
        "ec2:DescribeInstances",
        "ec2:CreateVolume",
        "ec2:DescribeTags",
        "ec2:CreateTags",
        "ec2:RegisterImage",
        "ec2:DescribeRegions",
        "ec2:RunInstances",
        "ec2:DescribeSnapshots",
        "ec2:DescribeAvailabilityZones",
        "ec2:CreateSnapshots",
        "ec2:DescribeVolumes",
        "ec2:CreateSnapshot",
        "ec2:DescribeSubnets",
        "iam:PassRole"
      ]
    }
  ]
}
```



```

    },
    "Resource": "*"
  }
]
}

```

8. Haga clic en **Revisar política**.
9. Escriba un nombre y una descripción (opcional) para la política que está creando.
10. Revise la sección **Resumen** para ver los permisos que otorga la política.
11. Pulse **Crear política**.
12. Cierre la ventana del navegador y vuelva a la ventana que contiene la página **Añadir usuario**.
13. Seleccione la política que ha creado de la lista de políticas.
14. Opcional: Establezca un límite de permisos.
15. Pulse **Siguiente: Códigos**.
16. Opcional: Añada metadatos al usuario adjuntando códigos como pares de valor de clave.  
Puede utilizar códigos para filtrar recursos cuando hace copia de seguridad o restaura datos de EC2.
17. Pulse **Siguiente: Revisar**.
18. Revise las opciones y, a continuación, haga clic en **Crear usuario**.  
Se abre una ventana nueva que muestra el nombre de usuario, la clave de acceso y la clave secreta.
19. Para ver la clave secreta, haga clic en **Mostrar** junto a la clave secreta.
20. Haga clic en **Download.csv** para guardar el ID de clave de acceso y la clave de acceso secreta en un archivo CSV en el sistema.  
Almacene el archivo en una ubicación segura. No puede acceder de nuevo a la clave de acceso secreta después de que se cierre este cuadro de diálogo.
21. Haga clic en **Cerrar** para cerrar la ventana.

#### Qué hacer a continuación

Añada una cuenta para EC2. Para crear una cuenta, siga las instrucciones de [“Adición de una cuenta de Amazon EC2”](#) en la página 299.

## Adición de una cuenta de Amazon EC2

Cuando se añade una cuenta de Amazon EC2 a IBM Spectrum Protect Plus, se captura un inventario de las instancias asociadas con la cuenta. Después, puede ejecutar trabajos de copia de seguridad y restauración y generar informes para las instancias.

#### Antes de empezar

Se necesita una clave de acceso para añadir una cuenta de EC2. La clave de acceso permite a IBM Spectrum Protect Plus conectar a e inventariar instancias de EC2 para la protección de datos. Las claves de acceso que ya se han especificado en IBM Spectrum Protect Plus se proporcionan en una lista de selección. Si la clave de acceso que desea utilizar no está en la lista, debe añadir la clave de acceso y la clave de seguridad. Asegúrese de que tiene la clave de acceso y la clave secreta que desea añadir.

#### Procedimiento

Para añadir una cuenta de EC2, complete los pasos siguientes:

1. En el panel de navegación, pulse **Gestionar protección > Sistemas virtualizados > Amazon EC2**.
2. Haga clic en **Gestionar cuentas**.
3. Pulse **Añadir cuenta**.
4. Rellene los campos de la sección **Propiedades de cuenta**:

##### Nombre de cuenta

Especifique un nombre significativo para identificar la clave de acceso que selecciona para la cuenta.

### Utilizar clave de acceso existente

Para especificar una clave de acceso especificada anteriormente, seleccione esta opción y, a continuación, seleccione la clave desde la lista **Seleccionar una clave**.

Si no selecciona esta opción, complete los campos siguientes para añadir una clave.

#### Clave de acceso

Escriba la clave de acceso.

#### Clave secreta

Escriba la clave secreta.

### 5. Pulse **Guardar**.

IBM Spectrum Protect Plus confirma la conexión de red, añade la cuenta de EC2 a la base de datos y, a continuación, cataloga las instancias de la cuenta.

Si un mensaje indica que la conexión no se ha realizado correctamente, revise las entradas. Si las entradas son correctas y la conexión no es satisfactoria, póngase en contacto con el administrador de red para revisar la conexión.

### Qué hacer a continuación

Cuando añade una cuenta de EC2 a IBM Spectrum Protect Plus, se ejecuta automáticamente un inventario en cada una de las instancias asociadas a la cuenta. Deben detectarse instancias para garantizar que se puede hacer copia de seguridad de ellas. Puede ejecutar un inventario manual en cualquier momento para detectar actualizaciones. Para obtener instrucciones sobre la ejecución de un inventario manual, consulte [“Detección de instancias de Amazon EC2” en la página 300](#).

#### Tareas relacionadas

[“Copia de seguridad de datos de Amazon EC2” en la página 300](#)

Utilice un trabajo de copia de seguridad para hacer copia de seguridad de los datos en una instancia de Amazon EC2.

[“Restauración de datos de Amazon EC2” en la página 302](#)

Utilice un trabajo de restauración para restaurar datos de EC2 desde una copia de seguridad. Por ejemplo, si los datos de una instancia se pierden o se dañan. Puede definir un trabajo que restaure datos en la zona de disponibilidad original o en una zona de disponibilidad diferente en la misma región, con diferentes tipos de configuraciones y opciones de recuperación disponibles.

### Detección de instancias de Amazon EC2

Las instancias de Amazon EC2 se detectan automáticamente una vez se añade una cuenta de EC2 a IBM Spectrum Protect Plus. Sin embargo, puede ejecutar un trabajo de inventario para detectar los cambios que se han producido desde que se ha añadido la cuenta.

### Procedimiento

Para ejecutar un trabajo de inventario, realice los pasos siguientes:

1. En el panel de navegación, pulse **Gestionar protección > Sistemas virtualizados > Amazon EC2**.
2. En la lista de cuentas de EC2, seleccione una cuenta o cuentas, o haga clic en el enlace de una cuenta para navegar a las regiones o instancias que desea en el inventario.

La navegación se encuentra en la cuenta de pedidos > región > instancia.

3. Pulse **Ejecutar inventario**.

### Copia de seguridad de datos de Amazon EC2

Utilice un trabajo de copia de seguridad para hacer copia de seguridad de los datos en una instancia de Amazon EC2.

#### Antes de empezar

Lleve a cabo los pasos siguientes:

1. Asegúrese de que se añaden las cuentas de las que se va a hacer una copia de seguridad IBM Spectrum Protect Plus. Para obtener más instrucciones, consulte [“Adición de una cuenta de Amazon EC2”](#) en la página 299.
2. Asegúrese de que se han configurado una o más políticas de SLA para las instancias de EC2. Para obtener más instrucciones, consulte [“Creación de una política de SLA para instancias de Amazon EC2”](#) en la página 248.
3. Asegúrese de que se asignan los roles y grupos de recursos de IBM Spectrum Protect Plus al usuario que ha configurado el trabajo de restauración. Para obtener más información sobre la asignación de roles, consulte [Capítulo 18, “Gestión del acceso de usuarios”](#), en la página 533.
4. Si una cuenta está asociada con varias políticas de SLA, asegúrese de que las políticas no están planificadas 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.

## Procedimiento

Para definir un trabajo de copia de seguridad de EC2, complete los pasos siguientes:

1. En el panel de navegación, pulse **Gestionar protección > Sistemas virtualizados > Amazon EC2**.
2. Seleccione las instancias a las que hacer copia de seguridad en el panel Copia de seguridad de Amazon EC2 realizando una de las siguientes acciones:
  - Para seleccionar todas las instancias que están asociadas con una cuenta de EC2, marque la casilla de selección de la cuenta. Las instancias que se añaden a esta cuenta se asignan automáticamente a la política de SLA que elija.
  - Para seleccionar instancias por región o instancias específicas, pulse el nombre de la cuenta y vaya a la región o instancia. La navegación se encuentra en la cuenta de pedidos > región > instancia. Si una instancia no tiene un nombre asignado, el ID de instancia se muestra como el nombre de instancia.

Para buscar instancias disponibles, utilice la función de búsqueda y alterne entre las instancias visualizadas utilizando el filtro **Ver**. Las opciones disponibles son **Instancias** y **Etiquetas**.

3. Haga clic en **Seleccionar política de SLA** para añadir una o más políticas de SLA que cumplan los criterios de copia de seguridad en la definición de trabajo de la tabla **Estado de política de SLA**.
4. Opcional: Para configurar opciones adicionales para las políticas de SLA que ha añadido a la definición, en la columna **Opciones de política** de la tabla **Estado de política de SLA**, haga clic en el icono de

portapapeles para una política de  y establezca las opciones siguientes.

Si el trabajo ya está configurado, pulse el icono para editar la configuración.

## 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 admiten 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 continuar 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 completa el proceso con un código de retorno distinto de cero, el estado de la tarea de script posterior se notifica 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 las instancias seleccionadas antes de iniciar el trabajo de copia de seguridad.

### **Excluir recursos**

Excluya instancias específicas del trabajo de copia de seguridad utilizando patrones de exclusión individuales 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.

#### **5. Pulse **Guardar** para crear la definición de trabajo.**

El trabajo se ejecutará según lo definido por las políticas de SLA que ha seleccionado. Para ejecutar el trabajo inmediatamente, haga clic en **Trabajos y operaciones > Planificar**. Seleccione el trabajo y pulse **Acciones > Iniciar**.

**Consejo:** Cuando se ejecuta un trabajo para la política de SLA seleccionada, todas las instancias que están asociadas con esa política de SLA se incluyen en la operación de copia de seguridad. Para hacer copia de seguridad únicamente de las instancias seleccionadas, puede ejecutar un trabajo bajo demanda. Un trabajo bajo demanda ejecuta inmediatamente la operación de copia de seguridad.

- Para ejecutar un trabajo de copia de seguridad bajo demanda para una única instancia, seleccione la instancia y haga clic en **Ejecutar**. Si el recurso no está asociado con una política de SLA, el botón **Ejecutar** no está disponible.
- Para ejecutar un trabajo de copia de seguridad bajo demanda para una o más instancias, haga clic en **Crear trabajo**, seleccione **Copia de seguridad ad hoc** y siga las instrucciones en [“Ejecución de un trabajo de copia de seguridad ad hoc”](#) en la página 517.

### **Qué hacer a continuación**

Después de definir un trabajo de copia de seguridad de EC2, cree una definición de trabajo de restauración de EC2.

### **Conceptos relacionados**

[“Configuración de scripts para las operaciones de copia de seguridad y restauración”](#) en la página 518

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**

[“Restauración de datos de Amazon EC2”](#) en la página 302

Utilice un trabajo de restauración para restaurar datos de EC2 desde una copia de seguridad. Por ejemplo, si los datos de una instancia se pierden o se dañan. Puede definir un trabajo que restaure datos en la zona de disponibilidad original o en una zona de disponibilidad diferente en la misma región, con diferentes tipos de configuraciones y opciones de recuperación disponibles.

[“Inicio de trabajos bajo demanda”](#) en la página 512

Puede ejecutar cualquier trabajo bajo demanda, incluso si el trabajo se ha establecido para que se ejecute en una planificación.

## **Restauración de datos de Amazon EC2**

Utilice un trabajo de restauración para restaurar datos de EC2 desde una copia de seguridad. Por ejemplo, si los datos de una instancia se pierden o se dañan. Puede definir un trabajo que restaure datos en la zona

de disponibilidad original o en una zona de disponibilidad diferente en la misma región, con diferentes tipos de configuraciones y opciones de recuperación disponibles.

### Antes de empezar

Complete las tareas siguientes:

- Asegúrese de que el trabajo de copia de seguridad de EC2 se ha ejecutado al menos una vez. Para obtener instrucciones, consulte [“Copia de seguridad de datos de Amazon EC2”](#) en la página 300.
- Asegúrese de que se asignan los roles y grupos de recursos de IBM Spectrum Protect Plus al usuario que ha configurado el trabajo de restauración. Para obtener más información sobre la asignación de roles, consulte [Capítulo 18, “Gestión del acceso de usuarios”](#), en la página 533.

### Acerca de esta tarea


IBM Spectrum Protect Plus utiliza la modalidad de clonación para crear copias de instancias a largo plazo.

### Procedimiento

Para definir un trabajo de restauración de EC2, complete los pasos siguientes:


1. En el panel de navegación, haga clic en **Gestionar protección > Sistemas virtualizados > Amazon EC2 > Crear trabajo** y, a continuación, seleccione **Restaurar** para abrir el asistente **Restaurar**.

#### Sugerencias:

- También puede abrir el asistente haciendo clic en **Trabajos y operaciones > Crear trabajo > Restaurar > Amazon EC2**.
  - Para obtener un resumen en ejecución de las selecciones en el asistente, pulse **Vista previa de restauración** en el panel de navegación del asistente.
  - El asistente se abre en la modalidad de configuración predeterminada. Para ejecutar el asistente en modalidad de configuración avanzada, seleccione **Configuración avanzada**. Con la modalidad de configuración avanzada, puede establecer más opciones para el trabajo de restauración.
2. En la página **Seleccionar origen**, realice las acciones siguientes:
    - a) Pulse una cuenta de la lista para mostrar las instancias que están disponibles para las operaciones de restauración. También puede utilizar la función de búsqueda para buscar instancias disponibles. Especifique todo o parte de un nombre para ubicar instancias que coincidan con los criterios de búsqueda. Puede utilizar el carácter comodín (\*) para representar todo o parte de un nombre. Utilice el filtro **Ver** para alternar entre las instancias visualizadas.
    - b) Haga clic en el icono del signo más  junto a la instancia que desea utilizar como origen de la operación de restauración.

Puede seleccionar más de una instancia de la lista. Sin embargo, todas las instancias seleccionadas deben estar en la misma región.

Si la instancia tiene volúmenes adjuntos, puede navegar a los volúmenes y seleccionarlos para la operación de restauración. No puede seleccionar instancias ni volúmenes adjuntos.

Las instancias o volúmenes adjuntos seleccionados se añaden a la lista de restauración junto a la lista de cuentas. 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. Complete los campos en la página **Instantánea de origen** para seleccionar las instantáneas de instancia que desea restaurar y haga clic en **Siguiente** para continuar.

Los campos que se muestran dependen del número de instancias seleccionadas en la página **Seleccionar origen**.

    - Si se selecciona una instancia única, seleccione el rango de fechas para las instantáneas que desea restaurar. Se listan las instantáneas que están disponibles para ese rango de fechas. Seleccione la instantánea que desea restaurar.

- Si se seleccionan varias instancias, seleccione el rango de fechas para las instantáneas que desea restaurar. Se listan las instancias que tienen instantáneas dentro de ese rango de fechas. Para cada instancia, seleccione el punto de restauración que desea restaurar.
4. En la página **Establecer destino**, especifique la zona de disponibilidad donde desea restaurar las instancias y haga clic en **Siguiente**:
- Zona de disponibilidad original**  
 Seleccione esta opción para restaurar instancias en la zona de disponibilidad original.
- Zona de disponibilidad alternativa**  
 Seleccione esta opción para restaurar instancias en una zona de disponibilidad diferente de la zona de disponibilidad original y, a continuación, seleccione la ubicación alternativa de los recursos disponibles.
- Si está restaurando un volumen adjunto, seleccione la instancia de destino en la zona de disponibilidad alternativa y especifique un nombre de dispositivo opcional en la sección **Conexión de destino**.
5. En la página **Establecer reds**, cambie la subred para cada zona de disponibilidad si ha seleccionado **Zonas de disponibilidad alternativas** en la página **Establecer destino**. Si ha seleccionado **Zona de disponibilidad original**, no se proporcionan valores en esta página. Pulse **Siguiente** para continuar.
- La subred de la zona de disponibilidad debe estar en la misma región que las instancias seleccionadas en el paso “2” en la página 303.
6. En la página **Método de restauración**, puede cambiar el nombre de la instancia restaurada especificando el nombre de instancia nuevo en el campo **Cambiar nombre de instancia (opcional)**. Pulse **Siguiente** para continuar.
7. Si está ejecutando el trabajo de restauración en modalidad avanzada, puede establecer opciones adicionales como se indica a continuación:

**Encender después de la recuperación**

Alterne el estado de alimentación de una instancia después de que se ejecute una recuperación. Las instancias se encienden en el orden en el que se recuperan.

**Continuar con la restauración incluso si falla**

Alterne la recuperación de una instancia en una serie si falla la recuperación de la instancia anterior. Si está inhabilitado, el trabajo de restauración se detiene si falla la recuperación de una instancia.

**Ejecutar la limpieza inmediatamente en caso de anomalía del trabajo**

Habilite esta opción para borrar automáticamente recursos asignados como parte de un trabajo de restauración si la recuperación de la instancia falla.

**Restaurar códigos de instancia**

Habilite esta opción para restaurar códigos que se aplican a instancias a través de vSphere.

**Agregar al principio el prefijo para el nombre de instancia**

Especifique un prefijo para añadirlo a los nombres de instancias restauradas.

**Añadir sufijo al nombre de instancia**

Especifique un sufijo para añadirlo a los nombres de instancias restauradas.

8. 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.

9. En la página **Revisar**, revise los valores del trabajo de restauración y pulse **Enviar** para crear el trabajo.

## Resultados

El trabajo comienza después de hacer clic en **Enviar** y se añade el registro **onDemandRestore** al panel **Sesiones de trabajo** en breve. Para ver el progreso de la operación de restauración, expanda el trabajo.

También puede descargar el archivo de registro pulsando el icono de descarga  .

Todos los trabajos en ejecución se pueden visualizar en la página **Trabajos y operaciones > Trabajos en ejecución**.

## Tareas relacionadas

[“Adición de una cuenta de Amazon EC2” en la página 299](#)

Cuando se añade una cuenta de Amazon EC2 a IBM Spectrum Protect Plus, se captura un inventario de las instancias asociadas con la cuenta. Después, puede ejecutar trabajos de copia de seguridad y restauración y generar informes para las instancias.

## 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 44](#).
- 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 que se copiaron 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 de SO de 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 realizando 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 posterior. 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 567.
  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.
- Nota:** Solo serán visibles los objetos de archivo para los que se ha realizado una instantánea durante el rango de fechas especificado. En esos objetos, cuando se pulsa la flecha al lado del objeto de archivo, se visualizan todas las instantáneas previas para ese objeto de archivo.
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 de SO de 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 262](#)

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 273](#)

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 11. Protección de sistemas de archivos

Los sistemas de archivos que contienen directorios y archivo que desea proteger se pueden registrar con IBM Spectrum Protect Plus. Seleccione los servidores de sistema de archivos y las unidades que contienen datos que desea proteger. Los sistemas de archivos ReFS y NTFS de Microsoft Windows pueden registrarse con IBM Spectrum Protect Plus para que pueda configurar los trabajos de copia de seguridad y las políticas de acuerdo de nivel de servicio (SLA) planificadas regularmente.

Puede proteger los sistemas de archivos locales que se asignan a una letra de unidad. Los volúmenes en clúster y las unidades compartidas no están protegidos por IBM Spectrum Protect Plus.

## Windows sistemas de archivos

Después de registrar correctamente la máquina que aloja Microsoft Windows NTFS o ReFS sistema de archivos con IBM Spectrum Protect Plus, puede empezar a proteger los datos de los volúmenes y unidades de la lista. También puede crear una copia de seguridad bajo demanda de los datos de los sistemas de archivos, o establecer políticas de acuerdo de nivel de servicio (SLA) para ejecutar trabajos de copia de seguridad planificada regulares.

Asegúrese de que el entorno en el que se encuentra sistema de archivos cumple los requisitos mínimos del sistema. Para obtener más información sobre los requisitos del sistema, consulte [“Requisitos de Sistema de archivos”](#) en la página 51.

La dirección IP de la máquina que registra debe ser accesible desde el servidor de IBM Spectrum Protect Plus y desde el servidor vSnap. Ambos deben tener un servicio de gestión remota de Windows que esté a la escucha en el puerto 5985.

Se debe poder resolver y redirigir el nombre de dominio completo desde el servidor de dispositivo IBM Spectrum Protect Plus y desde el servidor vSnap.

## Requisitos previos para sistemas de archivos

Deben cumplirse todos los requisitos previos para utilizar IBM Spectrum Protect Plus consisten en sistemas de archivos antes de empezar a proteger sus datos.

Los requisitos para trabajar con sistemas de archivos con IBM Spectrum Protect Plus están disponibles aquí, [“Requisitos de Sistema de archivos”](#) en la página 51.

**Nota:** El ID de usuario para registrar servidores de archivos de Windows se puede configurar con una de las siguientes configuraciones de Windows:

- La cuenta de usuario *Administrador del sistema local* con el componente de seguridad Control de cuenta de usuario (UAC) establecido en Inhabilitado. Con este usuario debe abrir el sistema Windows **Panel de control > Valores de control de cuenta de usuario** y mover el control deslizante a **No notificar nunca**.
- Un usuario que es miembro del Grupo de administradores locales con el valor de política de seguridad Modalidad de aprobación de administrador inhabilitado. Con este usuario, debe abrir el sistema Windows **Política de seguridad local**. En el menú **Configuración de seguridad**, elija **Políticas locales > Opciones de seguridad > Control de cuenta de usuario: Ejecutar todos los administradores en la política Modalidad de aprobación de administración** y establezca esta opción en Inhabilitado. Asegúrese de que el Grupo de administradores locales incluye la opción de política Iniciar sesión como servicio.

## Requisitos previos de espacio

Asegúrese de que tiene espacio suficiente en la máquina que aloja el sistema de archivos que está protegiendo. Para obtener más información sobre los requisitos de espacio, consulte [“Requisitos de](#)

espacio para la protección de sistemas de archivos” en la página 310. Cuando restaure datos en una ubicación alternativa, permita espacio adicional. Los archivos no se sobrescriben durante el proceso de restauración. Cuando se encuentran archivos de nombres idénticos, se conservan ambas copias.

### Gestión de un certificado de seguridad para Windows

Para el acceso seguro para proteger los archivos del sistema de archivos con IBM Spectrum Protect Plus, debe crear un certificado y gestionar su ubicación.

#### Acerca de esta tarea

**Nota:** Si el servicio de restauración no puede cargar el certificado, se suprimen los archivos y se crean una clave y un certificado autofirmado nuevos.

**Consejo:** Si se ha ejecutado el agente de sistema de archivos de IBM Spectrum Protect Plus, encontrará un certificado autofirmado y una clave en la ubicación siguiente: %LOCALAPPDATA%\FSPA\. Si el agente no se ha ejecutado todavía, siga los pasos para crear y mover el certificado autofirmado y la clave.

El administrador puede acceder a este directorio en la vía de acceso siguiente: C:\Users\Administrator\AppData\Local\

#### Procedimiento

1. Cree una clave y un certificado firmado para la máquina cliente.  
Ni la clave ni el certificado pueden tener una protección de paráfrasis ya que esto afecta a la carga de archivos.
2. Cree una carpeta de directorio llamada FSPA en una ubicación como esta %LOCALAPPDATA%\FSPA.
3. Copie la clave y el certificado y colóquelos en la carpeta FSPA.
4. Copie la clave y el certificado en esta carpeta.
5. Cambie el nombre de la clave por `localfspagent.key`.
6. Cambie el nombre del certificado por `localfspagent.crt`.

### Requisitos de espacio para la protección de sistemas de archivos

Antes de empezar a hacer una copia de seguridad de los datos que se almacenan en el sistema de archivos registrado, asegúrese de que tiene suficiente espacio libre de disco en los host de origen y de destino y en el repositorio de vSnap.

## Adición de un sistema de archivos

Para empezar a proteger los datos en un ReFS o NTFS de sistema de archivos, debe añadir la dirección host donde se encuentra sistema de archivos. Puede repetir el procedimiento para añadir cada host que desee proteger con IBM Spectrum Protect Plus.

#### Antes de empezar

**Nota:** El ID de usuario para registrar servidores de archivos de Windows se puede configurar con una de las siguientes configuraciones de Windows:

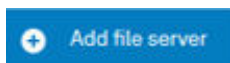
- La cuenta de usuario *Administrador del sistema local* con el componente de seguridad Control de cuenta de usuario (UAC) establecido en Inhabilitado. Con este usuario debe abrir el sistema Windows **Panel de control > Valores de control de cuenta de usuario** y mover el control deslizante a **No notificar nunca**.
- Un usuario que es miembro del Grupo de administradores locales con el valor de política de seguridad Modalidad de aprobación de administrador inhabilitado. Con este usuario, debe abrir el sistema Windows **Política de seguridad local**. En el menú **Configuración de seguridad**, elija **Políticas locales > Opciones de seguridad > Control de cuenta de usuario: Ejecutar todos los administradores en la política Modalidad de aprobación de administración** y establezca esta opción en Inhabilitado. Asegúrese de que el Grupo de administradores locales incluye la opción de política **Iniciar sesión como servicio**.

## Acerca de esta tarea

Para añadir un sistema de archivos a IBM Spectrum Protect Plus, debe tener el nombre DNS o la dirección IP de la máquina, un ID de usuario y la contraseña.

## Procedimiento

1. En el panel de navegación, expanda **Gestionar protección > Sistemas de archivos > Microsoft Windows**.
2. En la página **Microsoft Windows**, haga clic en **Gestionar servidores de archivos** y, a continuación, en **Añadir servidor de archivos** para añadir el servidor de host.



*Figura 22. Adición de un servidor de sistema de archivos*

3. En la sección **Propiedades del servidor de archivos**, especifique el nombre DNS o la dirección IP de la máquina.
4. Especifique el tipo de usuario para el servidor Windows que está añadiendo.
  - Use un ID de usuario y una contraseña existentes.
  - Especifique un ID de usuario y una contraseña nuevos.

**Nota:** El ID de usuario para registrar sistemas de archivos de Windows debe configurarse con una de las siguientes configuraciones de Windows:

- La cuenta de usuario Administrador de sistema local con el componente de seguridad Control de cuenta de usuario (UAC) inhabilitado. Con este usuario, debe acceder al cuadro de diálogo Valores de control de cuenta de usuario en el sistema Windows **Panel de control** y mover el control deslizante a **Nunca**.
- Un usuario que es miembro del Grupo de administradores locales con el valor de política de seguridad Modalidad de aprobación de administrador inhabilitado. Con este usuario debe acceder al cuadro de diálogo Valores de seguridad local del sistema Windows e inhabilitar el valor **Control de cuenta de usuario: Ejecutar todos los administradores en la política Modalidad de aprobación de administración**. Asegúrese de que el Grupo de administradores locales incluye la opción de política **Iniciar sesión como servicio**.

Figura 23. Gestión de usuarios agentes

**Importante:** Cuando especifica el ID de usuario, no necesita especificar el dominio.

5. Establezca el número máximo de sistemas de archivos paralelos que se van a utilizar para realizar una copia de seguridad de datos del sistema de archivos que está protegido.

Este valor se aplica a todos los sistemas de archivos en este host. Se puede hacer copia de seguridad de varios recursos en paralelo cuando el valor de la opción se establece en más de 1. Varios sistemas de archivos paralelos pueden acelerar las operaciones de restauración.

6. Guarde el formulario.

### Qué hacer a continuación

Después de añadir el host de sistema de archivos a IBM Spectrum Protect Plus, se ejecuta automáticamente un inventario para detectar los volúmenes y unidades relevantes.

Para verificar que se han añadido las unidades y los volúmenes, revise el registro de trabajo. Vaya a



**Trabajos y operaciones,** Haga clic en la pestaña **Trabajos en ejecución** y busque la entrada de registro Inventario del servidor de aplicaciones que se corresponde con el inventario que se ha iniciado.

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 sistemas de archivos para garantizar que se pueden proteger. Para obtener instrucciones sobre la ejecución de un inventario, consulte [Detección de sistemas de archivos](#).

### Ejecución de un inventario para detectar sistemas de archivos

Después de añadir un sistema de archivos a IBM Spectrum Protect Plus, se ejecuta automáticamente un inventario para detectar volúmenes, unidades y puntos de montaje. El inventario detecta, lista y almacena los recursos de sistema de archivos que se encuentran en el host seleccionado y hace que los datos estén disponibles para la protección con IBM Spectrum Protect Plus.

## Antes de empezar

Asegúrese de que ha añadido sistema de archivos a IBM Spectrum Protect Plus. Para obtener instrucciones, consulte [Adición de un sistema de archivos](#).

## Procedimiento

1. En el panel de navegación, expanda **Gestionar protección** > **Sistemas de archivos** > **Microsoft Windows**.

**Consejo:** Para añadir sistemas de archivos al panel **Servidores**, siga las instrucciones en [Adición de un sistema de archivos](#).

2. Haga clic en **Ejecutar inventario**, .

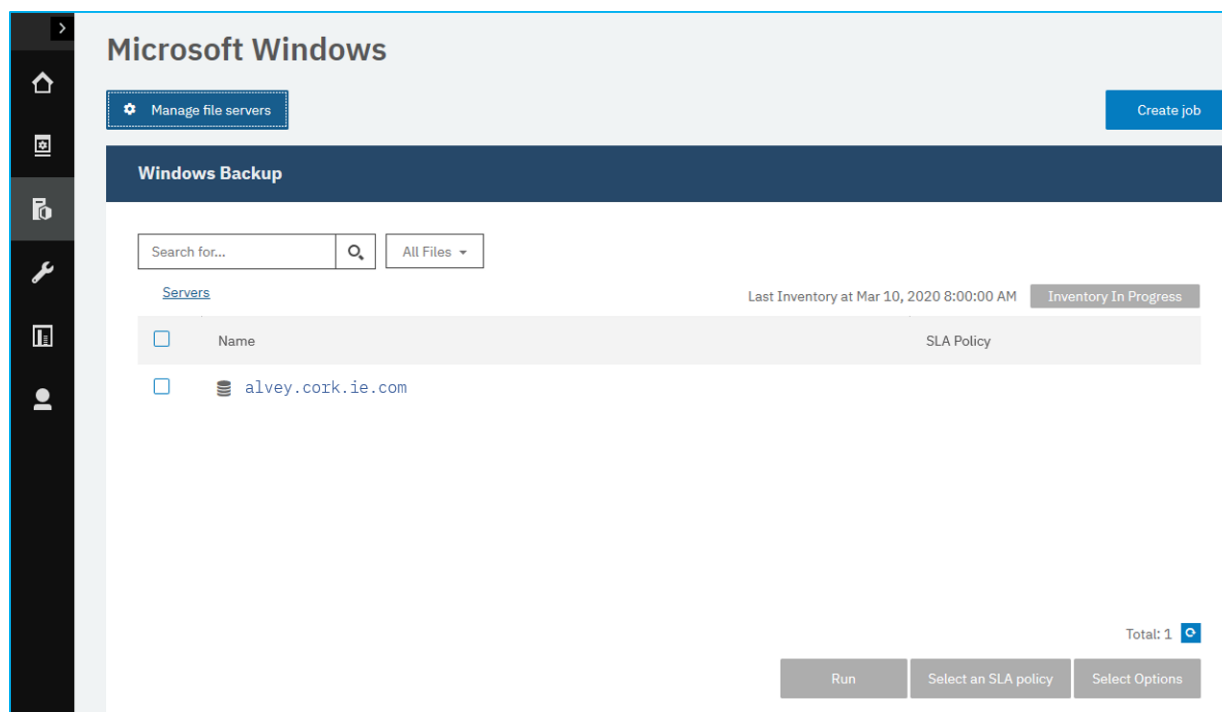



Figura 24. Detección de sistemas de archivos

Cuando se ejecuta un inventario, el texto cambia para mostrar **Inventario en curso**. Puede ejecutar un inventario en cualquier servidor de sistema de archivos, pero solo puede ejecutar un proceso de inventario a la vez.



Para ver el registro de trabajo, vaya a **Trabajos y operaciones**, . Haga clic en la pestaña **Trabajos en ejecución** y busque la entrada de registro Inventario del 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. Si no se visualiza el trabajo, ajuste el **Periodo del historial de trabajos** a un intervalo de tiempo más largo.

3. Haga clic en un servidor para abrir una vista que muestre los volúmenes, unidades y puntos de montaje detectados para ese servidor. Si faltan entradas de la lista **Servidores**, compruebe sistemas de archivos y vuelva a ejecutar el inventario. En algunos casos, determinadas entradas se marcan como no elegibles para la copia de seguridad; pase el cursor por encima de la entrada para revelar el motivo de porqué no lo son.

**Consejo:** Para volver a la lista de servidores, haga clic en el hipertexto **Servidores**.

## Prueba de conexión de sistemas de archivos

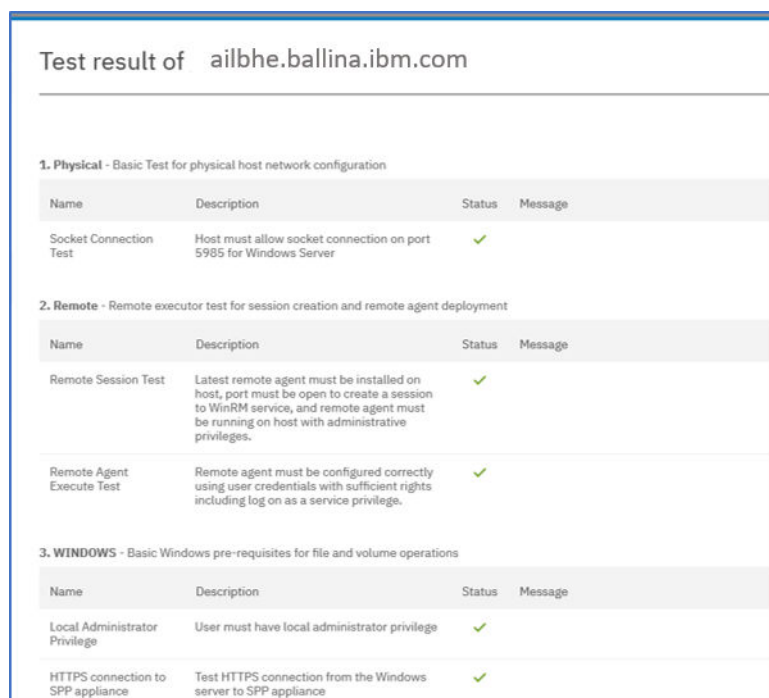
Después de añadir un sistemas de archivos, puede probar la conexión. La prueba verifica la comunicación con los valores del servidor y de DNS entre IBM Spectrum Protect Plus y el servidor de sistemas de archivos.

### Procedimiento

1. En el panel de navegación, haga clic en **Gestionar protección > Sistemas de archivos > Microsoft Windows**.
2. En la ventana **Microsoft Windows**, haga clic en **Gestionar servidores de archivo** y seleccione la **Dirección de host** que desea probar.

Se muestra una lista de los host de máquina que están disponibles.

3. Haga clic en **Acciones** y seleccione **Probar** para iniciar las pruebas de verificación para la conexión de red física, el acceso remoto y las conexiones y valores de los privilegios de Windows.



<b>1. Physical</b> - Basic Test for physical host network configuration			
Name	Description	Status	Message
Socket Connection Test	Host must allow socket connection on port 5985 for Windows Server	✓	
<b>2. Remote</b> - Remote executor test for session creation and remote agent deployment			
Name	Description	Status	Message
Remote Session Test	Latest remote agent must be installed on host, port must be open to create a session to WinRM service, and remote agent must be running on host with administrative privileges.	✓	
Remote Agent Execute Test	Remote agent must be configured correctly using user credentials with sufficient rights including log on as a service privilege.	✓	
<b>3. WINDOWS</b> - Basic Windows pre-requisites for file and volume operations			
Name	Description	Status	Message
Local Administrator Privilege	User must have local administrator privilege	✓	
HTTPS connection to SPP appliance	Test HTTPS connection from the Windows server to SPP appliance	✓	

Figura 25. Probar la conexión

El informe de prueba muestra una lista de las pruebas que se han ejecutado. Consta de una prueba de la configuración de red de host física, para la instalación del servidor remoto en el host, y los privilegios y conexiones de Windows.

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 del sistema de archivos

Defina trabajos de copia de seguridad regulares y especifique opciones para ejecutar y crear copias de seguridad para proteger los datos del sistema de archivos.

### 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 de sistema de archivos de IBM Spectrum Protect Plus monta el recurso compartido en el servidor 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 sistema de archivos a los que desea hacer copia de seguridad. Para ver el procedimiento, consulte [Adición de un servidor de sistema de archivos](#).
- Configure una política de acuerdo de nivel de servicio (SLA) tal como se describe en esta tarea.
- 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 18, “Gestión del acceso de usuarios”](#), en la página 533.
- Los trabajos de inventario no deben planificarse para ejecutarse al mismo tiempo que los trabajos de copia de seguridad.

La operación de copia de seguridad falla si la vía de acceso supera los 255 caracteres. Si las vías de acceso tienen más de 255 caracteres, debe habilitar vías de acceso más largas utilizando la opción **Habilitar vías de acceso largas de Win32** en el editor de políticas de Windows.

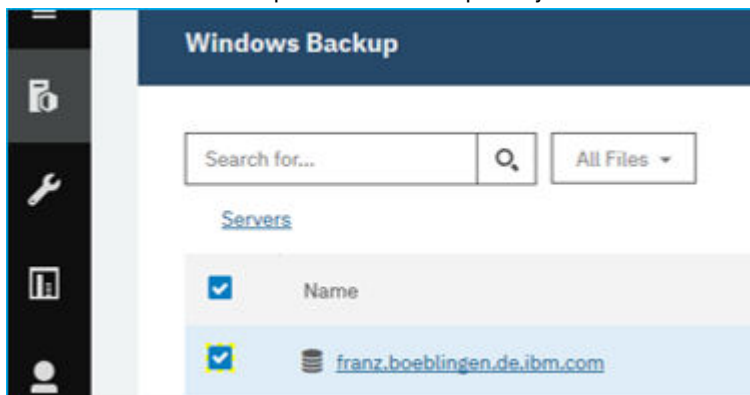
**Nota:** Ni los recursos compartidos del sistema de archivos ni los volúmenes de clúster de Microsoft se pueden proteger con IBM Spectrum Protect Plus.

### Acerca de esta tarea

Los pasos siguientes describen cómo hacer copia de seguridad de los recursos asignados a una política de SLA. Para ejecutar un trabajo de copia de seguridad bajo demanda para uno o más recursos independientemente de si esos recursos ya están asociados a una política de SLA, haga clic en **Crear trabajo**, seleccione **Copia de seguridad ad hoc** y siga las instrucciones en [“Ejecución de un trabajo de copia de seguridad ad hoc”](#) en la página 517.

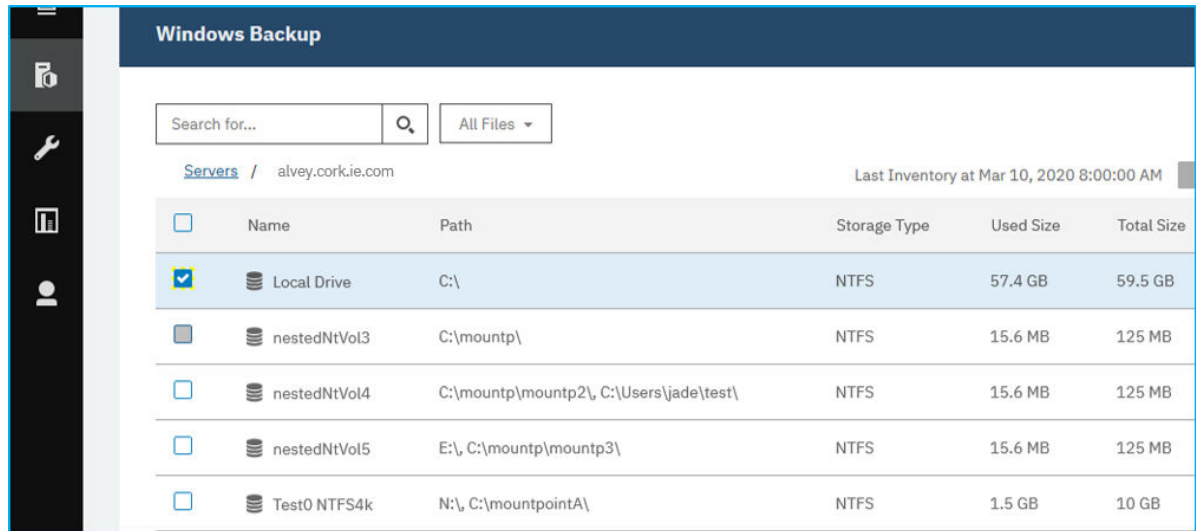
### Procedimiento


1. En el panel de navegación, expanda **Gestionar protección > Sistemas de archivos > Microsoft Windows**.
2. Seleccione un servidor de sistema de archivos para hacer copia de seguridad en el panel **Copia de seguridad de Windows**.
  - Puede seleccionar un servidor de sistema de archivos entero haciendo clic en la casilla de verificación del nombre de servidor. Todos los datos añadidos a este servidor se asignan automáticamente a la política de SLA que elija.



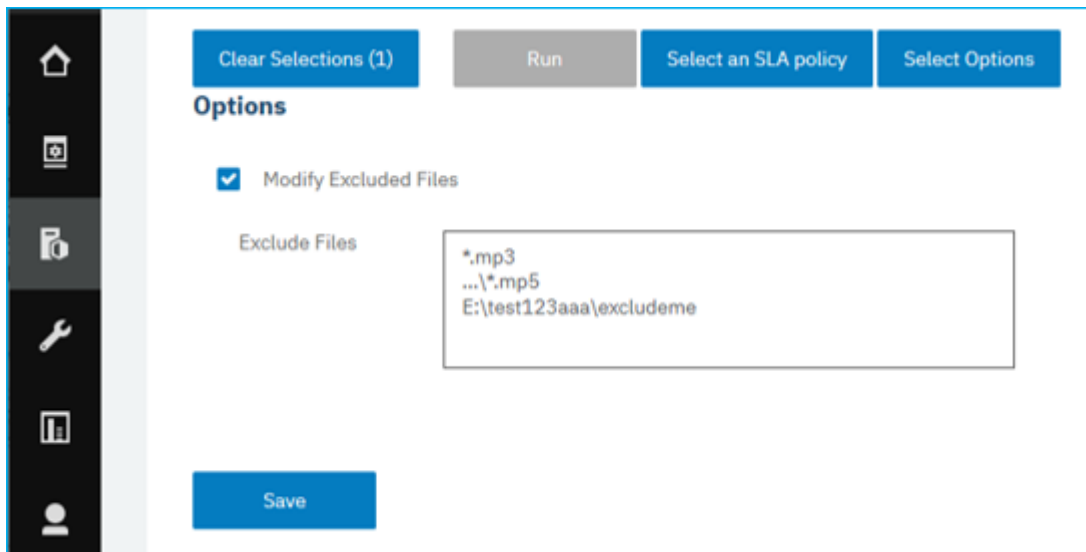
- O bien, puede seleccionar una unidad o punto de montaje específicos de un servidor del sistema de archivos específico haciendo clic en el nombre del servidor o eligiendo una unidad o punto de

montaje de la lista.




3. Haga clic en **Seleccionar opciones**  para especificar los archivos que se van a excluir del trabajo de copia de seguridad que está configurando. De forma alternativa, puede hacer clic en **Modificar archivos excluidos** para dejar las reglas de exclusión ya que ya están definidas. Haga clic en **Guardar** para confirmar los cambios.

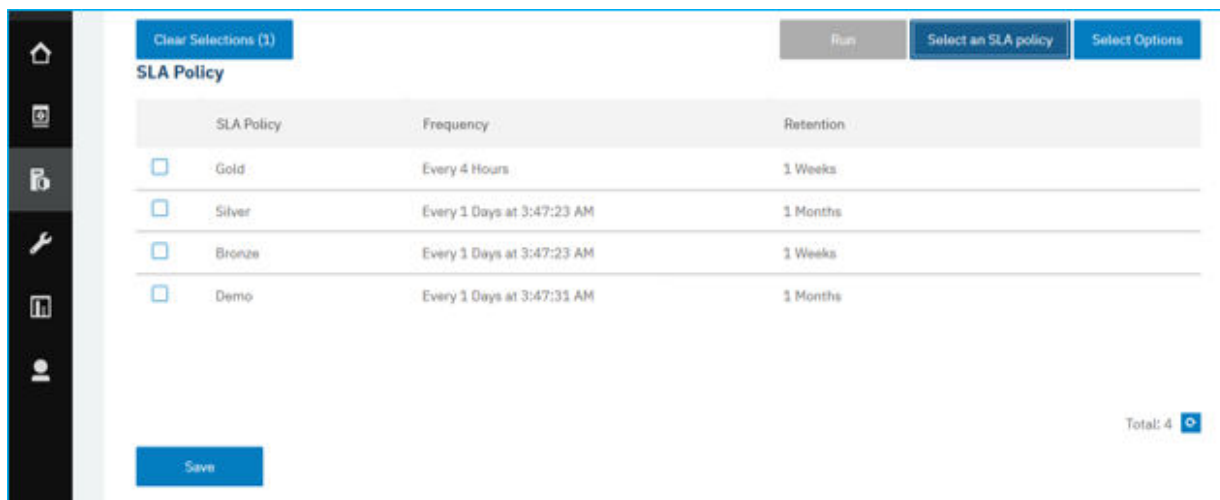
Si desea excluir todos los archivos de una unidad, puede especificar la unidad o una carpeta de la unidad como Z:\test. Si desea excluir todos los archivos de un determinado tipo del trabajo de copia de seguridad, puede especificar esa exclusión utilizando una serie como este ejemplo \*.png.




**Consejo:** Para cerrar el panel **Opciones** sin guardar los cambios, pulse **Seleccionar opciones**.

4. Seleccione el servidor de sistemas de archivos, unidad o punto de montaje para la copia de seguridad y haga clic en **Seleccionar una política de SLA**  para elegir una política de SLA para ese elemento.

Puede elegir entre las opciones siguientes: Oro, Plata o Bronce. Cada tipo de política tiene tasas de retención y frecuencias diferentes, tal y como se muestra en la imagen siguiente:



Si desea definir una política de SLA nueva, seleccione **Gestionar protección > Visión general de políticas**. En el panel **Políticas de SLA**, pulse **Añadir política de SLA** y defina las preferencias de política. Para editar una política existente con tasas de frecuencia y retención personalizadas, haga

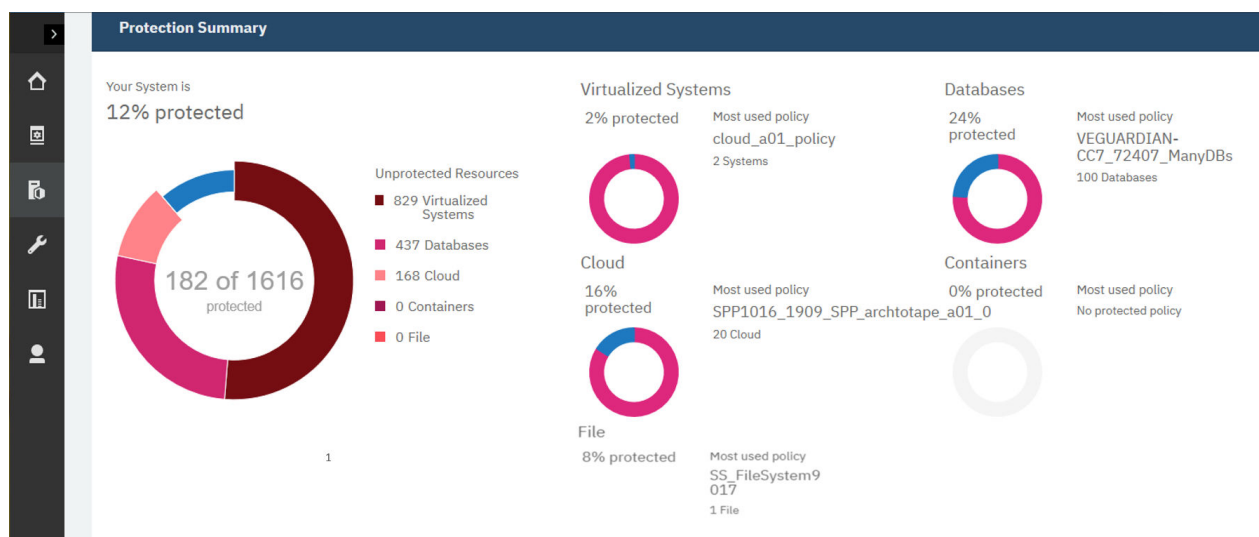
clic en el icono de edición  y defina sus preferencias. Haga clic en **Guardar** para confirmar los cambios.

5. Pulse **Guardar** para guardar la política de SLA.

Si desea ejecutar el trabajo de copia de seguridad inmediatamente, pulse **Acciones > Inicio**. El estado del registro cambia para mostrar que la copia de seguridad es En ejecución.

### Qué hacer a continuación

Para ver el estado de las políticas de SLA del sistema de archivos existente, seleccione **Gestionar protección > Visión general de políticas** para ver un resumen de su protección, tal como se muestra en la imagen siguiente:



### Excluir sintaxis de reglas

Cuando hace copias de seguridad de los sistemas de archivos, puede definir las reglas de exclusión para excluir determinadas unidades, directorios o archivos de los trabajos de copia de seguridad. No se hace copia de seguridad de estos archivos como parte de la política de SLA o como parte del trabajo de copia de seguridad ad hoc que está ejecutando. Cuando ejecuta un trabajo de restauración, las reglas de exclusión significan que las unidades, directorios o archivos especificados en las reglas de exclusión no se restauran en la nueva copia.

Las reglas de exclusión se pueden definir para la aplicación de sistema de archivos Windows entera. Las reglas que definen los recursos excluidos se heredan en cada uno de los sistemas de archivos que se están protegiendo. Si desea definir reglas nuevas para una instancia de sistema de archivos particular, puede añadir las reglas existentes en la ventana **Gestionar protección > Sistemas de archivos > Microsoft Windows Copia de seguridad de Windows**. Las reglas nuevas que define para ese trabajo de copia de seguridad del sistema de archivos sustituye el conjunto de reglas de exclusión para los sistemas de archivos Windows. Para obtener más información sobre la definición de un trabajo de copia de seguridad, consulte [“Copia de seguridad de datos del sistema de archivos”](#) en la página 314.

Si desea excluir un archivo, puede especificar el nombre del archivo de la siguiente manera `Z:\test\excludedFile.txt`. Si desea excluir todos los archivos de una carpeta, puede especificar una regla como esta `Z:\test\*`. Si desea excluir una carpeta, puede especificar una regla como esta `DIR Z:\excludedFolder`.

Tabla 56. Sintaxis de reglas de exclusión para Windows	
Sintaxis	Comportamiento de la sintaxis
:\ 	<ul style="list-style-type: none"> <li>Indica un sistema de archivos y una unidad Windows.</li> <li>Debe incluirse en todas las reglas excepto para la regla FS.</li> <li>Una regla no puede comenzar o terminar con esta sintaxis.</li> <li>Una regla debe comenzar con una letra de unidad o un comodín seguido de esta secuencia.</li> </ul>
\	<ul style="list-style-type: none"> <li>Indica el siguiente nivel de directorio.</li> <li>Una regla no puede terminar con un carácter de barra inclinada invertida \.</li> </ul>
\...\	<ul style="list-style-type: none"> <li>Indica que la regla se aplica en todos los directorios por debajo de este nivel.</li> <li>Una regla no puede comenzar o finalizar con una secuencia \ . . \ .</li> <li>Esta secuencia debe ser posterior a la secuencia de especificación de unidad.</li> </ul>
*	<ul style="list-style-type: none"> <li>Esta sintaxis es el comodín para cualquier carácter o para cualquier número de caracteres. También se utiliza cuando no se ha definido ningún carácter.</li> <li>Una regla puede comenzar o finalizar con esta sintaxis.</li> <li>Cuando se utiliza para indicar una letra de unidad, esta sintaxis debe ser un carácter alfabético.</li> <li>Este comodín no puede ser un carácter de barra inclinada invertida \.</li> </ul>

Tabla 56. Sintaxis de reglas de exclusión para Windows (continuación)

Sintaxis	Comportamiento de la sintaxis
?	<ul style="list-style-type: none"> <li>Esta sintaxis se utiliza como comodín para cualquier carácter para una única aparición.</li> <li>Una regla puede comenzar y finalizar con esta sintaxis.</li> <li>Cuando se utiliza esta sintaxis para indicar una letra de unidad, debe ser un carácter alfabético entre A y Z.</li> </ul>
DIR	<ul style="list-style-type: none"> <li>Esta sintaxis indica una regla de directorio, pero no excluye ningún archivo del directorio afectado.</li> <li>La sintaxis debe ser una regla de cabecera seguida de un espacio en blanco.</li> </ul>
FS	<ul style="list-style-type: none"> <li>Indica que se ha excluido una unidad del sistema de archivos completa del trabajo.</li> <li>Esta sintaxis debe ir seguida de una letra de unidad que puede ser un único carácter o un comodín.</li> </ul>
Espacios	<ul style="list-style-type: none"> <li>Los espacios están permitidos en nombres de archivo o en nombres de directorio.</li> <li>No se permite un espacio en blanco antes de una barra inclinada invertida, \, o en una cabecera o cola de una fila de regla.</li> <li>Los espacios se validan como caracteres individuales.</li> </ul>
Texto en mayúsculas y minúsculas	Microsoft Windows distingue entre mayúsculas y minúsculas. Las reglas de exclusión ignoran las mayúsculas y minúsculas.

Tabla 57. Sentencias de exclusión válidas

Ejemplo de regla	
*.*	Esta regla excluye todos los archivos de la raíz del sistema de archivos de todas las unidades, pero no excluye los directorios.
DIR *.*	Esta regla excluye todos los directorios de todas las unidades, pero no excluye los archivos del directorio raíz.
DIR E:\...*temp*	Esta regla excluye todos los directorios que empiezan por temp en el nombre de directorio en todos los directorios de la unidad E:
DIR F:\Users\Bobby\*	Esta regla excluye todo el contenido del directorio Bobby sin excluir dicho directorio. Los archivos del directorio Bobby no se excluyen.

Tabla 57. Sentencias de exclusión válidas (continuación)

Ejemplo de regla	
DIR F:\Users	Esta regla excluye a todos los usuarios que se listan en los directorios de usuarios y también excluye el directorio de usuarios.
DIR F:\Users\Bobby M?gee	Esta regla excluye todos los directorios que coincidan con el nombre con un comodín para la letra. Esta regla excluye a usuarios con nombres como Magee, Megee, Mige, etc.
DIR F:\Users\Bobby Magee	Esta regla excluye el directorio para el usuario que está definido, en este caso Bobby Magee. Con esta regla, se excluye el directorio para ese usuario y todo su contenido que incluye archivos y subcarpetas.
F:\...*	Esta regla excluye todos los archivos de la unidad F: \, pero no excluye los directorios.
F:\Bobby.mp?	Esta regla excluye todos los archivos que coincidan con Bobby .mp? en la raíz del sistema de archivos, como Bobby.MP3, Bobby.MP4, etc.
F:\Bobby.txt	Esta regla excluye el archivo Bobby.txt en la raíz del sistema de archivos.
F:\Users\...*.mp3	Esta regla excluye todos los archivos MP3 para todos los usuarios listados en la unidad F.
F:\Users\Bobby\...*.mp3	Esta regla excluye todos los archivos MP3 del directorio de usuario Bobby.
F:\Users\Bobby\...*music*\...*.mp?	Esta regla excluye todos los archivos MP en todos los directorios que tienen la palabra música en el nombre de directorio para el usuario Bobby. Los archivos que se excluyen son MP2, MP3, MP4, etc.
F:\Users\John\* DIR F:\Users\John\*	Esta combinación de reglas excluye todos los archivos y todos los subdirectorios para el usuario John, pero no excluye el directorio de John en sí.
F:\Users\John\tax\Tax_20???.pdf	Esta regla excluye todos los documentos que coinciden con el patrón Tax_20 en el directorio John\tax. Se excluyen archivos como estos, TAX_2000.pdf, TAX_2019.pdf, etc.
FS F	Esta regla excluye la unidad F del sistema de archivos.
FS *	Esta regla excluye todas las unidades del sistema de archivos.
FS ?	Esta regla excluye todas las unidades.

### Sintaxis de exclusión no válida

La siguiente sintaxis no válida no funciona en las definiciones de reglas de exclusión.

- \no
- \*

- \\*
- F:\no\
- DIR \no
- DIR F:\no\
- DIR \*
- DIR F:\\*\

Para ver el archivo de registro de trabajos, vaya a **Trabajos y operaciones** y abra la pestaña **Trabajos en ejecución**. Encuentre la entrada de registro más reciente de **Copia de seguridad del servidor de aplicaciones**.

## Restauración de datos de sistema de archivos

Para restaurar los datos de sistema de archivos 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. Utilizando el navegador de Restauración a nivel de archivo de los sistemas de archivos, puede seleccionar los recursos del sistema de archivos que va a añadir al trabajo y especificar si restaurar los datos en la instancia original o en una instancia alternativa en una máquina diferente.

### Antes de empezar

**Importante:** En todas las operaciones de restauración, sistema de archivos debe estar en el mismo nivel de versión en los host de origen y destino. Además, debe asegurarse de que exista en cada host una instancia con el mismo nombre que el de la instancia que se está restaurando.

Asegúrese de que se cumplen los requisitos adicionales siguientes:

- Asegúrese de que al menos un trabajo de copia de seguridad de sistema de archivos se ha ejecutado correctamente. Para obtener instrucciones sobre la configuración de un trabajo de copia de seguridad, consulte [“Copia de seguridad de datos del sistema de archivos”](#) en la página 314.
- Asegúrese de que se asignan los roles y grupos de recursos de IBM Spectrum Protect Plus al usuario que ha configurado el trabajo de restauración. Para obtener más información sobre la asignación de roles, consulte [Capítulo 18, “Gestión del acceso de usuarios”](#), en la página 533.
- Asegúrese de que el objetivo del destino de IBM Spectrum Protect Plus para el trabajo de restauración esté registrado y configurado correctamente.

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. Para obtener más información sobre los requisitos de espacio, consulte [Requisitos de espacio para la protección del sistema de archivos](#). Para obtener más información sobre los requisitos previos y la configuración, consulte [Requisitos previos para la protección del sistema de archivos](#).

### Procedimiento

1. En el panel de navegación, expanda **Gestionar protección > Sistemas de archivos > Microsoft**

**Windows** y haga clic en **Crear trabajo**


Create job

2. Seleccione **Restaurar**.

Se abre el asistente para **Restaurar**.

3. Opcional: Si ha iniciado el asistente de restauración desde la página **Trabajos y operaciones**, haga clic en **sistema de archivos** como el tipo de origen y, a continuación, en **Siguiente**.

**Sugerencias:**

- Para obtener un resumen en ejecución de las selecciones en el asistente, pulse **Vista previa de restauración** en el panel de navegación del asistente.
  - El asistente se abre en la modalidad de configuración predeterminada. Para ejecutar el asistente en modalidad de configuración avanzada, seleccione **Configuración avanzada**. Con la modalidad de configuración avanzada, puede establecer más opciones para el trabajo de restauración.
4. En la página **Seleccionar origen**, haga clic en un servidor de sistema de archivos para mostrar los volúmenes que están disponibles en dicho servidor. Seleccione un volumen pulsando el icono de signo más al lado del nombre de ese volumen . Pulse **Siguiente** para continuar.
  5. En la página **Instantánea de origen**, seleccione la instantánea que desea restaurar en el destino. Pulse **Siguiente** para continuar.

Las instantáneas disponibles para el volumen seleccionado se listan con una indicación de fecha y hora, la política de SLA asociada con esa instantánea y el tipo de origen que está disponible, ya sea copia de seguridad, archivado o réplica.

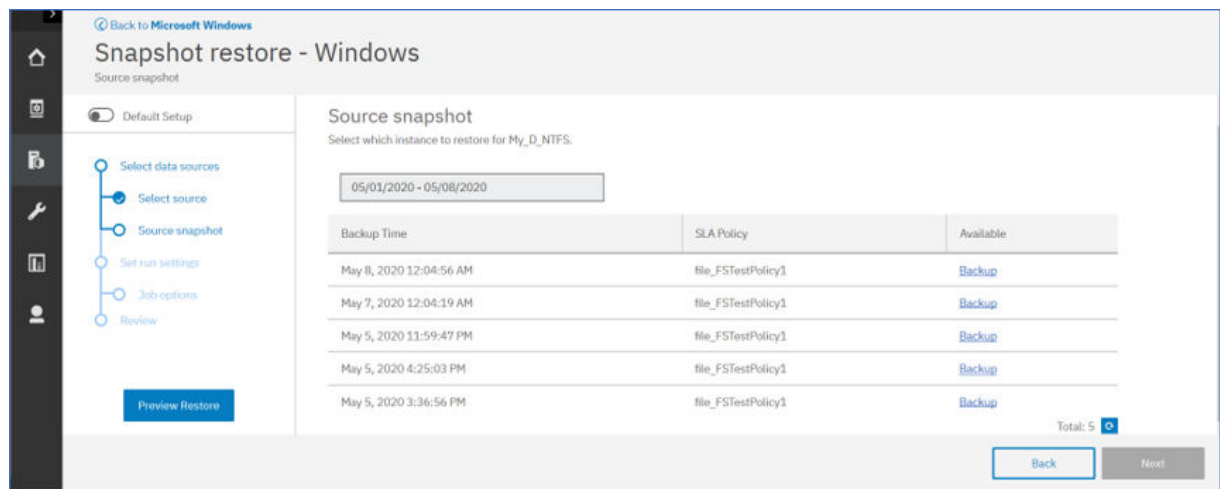


Figura 26. Selección de instantánea de origen

6. Puede establecer los valores de ejecución en la página **Opciones de trabajo**. Indique si debe realizarse una operación de limpieza si falla el trabajo de restauración. Pulse **Siguiente** para continuar.
7. En la página **Revisar**, revise las selecciones para el trabajo de restauración. Si todas las selecciones son correctas, pulse **Enviar** o pulse **Atrás** para editar las selecciones.

La pestaña **Recursos activos** de Trabajos y operaciones se abre para mostrar el recurso activo que está preparado cuando sale del asistente de restauración.

**Nota:** El recurso activo para el trabajo de restauración que se envía no es inmediato y tarda algún tiempo en visualizarse.

8. Abra el navegador de Restauración a nivel de archivo de los sistemas de archivos haciendo clic en **Abrir navegador** en la pestaña **Recursos activos**.



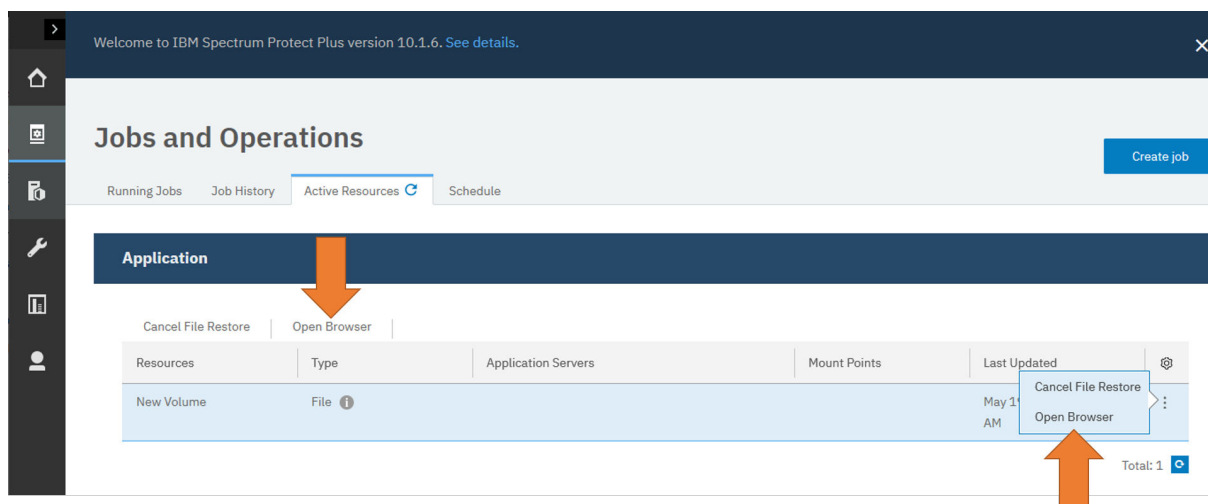


Figura 27. Apertura del navegador de Restauración a nivel de archivo de los sistemas de archivos desde la pestaña Recursos activos

9. En el navegador **Restauración a nivel de archivo de los sistemas de archivos**, seleccione los recursos del sistema de archivos que se van a añadir al trabajo de restauración. Añada elementos



haciendo clic en el icono de adición al lado del elemento adecuado.

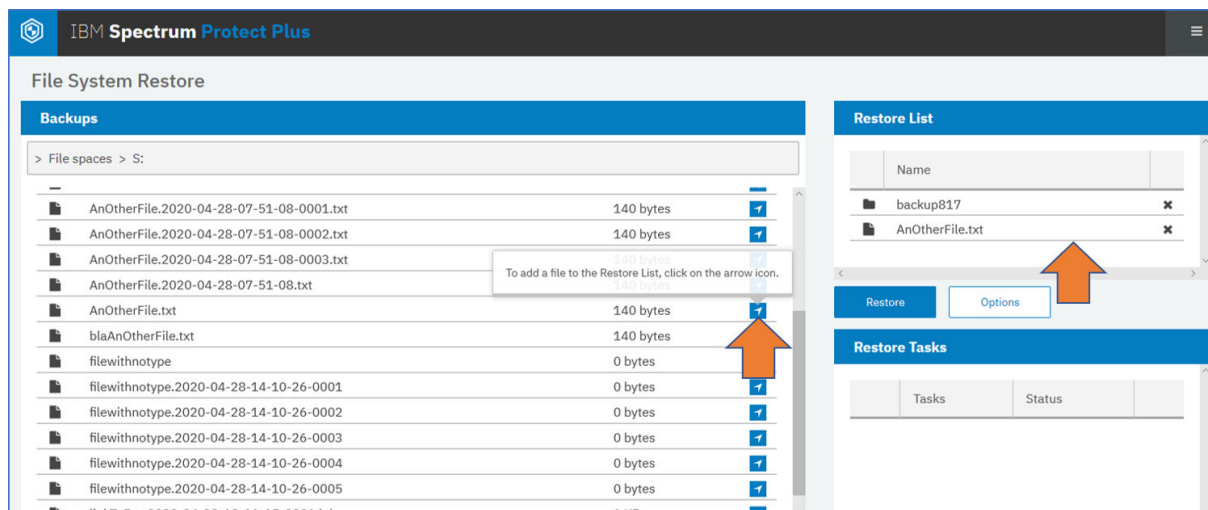


Figura 28. Navegador de Restauración a nivel de archivo de los sistemas de archivos: adición de recursos a la sección Lista de restauración

10. Para especificar una ubicación alternativa para el trabajo de restauración, haga clic en **Opciones** y especifique una vía de acceso de volumen local de Windows válida como destino.

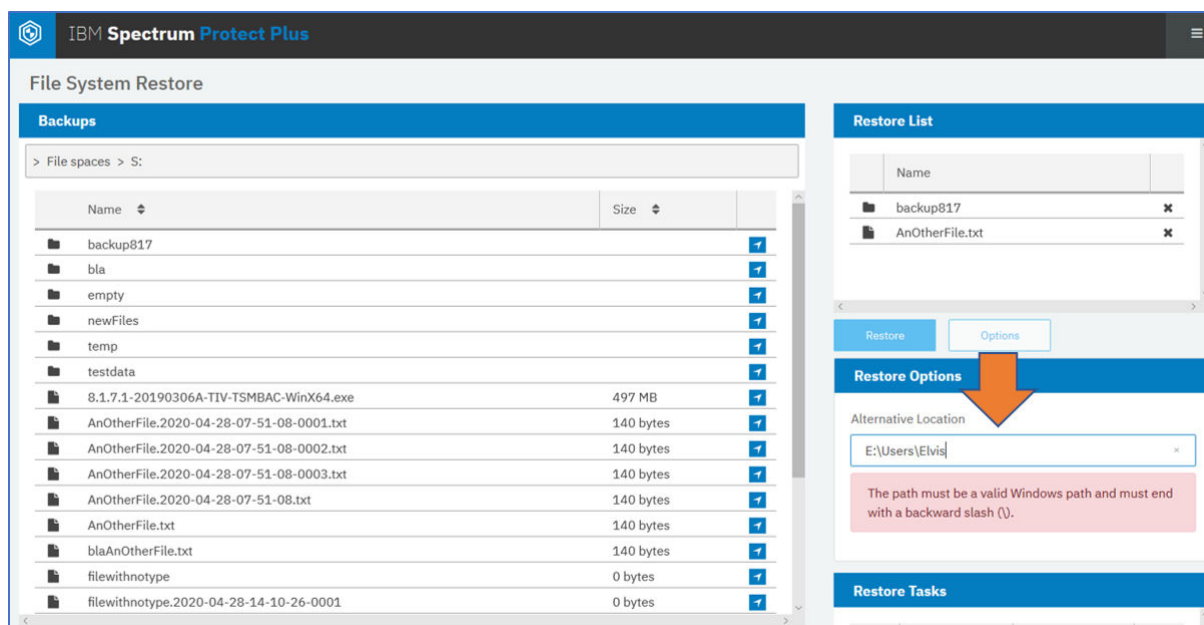


Figura 29. Especificación de una ubicación alternativa para el trabajo de restauración en el navegador Restauración a nivel de archivo de los sistemas de archivos

**Restricción:** Los recursos compartidos de red no son ubicaciones alternativas válidas para los trabajos de restauración.

11. Pulse **Restaurar** para iniciar el proceso de restauración.

No se sobrescriben archivos existentes durante la operación de restauración. Si se encuentran archivos con nombres idénticos en el destino, se añade una indicación de fecha y hora al nuevo archivo y ambos archivos se almacenan en el destino.

12. Opcional: Supervise el progreso de la operación de restauración en el panel **Tareas de restauración**.

**Consejo:** No se realiza el seguimiento del proceso de restauración en la página IBM Spectrum Protect Plus **Trabajos y operaciones**. Se realiza un seguimiento del progreso del trabajo de restauración en el navegador de Restauración a nivel de archivo de los sistemas de archivos.

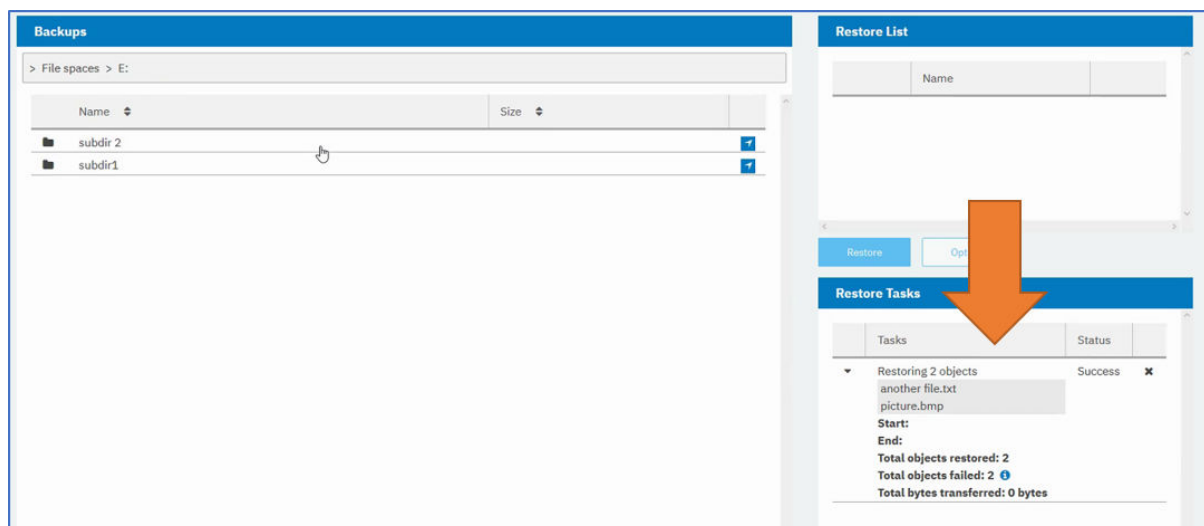


Figura 30. Supervisión del trabajo de restauración en el navegador de Restauración a nivel de archivo de los sistemas de archivos

## Qué hacer a continuación

Cuando se complete el trabajo de restauración, elimine el recurso activo realizando las siguientes acciones:

1. En el panel de navegación, haga clic en **Trabajos y operaciones > Recursos activos**.
2. Seleccione el recurso activo con el que ha finalizado y pulse **Cancelar restauración de sistema de archivos**.

## Navegador de Restauración a nivel de archivo de los sistemas de archivos

Cuando se prepara un trabajo de restauración para un sistema de archivos específico, el recurso activo que se crea se puede ver en el navegador **Restauración a nivel de archivo de los sistemas de archivos** para que pueda definir los elementos que se van a restaurar. Utilice el navegador para buscar y especificar los directorios o archivos que desea restaurar desde ese sistema de archivos. A continuación, puede especificar una ubicación alternativa para dirigir los recursos restaurados a una ubicación distinta de la fuente.

## Apertura del navegador de Restauración a nivel de archivo de los sistemas de archivos

Después de pulsar **Enviar** en el asistente Restaurar, se prepara el trabajo de restauración y se abre la pestaña **Recursos activos** en la página **Trabajos y operaciones**. Para abrir el navegador Restauración a nivel de archivo de los sistemas de archivos, haga clic en el icono de acciones en la tabla **Recursos**

 o pulse **Abrir navegador** como se muestra.

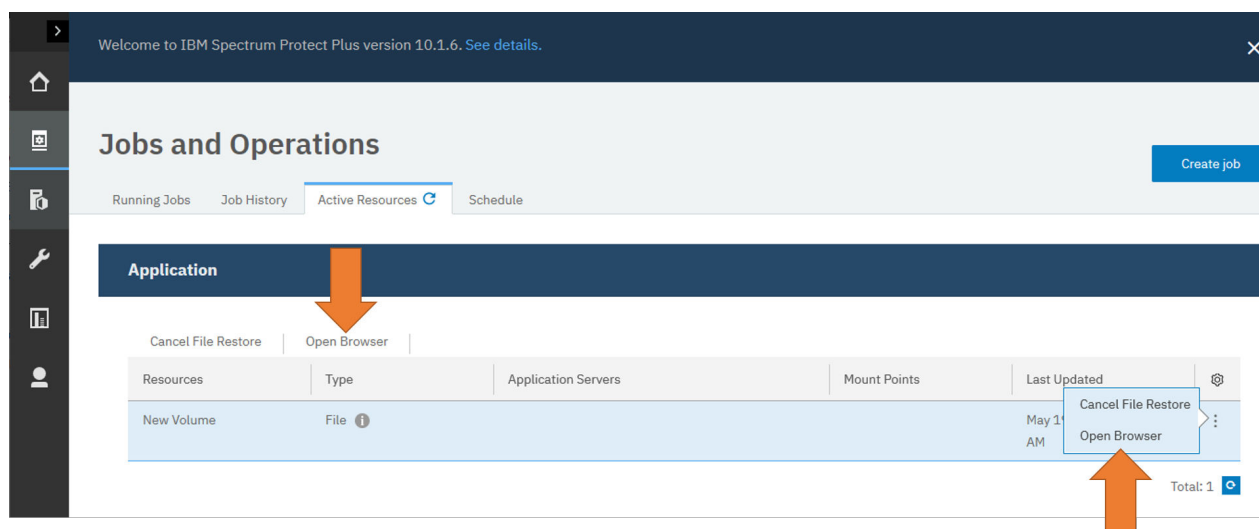


Figura 31. Apertura de Restauración a nivel de archivo de los sistemas de archivos desde la pestaña Recursos activos.

## Adición de recursos a la operación de restauración utilizando el navegador Restauración a nivel de archivo de los sistemas de archivos

Para añadir recursos del sistema de archivos específicos para un trabajo de restauración, vaya al sistema de archivos, directorios o archivos necesarios. Añada elementos a la sección Lista de restauración



pulsando el icono al lado del elemento de sistema de archivos

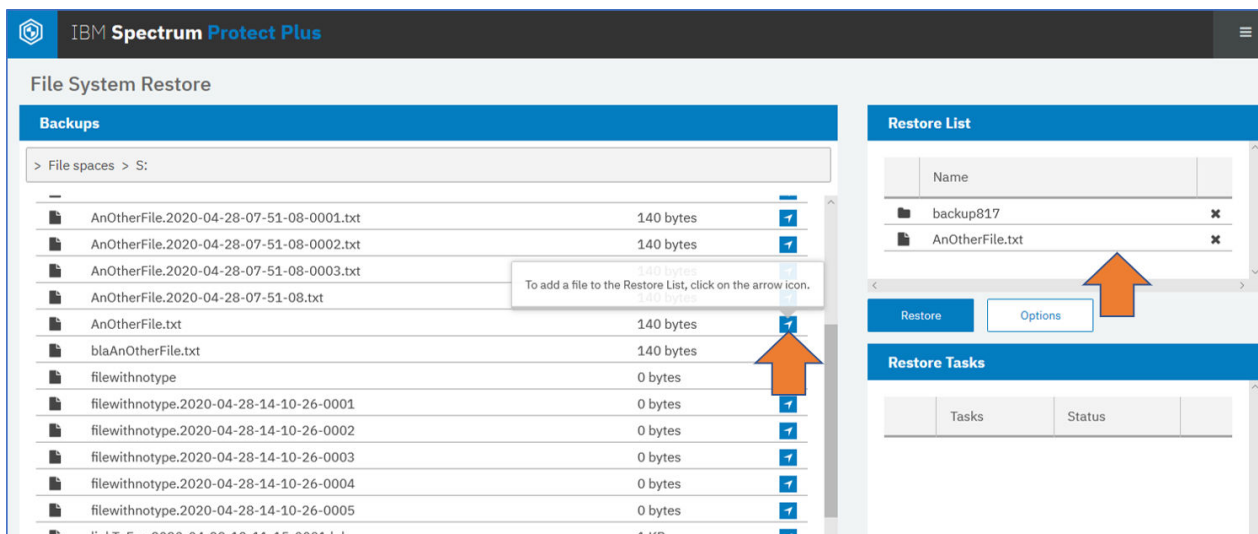


Figura 32. Adición de objetos de sistema de archivos al trabajo de restauración en el navegador Restauración a nivel de archivo de los sistemas de archivos

### Restauración de recursos del sistema de archivos en una ubicación alternativa

Para clonar o copiar recursos, y para restaurar esos recursos en una ubicación distinta de la ubicación de origen, puede especificar una vía de acceso de Windows válida como destino en **Ubicación alternativa** en el panel **Opciones**.

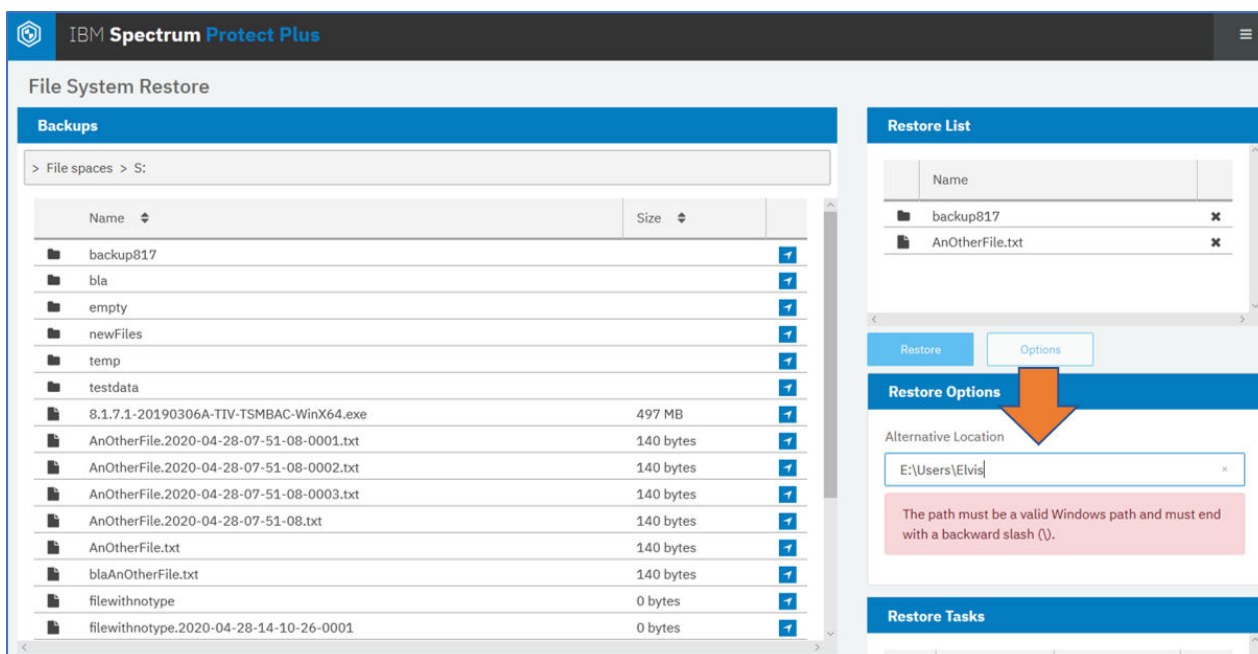


Figura 33. Especificación de una ubicación alternativa para el trabajo de restauración en el navegador Restauración a nivel de archivo de los sistemas de archivos

### Supervisión de un trabajo de restauración

Cuando pulsa **Restaurar** en el navegador Restauración a nivel de archivo de los sistemas de archivos, puede supervisar el progreso del trabajo de restauración en el panel **Tareas de restauración**.

Figura 34. Supervisión de un trabajo de restauración en el navegador Restauración a nivel de archivo de los sistemas de archivos

Backups

> File spaces > E:

Name	Size
subdir 2	
subdir1	

Restore List

Name
------

Restore Options

Restore Tasks

Tasks	Status
Restoring 2 objects another file.txt picture.bmp Start: End: Total objects restored: 2 Total objects failed: 2 Total bytes transferred: 0 bytes	Success



## Capítulo 12. Protección de contenedores

Soporte de copia de seguridad de Kubernetes es una característica de IBM Spectrum Protect Plus que amplía la protección de datos a los contenedores de los clústeres Kubernetes. Kubernetes es un sistema para la orquestación de contenedores en clústeres de hosts.

Para proteger los volúmenes persistentes en el entorno Kubernetes, en primer lugar, cree políticas de acuerdo de nivel de servicio que especifiquen el periodo de retención y frecuencia de copia de seguridad. A continuación, cree trabajos para las operaciones de copia de seguridad y restauración.

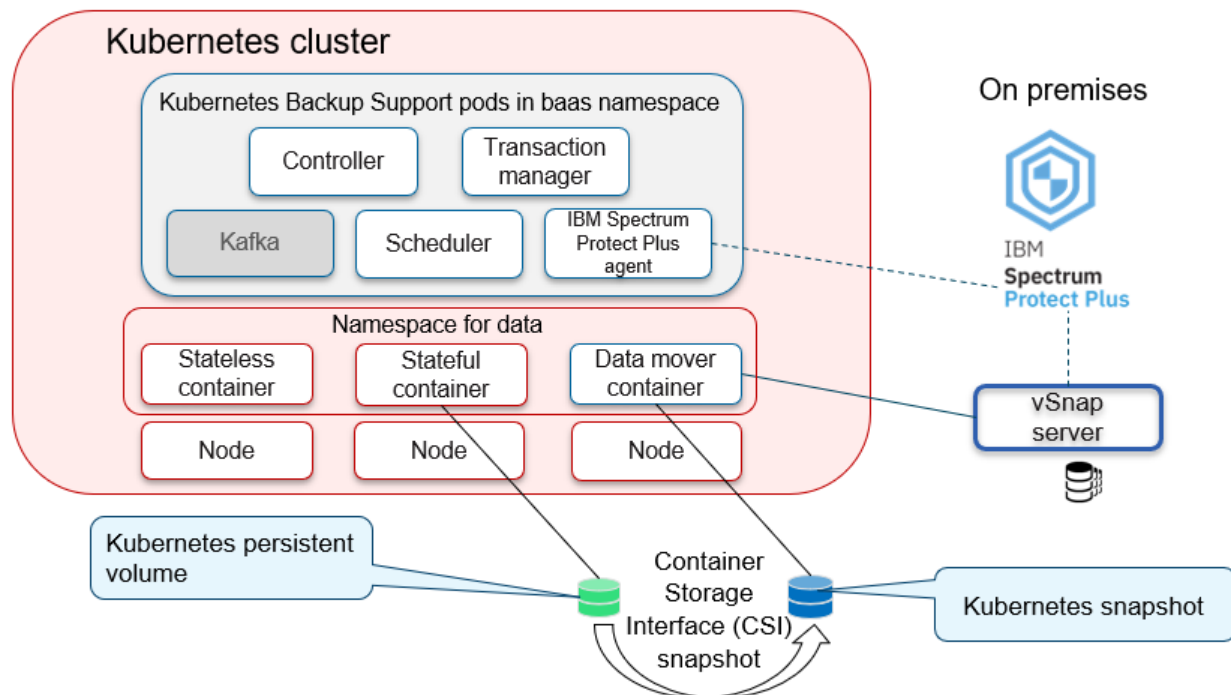
### Visión general de Soporte de copia de seguridad de Kubernetes

Soporte de copia de seguridad de IBM Spectrum Protect Plus Kubernetes protege los volúmenes persistentes que están conectados a contenedores en clústeres Kubernetes. Se crean copias de seguridad de instantánea de los volúmenes persistentes y se copian en servidores vSnap de IBM Spectrum Protect Plus.

Los volúmenes persistentes que contienen datos de aplicación que están protegidos por las políticas de acuerdo de nivel de servicio (SLA) predefinidas que especifican la frecuencia con la que se crean las copias de seguridad de instantánea y de copia y cuánto tiempo se conservan. Si los datos de los volúmenes originales están dañados o se han perdido, los volúmenes se pueden restaurar desde las copias de seguridad de copia o de instantánea en los servidores vSnap.

Soporte de copia de seguridad de Kubernetes protege únicamente el almacenamiento persistente que ha asignado un conector de almacenamiento que soporta la Interfaz de almacenamiento de copias de seguridad (CSI) proporcionada por Kubernetes. Soporte de copia de seguridad de Kubernetes se ha probado completamente con el almacenamiento en bloques de Red Hat Ceph, que admite CSI. El plug-in de CSI proporciona prestaciones de instantáneas que se utilizan para las operaciones de copia de seguridad.

La siguiente figura muestra cómo se despliega Soporte de copia de seguridad de Kubernetes en el entorno de Kubernetes y cómo interactúa con el diagrama de despliegue de IBM Spectrum Protect Plus:



## Contenedor de transportador de datos

El transportador de datos se despliega como un contenedor en el espacio de nombres donde existen las reclamaciones de volumen persistente (PVC). El contenedor del transportador de datos se comunica con la instancia de IBM Spectrum Protect Plus fuera del entorno de Kubernetes para el soporte de copia de seguridad de copia.

Soporte de copia de seguridad de Kubernetes utiliza las PVC para identificar los volúmenes persistentes a los que se hace copia de seguridad. En las operaciones de copia de seguridad de copia, cuando se ejecuta una planificación, se crean copias de seguridad de instantánea y de copia de una PVC en los intervalos de tiempo especificados por el SLA. El transportador de datos copia los datos y registra las copias de seguridad de instantánea en la ventana IBM Spectrum Protect Plus **Trabajos y operaciones**. Las instantáneas creadas por copias de seguridad bajo demanda también se registran en IBM Spectrum Protect Plus.

## Se admite la multitenencia

Soporte de copia de seguridad de Kubernetes gestiona operaciones de copia de seguridad y restauración mediante recursos personalizados de Kubernetes. Todos los objetos de copia de seguridad y restauración pertenecen a un espacio de nombres Kubernetes. El administrador de Kubernetes puede restringir el acceso a estos objetos. Con el acceso controlado, varios usuarios pueden ejecutar solicitudes de copia de seguridad y restauración en el mismo clúster de Kubernetes. Los objetos de copia de seguridad y restauración heredan un espacio de nombres de la PVC que identifica el volumen persistente para operaciones de copia de seguridad y restauración. Para obtener más información sobre la multitenencia, consulte [“Características de seguridad de Soporte de copia de seguridad de Kubernetes” en la página 333](#).

## Tipos de copia de seguridad y restauración

Soporte de copia de seguridad de Kubernetes proporciona varios tipos de funciones de copia de seguridad y restauración. Puede utilizar la interfaz de usuario de IBM Spectrum Protect Plus o la línea de mandatos de Kubernetes para iniciar las operaciones de copia de seguridad y restauración.

### Tipos de copia de seguridad

Están disponibles los siguientes tipos de operaciones de seguridad:

#### **copia de seguridad de instantánea**

Crea una copia de seguridad del volumen persistente utilizando las prestaciones de instantánea del complemento de almacenamiento de la Interfaz de almacenamiento de copias de seguridad (CSI). La instantánea se almacena en una ubicación asignada por una clase de instantánea de Kubernetes tal como la define el administrador de copia de seguridad. Generalmente, esta ubicación es el mismo sitio de almacenamiento que el volumen persistente al que se está haciendo la copia de seguridad. La clase de instantánea debe ser compatible con la clase de almacenamiento del volumen persistente. En otras palabras, la clase de instantánea y la clase de almacenamiento están definidas y proporcionadas por el mismo plug-in de almacenamiento de CSI.

Las copias de seguridad de instantánea se crean mediante las solicitudes de copia de seguridad planificadas y las solicitudes de copia de seguridad bajo demanda.

Durante las copias de seguridad planificadas, las copias de seguridad de instantánea se crean en intervalos definidos por una política de acuerdo de nivel de servicio (SLA).

Durante una solicitud de copia de seguridad bajo demanda, la instantánea se toma inmediatamente pero no se crea ninguna copia de seguridad de copia. Después de la copia de seguridad de instantánea inicial, el volumen está protegido por la política de SLA especificada.

#### **Copia de reserva**

Copia el volumen persistente completo en un servidor vSnap de IBM Spectrum Protect Plus. En función de las políticas de SLA predefinidas, IBM Spectrum Protect Plus ofrece una mayor retención de copias de seguridad de copia en comparación con las copias de seguridad de instantánea.



Durante las copias de seguridad planificadas, se crean copias de seguridad de copia y de instantánea en intervalos definidos por la política de SLA.

## Tipos de restauración

Están disponibles los siguientes tipos de operaciones de restauración:

### Restauración de instantánea

Restaura una instantánea en un volumen persistente nuevo. Este tipo de operación es adecuado para restaurar rápidamente copias de seguridad de instantánea recientes.

### Restauración de copia de seguridad de copia

Restaura una copia de seguridad de copia en el volumen persistente original o en un volumen persistente nuevo. Si desea restaurar una copia de seguridad de copia en el volumen persistente original, el contenedor al que está conectado el volumen persistente no debe estar en ejecución.

Este tipo de operación es adecuado para la restauración de volúmenes persistentes desde las copias de seguridad de copia retenidas durante un periodo más largo en IBM Spectrum Protect Plus.

## Políticas de SLA

Las políticas de acuerdo de nivel de servicio (SLA) definen la frecuencia con la que se ejecutan las operaciones de copia de seguridad de copia y de copia de seguridad de instantánea y durante cuánto tiempo se retienen las copias de seguridad de copia y de instantánea. Puede configurar SLA personalizados que cumplan los requisitos operativos.

El administrador de almacenamiento puede crear políticas de SLA utilizando la interfaz de usuario de IBM Spectrum Protect Plus. Para obtener instrucciones, consulte [“Creación de una política de SLA para clústeres Kubernetes”](#) en la página 250.

Para ver la lista de políticas de SLA que se crean para contenedores, utilice uno de los métodos siguientes:

- En la interfaz de usuario de IBM Spectrum Protect Plus, pulse **Gestionar protección > Descripción general de política**. La sección **Políticas de SLA** lista todas las políticas que están disponibles. Una política de SLA predefinida, **Contenedor**, está disponible para ayudarle a proteger los volúmenes persistentes. La política **Contenedor** ejecuta las siguientes operaciones:
  - Copias de seguridad de instantánea cada 6 horas con un periodo de retención de 1 día
  - Copias de seguridad de copia diarias con un periodo de retención de 31 días
- En el entorno de Kubernetes, emita el mandato siguiente para ver las políticas de SLA en el objeto ConfigMap baas-sla en el espacio de nombres baas:

```
kubect1 describe configmap baas-sla -n baas
```

Este mandato muestra las políticas de SLA disponibles para contenedores. Si no se ha creado ninguna política de SLA para contenedores, la salida está vacía.

La salida es similar a la que se muestra en el ejemplo siguiente:

```
Name:          baas-sla
Namesapce:     baas
Labels:        app=baas
               component=scheduler
               release=10.1.6
Annotations:   <none>

Data
====
SLAs:
----
daily_midnight:
Las instantáneas se realizan todos los días y se conservan durante 7 días.
No se realiza ninguna copia de seguridad de copia.
----
every_4hours:
Las instantáneas se realizan cada 4 horas y se conservan 1 día.
No se realiza ninguna copia de seguridad de copia.
```

```
----  
hourly:  
Las instantáneas se realizan cada hora y se conservan 1 día.  
No se realiza ninguna copia de seguridad de copia.
```

El SLA se asigna a un volumen en la definición de planificación de copia de seguridad. Puede asignar más de un SLA a un volumen.

Cuando las copias de seguridad de copia y de instantánea caducan, se marcan para caducidad en IBM Spectrum Protect Plus y los trabajos de mantenimiento de IBM Spectrum Protect Plus las suprimen.

### Tareas relacionadas

[“Definición de copias de seguridad del acuerdo de nivel de servicio de volúmenes persistentes” en la página 338](#)

Puede utilizar la interfaz de usuario de IBM Spectrum Protect Plus para definir trabajos de copia de seguridad según la política de acuerdo de nivel de servicio (SLA). La política de SLA especifica la frecuencia con la que se ejecutan las operaciones de copia de seguridad y cuánto tiempo se guardan las copias de seguridad de instantáneas o de copia

[“Planificación de copias de seguridad de volúmenes persistentes utilizando la línea de mandatos” en la página 350](#)

Mediante la línea de mandatos de Kubernetes, puede planificar solicitudes de copia de seguridad basadas en políticas de acuerdo de nivel de servicio (SLA). Las políticas de SLA especifican la frecuencia con la que se ejecutan las operaciones de copia de seguridad y la cantidad de copias de seguridad de copia y de instantánea que se retienen.

## Roles de usuario

En función de su rol, los desarrolladores de aplicaciones empresariales y los administradores de copias de seguridad interactúan con diferentes interfaces de usuario para proteger los datos persistentes de los contenedores.

### Desarrollador de aplicaciones

El desarrollador de aplicaciones empresariales utiliza la herramienta de línea de mandatos de Kubernetes (**kubect1**) para completar las siguientes tareas independientes del administrador de copia de seguridad:

- Inicia solicitudes de copia de seguridad y restauración de autoservicio
- Selecciona una política de acuerdo de nivel de servicio (SLA) para utilizarla en las solicitudes de copia de seguridad para proteger sus volúmenes
- Restaura volúmenes
- Visualiza el estado de las solicitudes de copia de seguridad y restauración
- Consulta información sobre copias de seguridad de copia y de instantánea
- Elimina asignaciones de políticas de SLA de PVC
- Elimina solicitudes de copia de seguridad planificada obsoletas y solicitudes de instantánea bajo demanda

### Administrador de copias de seguridad

El administrador de copias de seguridad completa las siguientes tareas:

- Despliega y configura software de Soporte de copia de seguridad de Kubernetes en el entorno de Kubernetes
- Crea la clase de almacenamiento Kubernetes para volúmenes persistentes y la clase de instantánea para almacenar instantáneas
- Instala y configura IBM Spectrum Protect Plus
- Completa las tareas siguientes en la interfaz de usuario de IBM Spectrum Protect Plus:
  - Registra manualmente un clúster Kubernetes o actualiza las propiedades del clúster

- Ejecuta manualmente un inventario para detectar recursos de clúster
- Crea políticas de SLA
- Define trabajos de copia de seguridad de SLA para proteger volúmenes
- Elimina asignaciones de políticas de SLA de PVC
- Restaura volúmenes
- Supervisa trabajos de inventario, copia de seguridad y restauración mediante la interfaz de usuario de IBM Spectrum Protect Plus
- Genera informes que muestran el historial de trabajos de copia de seguridad de contenedor mediante la interfaz de usuario de IBM Spectrum Protect Plus
- Completa las tareas de resolución de problemas, como la recopilación de archivos de registro para la depuración en el entorno de Kubernetes y la visualización de archivos de registro de rastreo para Soporte de copia de seguridad de Kubernetes

## **Características de seguridad de Soporte de copia de seguridad de Kubernetes**

Además de las características de seguridad básicas que se integran en Soporte de copia de seguridad de Kubernetes, se proporcionan características de seguridad avanzadas para ayudar a proteger contenedores, proteger conexiones de red, cifrar datos y verificar paquetes de instalación.

### **Exploración de seguridad de contenedores**

Los contenedores de Soporte de copia de seguridad de Kubernetes se crean en contenedores que se derivan de la Universal Based Image (UBI) de Red Hat. El software de Soporte de copia de seguridad de Kubernetes en cada contenedor se ha escaneado de forma estática para los componentes vulnerables o bibliotecas. Además, los contenedores se exploran de forma dinámica para ayudar a prevenir vulnerabilidades de tiempo de ejecución como la inyección de código. Después de la exploración, el software se prueba utilizando una suite de pruebas automatizada para verificar que Soporte de copia de seguridad de Kubernetes puede funcionar como se esperaba y puede procesar correctamente la entrada errónea.

Todos los contenedores, excepto el contenedor del transportador de datos, se ejecutan en un espacio de nombres dedicado que proporciona más aislamiento de seguridad. El transportador de datos debe ejecutarse en el mismo espacio de nombres que la reclamación de volumen persistente (PVC) para operaciones de copia de seguridad o restauración porque el montaje del volumen se limita a contenedores de un único espacio de nombres.

### **Contenedores menos privilegiados**

Cada uno de los componentes de Soporte de copia de seguridad de Kubernetes se ejecuta bajo el principio de menor privilegio. Las acciones de los contenedores están restringidas por las reglas de control de autenticación basada en roles que están asociadas con sus cuentas de servicio en su espacio de nombres separado. Además, el software de cada contenedor se ejecuta como un usuario no root. Solo el transportador de datos se ejecuta como contenedor privilegiado porque el transportador de datos requiere acceso al punto de montaje en el sistema host del volumen al que se está haciendo copia de seguridad o restauración. Todos los demás contenedores no tienen privilegios.

### **Autenticación de conexiones de red**

Las conexiones de red entre componentes de Soporte de copia de seguridad de Kubernetes se controlan mediante políticas de red que limitan las conexiones a aquellas que son necesarias para una operación correcta. Las conexiones a IBM Spectrum Protect Plus se basan en protocolos de seguridad que proporciona IBM Spectrum Protect Plus.

### **Multitenencia**

La multitenencia está soportada en Soporte de copia de seguridad de Kubernetes, que se basa ampliamente en la autenticación y la autorización que proporciona el clúster Kubernetes para los

espacios de nombres. Dado que la autorización está relacionada con un espacio de nombres, cualquier usuario autorizado para crear un objeto BaaSReq en dicho espacio de nombres puede solicitar una copia de seguridad o una restauración para cualquier PVC que esté asociada con dicho espacio de nombres. Un objeto BaaSReq es un recurso de Kubernetes personalizado que se utiliza en las solicitudes de Soporte de copia de seguridad de Kubernetes.

Las instantáneas están protegidas por la Interfaz de almacenamiento de contenedores (CSI) para restringir el acceso al espacio de nombres de la PVC original. Soporte de copia de seguridad de Kubernetes asocia el espacio de nombres con las copias de seguridad que se almacenan en IBM Spectrum Protect Plus, y las copias de seguridad deben restaurarse en volúmenes en el mismo espacio de nombres.

### **Cifrado de datos en reposo**

El clúster y los administradores de almacenamiento son responsables de habilitar los mecanismos para proteger los datos en reposo mediante el cifrado. Los datos confidenciales incluyen los datos de copia de seguridad de copia y los secretos de Soporte de copia de seguridad de Kubernetes, que constan de los ID de usuario y contraseñas especificados durante el proceso de instalación. El administrador de clúster puede especificar qué secretos se cifran cuando se almacenan en la base de datos etcd de clúster. Para obtener más información, consulte [Cifrado de datos secretos en reposo](#).

Soporte de copia de seguridad de Kubernetes no implementa un cifrado adicional más allá del que proporciona el clúster. Sin embargo, el administrador de almacenamiento puede desplegar un servidor vSnap de IBM Spectrum Protect Plus habilitado para el cifrado.

Al utilizar la interfaz de usuario de IBM Spectrum Protect Plus, el administrador de almacenamiento puede definir acuerdos de nivel de servicio (SLA) que almacenan datos de copia de seguridad en discos cifrados. Cuando se crean solicitudes de copia de seguridad que especifican SLA habilitados para el cifrado, los datos se dirigen a un servidor vSnap para el cifrado si el servidor vSnap está habilitado para el cifrado de datos en reposo.

### **Firma de código**

El administrador de clústeres puede verificar que el paquete de instalación de Soporte de copia de seguridad de Kubernetes no se ha modificado desde que IBM lo ha generado. Este proceso se lleva a cabo verificando el archivo de firmas que se incluye con el paquete de instalación los certificados y firma adecuados. El proceso de verificación se describe en la documentación de instalación.

Para obtener más información, consulte [“Instalación y despliegue de imágenes de Soporte de copia de seguridad de Kubernetes en el entorno de Kubernetes”](#) en la página 156.

## **Copia de seguridad y restauración de clústeres Kubernetes utilizando la interfaz de usuario de IBM Spectrum Protect Plus**

Para proteger los volúmenes persistentes conectados a un clúster Kubernetes, cree políticas de acuerdo de nivel de servicio (SLA) y cree trabajos para operaciones de copia de seguridad y restauración en la interfaz de usuario de IBM Spectrum Protect Plus.

Asegúrese de que el entorno de Kubernetes cumple los requisitos del sistema en [“Requisitos de Soporte de copia de seguridad de Kubernetes”](#) en la página 56.

### **Conceptos relacionados**

[“Visión general de Soporte de copia de seguridad de Kubernetes”](#) en la página 329

Soporte de copia de seguridad de IBM Spectrum Protect Plus Kubernetes protege los volúmenes persistentes que están conectados a contenedores en clústeres Kubernetes. Se crean copias de seguridad de instantánea de los volúmenes persistentes y se copian en servidores vSnap de IBM Spectrum Protect Plus.

[“Protección de contenedores utilizando la línea de mandatos”](#) en la página 348

Como desarrollador de aplicaciones en un entorno de Kubernetes, puede utilizar la interfaz de línea de mandatos para hacer copia de seguridad y restaurar datos de contenedor, y para consultar el estado de las solicitudes de Soporte de copia de seguridad de Kubernetes.

## Registro de un clúster Kubernetes

Si es necesario, puede utilizar la interfaz de usuario de IBM Spectrum Protect Plus para registrar manualmente un clúster Kubernetes o para modificar las propiedades de un clúster Kubernetes registrado.

### Acerca de esta tarea

Una vez que Soporte de copia de seguridad de Kubernetes esté instalado, el host de aplicación para el contenedor de Soporte de copia de seguridad de Kubernetes se registra automáticamente al iniciarse el host de clúster en Kubernetes. Cuando se registra un clúster con IBM Spectrum Protect Plus, se captura automáticamente un inventario de los recursos del clúster, lo que le permite completar los trabajos de copia de seguridad y restauración, así como ejecutar informes.


Sin embargo, si el registro automático no se ha realizado correctamente o si se ha anulado accidentalmente el registro de un clúster registrado, puede registrar manualmente el clúster utilizando la interfaz de usuario de IBM Spectrum Protect Plus.

También puede modificar las propiedades del clúster registrado, como cambiar el puerto SSH que se utiliza para conectarse al servicio de agente del contenedor de Soporte de copia de seguridad de Kubernetes.

Por ejemplo, si utiliza un equilibrador de carga en su clúster, puede editarlo para utilizar el número de puerto para el servicio de contenedor del agente de Soporte de copia de seguridad de Kubernetes. A continuación, puede registrar el equilibrador de carga y el número de puerto con IBM Spectrum Protect Plus para que no tenga que volver a configurar el número de puerto.

### Procedimiento

Para registrar manualmente un clúster o para modificar las propiedades de clúster, complete los pasos siguientes:

1. En el panel de navegación, haga clic en **Gestionar protección > Contenedores > Kubernetes**.
2. En la página **Kubernetes**, pulse **Gestionar clústeres**.
3. Realice una de las acciones siguientes:
  - Para registrar manualmente un clúster, pulse **Añadir clúster**.
  - Para actualizar las propiedades de clúster existentes, en la lista de direcciones de host, haga clic en el icono de edición  para el host de clúster que desea actualizar.
4. Actualice los campos en la sección **Propiedades de aplicación**:

#### Nombre de clúster

El nombre del host de clúster o equilibrador de carga para el contenedor de Soporte de copia de seguridad de Kubernetes. Puede especificar un nombre de host o una dirección IP.

El nombre de clúster debe coincidir con el valor que se utiliza para el parámetro **CLUSTER\_NAME** en el archivo de configuración `baas_config.cfg`.

#### Dirección de host

La dirección de host para el host de clúster o el equilibrador de carga. Puede especificar una dirección IP o un nombre de dominio completo.

#### Número de puerto

El puerto SSH para la conexión al servicio de contenedor de agente de Soporte de copia de seguridad de Kubernetes.

De forma predeterminada, Kubernetes asigna automáticamente el puerto durante la instalación de Soporte de copia de seguridad de Kubernetes. Para obtener este número de puerto, emita el mandato siguiente en la línea de mandatos de **kubect1**:

```
kubect1 get service -n baas | grep baas-spp-agent
```

La salida es similar a la que se muestra en el ejemplo siguiente:

baas-spp-agent	NodePort	10.110.235.90	<none>	22:31299/TCP	111m
----------------	----------	---------------	--------	--------------	------

El número de puerto es la serie numérica que sigue a 22:. En el ejemplo, el número de puerto es 31299.

### Utilizar usuario existente

Seleccione esta casilla de verificación para utilizar un nombre de usuario y una contraseña especificados anteriormente para el host de clúster. Seleccione un nombre de usuario de la lista **Seleccionar usuario**.

### ID de usuario

Especifique el nombre de usuario del host de aplicación. Este campo no está disponible si está utilizando un usuario existente.

Para recuperar el nombre de usuario del host de aplicación del objeto baas-secret, emita el siguiente mandato para obtener y decodificar el nombre de usuario del transportador de datos:

```
echo "`kubect1 get secret baas-secret -n baas -o yaml | /bin/grep datamoveruser | cut -d: -f2 | tr -d ' ' | base64 -d`"
```

Especifique el resultado en el campo **ID de usuario**. Por ejemplo, especifique W36KdGtLWXtuN6L.

Las credenciales del host de aplicación se añadirán a la lista de usuarios existentes.

### Contraseña

Especifique la contraseña para el host de aplicación. Este campo no está disponible si está utilizando un usuario existente.

Para recuperar la contraseña del host de aplicación del objeto baas-secret, emita el mandatos siguiente para obtener y decodificar la contraseña del transportador de datos:

```
echo "`kubect1 get secret baas-secret -n baas -o yaml | /bin/grep datamoverpassword | cut -d: -f2 | tr -d ' ' | base64 -d`"
```

Especifique el resultado en el campo **Contraseña**. Por ejemplo, especifique w6EFx36vrdPzm0BC5Rth0S66f23PCznL.

## 5. Opcional: Rellene el campo en la sección **Opciones**:

### Máximo de PVC simultáneos

Establezca el número de copias de seguridad de copia o instantáneas de PVC que se pueden crear simultáneamente simultáneamente. El rendimiento de clúster se ve afectado cuando realiza una copia de seguridad de muchas PVC de forma simultánea, ya que cada PVC utiliza varias hebras y consume ancho de banda al copiar datos. Utilice esta opción para controlar el impacto en los recursos de clúster y minimizar el impacto en las operaciones de producción.

El valor predeterminado es 10.

## 6. Pulse **Guardar**. IBM Spectrum Protect Plus confirma una conexión de red, añade el clúster a la base de datos de IBM Spectrum Protect Plus y, a continuación, cataloga los recursos de clúster, incluidos los espacios de nombres y los PVC.

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 es satisfactoria, póngase en contacto con el administrador de red para revisar la conexión.

## Qué hacer a continuación

Para verificar que los clústeres se han actualizado, revise el registro de trabajo. En el panel de navegación, haga clic en **Trabajos y operaciones**. Haga clic en la pestaña **Trabajos en ejecución** y busque la entrada de registro **Inventario de servidor de aplicaciones** más reciente. Puede especificar un filtro para mostrar solo los trabajos de inventario pulsando el icono de filtro, seleccionando **Inventario** y haciendo clic en **Aplicar**.

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. Si el estado de un trabajo de inventario es **Parcial**, haga clic en **Registro de trabajo** y revise las entradas de registro para encontrar el error.

Deben detectarse clústeres para garantizar que se puede hacer copia de seguridad de ellos. Puede ejecutar un inventario manual en cualquier momento para detectar actualizaciones en los recursos de clúster. Para obtener instrucciones sobre la ejecución de un inventario manual, consulte [“Detección de recursos del clúster Kubernetes”](#) en la página 337. Para obtener instrucciones sobre la planificación de trabajos de copia de seguridad de Kubernetes, consulte [“Definición de copias de seguridad del acuerdo de nivel de servicio de volúmenes persistentes”](#) en la página 338.

## Detección de recursos del clúster Kubernetes

Los recursos del clúster Kubernetes se detectan automáticamente después de que se añade el clúster a IBM Spectrum Protect Plus. Sin embargo, puede ejecutar un trabajo de inventario para detectar los cambios que se han producido desde que se ha añadido el clúster.

## Acerca de esta tarea

Ejecute un trabajo de inventario de forma periódica para ayudar a garantizar que se detectan todos los recursos de clúster y que se puede realizar una copia de seguridad de ellos.

## Procedimiento

Para ejecutar un trabajo de inventario, realice los pasos siguientes:

1. En el panel de navegación, haga clic en **Gestionar protección > Contenedores > Kubernetes**.
2. En la lista de clústeres, seleccione un clúster o pulse el enlace para que el clúster vaya al recurso que desee.
3. Pulse **Ejecutar inventario**.

Cuando se ejecuta el inventario, el botón **Ejecutar inventario** cambia a **Inventario en curso**. Puede ejecutar un inventario en cualquier clúster disponible, pero solo puede ejecutar un proceso de inventario a la vez.

Si no selecciona un clúster en la lista de clústeres y pulsa **Ejecutar inventario**, se inicia un trabajo de inventario para todos los clústeres.

## Qué hacer a continuación

Para supervisar el trabajo de inventario, en el panel de navegación, haga clic en **Trabajos y operaciones**. Haga clic en la pestaña **Trabajos en ejecución** y busque la entrada de registro **Inventario de servidor de aplicaciones** más reciente. Puede especificar un filtro para mostrar solo los trabajos de inventario pulsando el icono de filtro, seleccionando **Inventario** y haciendo clic en **Aplicar**.

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. Si el estado de un trabajo de inventario es **Parcial**, haga clic en **Registro de trabajo** y revise las entradas de registro para encontrar el error.

### Prueba de conexión a un clúster Kubernetes

Puede probar la conexión a un clúster Kubernetes que ha añadido a IBM Spectrum Protect Plus. La función de prueba verifica la comunicación con el clúster y prueba los valores del servidor de nombres de dominio (DNS) entre el servidor de IBM Spectrum Protect Plus y el clúster.

#### Procedimiento

Para probar la conexión a un clúster, complete los pasos siguientes:

1. En el panel de navegación, haga clic en **Gestionar protección > Contenedores > Kubernetes**.
2. Pulse **Gestionar clústeres**.  
Se muestra la lista de clústeres disponibles.
3. Desplácese a través de la lista y localice el clúster que desea probar.
4. Haga clic en el menú **Acciones** asociado con el clúster y seleccione **Probar**.

El informe de prueba le muestra una lista de las pruebas que se han ejecutado y su estado.

### Definición de copias de seguridad del acuerdo de nivel de servicio de volúmenes persistentes

Puede utilizar la interfaz de usuario de IBM Spectrum Protect Plus para definir trabajos de copia de seguridad según la política de acuerdo de nivel de servicio (SLA). La política de SLA especifica la frecuencia con la que se ejecutan las operaciones de copia de seguridad y cuánto tiempo se guardan las copias de seguridad de instantáneas o de copia

#### Antes de empezar

Realice las acciones siguientes:

- Asegúrese de que se formatean las reclamaciones de volumen persistente (PVC) para los volúmenes que desea proteger. Las solicitudes de copia de seguridad se dirigen a las PVC. No se admiten las operaciones de copia de seguridad de volúmenes de bloque en bruto.
- Si no tiene previsto utilizar la política de SLA predeterminada para contenedores, asegúrese de configurar una política de SLA. Para obtener instrucciones, consulte [“Creación de una política de SLA para clústeres Kubernetes”](#) en la página 250.
- Asegúrese de que se asignan los roles y grupos de recursos adecuados al usuario que ejecutará el trabajo de copia de seguridad. 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. Para obtener instrucciones, consulte [Capítulo 18, “Gestión del acceso de usuarios”](#), en la página 533.
- Si una PVC está asociada con varias políticas de SLA, asegúrese de que las políticas no están planificadas 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.

#### Acerca de esta tarea





Para empezar a proteger las PVC en una planificación regular, debe aplicar una política de SLA a su PVC. La política de SLA también define las ubicaciones de destino de copia de seguridad para las PVC.

#### Procedimiento

Para definir un trabajo de copia de seguridad de SLA para una o más PVC, realice los pasos siguiente:

1. En el panel de navegación, haga clic en **Gestionar protección > Contenedores > Kubernetes**.
2. En el panel **Copia de seguridad de Kubernetes**, seleccione las PVC de las que desea hacer copia de seguridad. Puede utilizar uno de los métodos siguientes:



Método	Pasos
Para hacer copia de seguridad de todas las PVC de un clúster	Seleccione la casilla de verificación para un nombre de clúster. Un clúster se identifica por el icono de clúster  .
Para hacer copia de seguridad de todas las PVC asociadas con un espacio de nombres	<p>a. Haga clic en <b>Ver &gt; Espacio de nombres</b>.</p> <p>b. Haga clic en el nombre del clúster que contiene las PVC de las que desea hacer copia de seguridad. Se muestra la lista de los espacios de nombres dentro del clúster. Un espacio de nombres se identifica mediante el icono de espacio de nombres .</p> <p>c. Para hacer copia de seguridad de todas las PVC del espacio de nombres, seleccione la casilla de verificación para el espacio de nombres. Para hacer copia de seguridad de las PVC individuales, haga clic en el enlace de espacio de nombres y seleccione la casilla de verificación para cada PVC de la que desee hacer copia de seguridad. Una PVC se identifica mediante el icono PVC .</p>
Para hacer copia de seguridad de las PVC que están asociadas con una etiqueta	<p>a. Haga clic en <b>Ver &gt; Etiqueta</b>.</p> <p>b. Haga clic en el nombre del clúster que contiene las PVC de las que desea hacer copia de seguridad. Se visualiza la lista de etiquetas del clúster. Se visualiza una etiqueta como un par de clave-valor y se identifica mediante el icono de etiqueta .</p> <p>c. Para hacer copia de seguridad de todas las PVC asignadas a una etiqueta, seleccione la casilla de verificación para la etiqueta. Para hacer copia de seguridad de las PVC individuales, haga clic en el nombre de etiqueta y seleccione la casilla de verificación para cada PVC de la que desee hacer copia de seguridad.</p>
Para utilizar la función de búsqueda para filtrar la lista de PVC por SLA	<p>a. Escriba el criterio de búsqueda en el campo <b>Buscar</b>. Puede escribir todo el nombre de una PVC o parte de él. De forma alternativa, puede dejar el campo <b>Buscar</b> vacío para mostrar todas las PVC en un SLA.</p> <p>b. Seleccione un elemento del menú <b>Todas las PVC</b> para filtrar los resultados que coinciden con los criterios de búsqueda. Puede filtrar los resultados para mostrar todas las PVC, las PVC que no están en ningún SLA y las PVC que están en un SLA específico.</p> <p>c. Seleccione la casilla de verificación para cada PVC de la que desee hacer copia de seguridad.</p>

- Haga clic en **Seleccionar una política de SLA** y seleccione una o más políticas de la tabla **Política de SLA**. Puede elegir la política **Contenedor** predeterminada o puede elegir las políticas de SLA que ha definido.

Esta acción asigna la política de SLA seleccionada a las PVC seleccionadas. Si asigna una política de SLA en el nivel de etiqueta o espacio de nombres, cualquier PVC que cree con la etiqueta o en el espacio de nombres se asignará automáticamente al SLA.

- Para crear la definición de trabajo, haga clic en **Guardar**.

El trabajo se ejecuta según lo definido en las políticas de SLA que ha seleccionado. Para ejecutar el trabajo inmediatamente, haga clic en **Trabajos y operaciones > Planificar**. Seleccione el trabajo y haga clic en **Acciones > Inicio**.

**Ejecución de trabajos de copia de seguridad bajo demanda:** Cuando se ejecuta el trabajo para la política de SLA seleccionada, todas las PVC asociadas con esa política de SLA se incluyen en la operación de copia de seguridad. Para hacer copia de seguridad únicamente de las PVC seleccionadas,

puede ejecutar un trabajo bajo demanda. Un trabajo bajo demanda ejecuta inmediatamente la operación de copia de seguridad de instantánea.

- Para ejecutar un trabajo de copia de seguridad bajo demanda para una única PVC, seleccione la PVC y haga clic en **Ejecutar**. Si el recurso no está asociado con una política de SLA, el botón **Ejecutar** está inhabilitado.
- Para ejecutar un trabajo de copia de seguridad bajo demanda para una o más PVC, haga clic en **Crear trabajo**, seleccione **Copia de seguridad ad hoc** y siga las instrucciones de [“Ejecución de un trabajo de copia de seguridad ad hoc”](#) en la página 517.

### Qué hacer a continuación

Si es necesario, puede configurar opciones adicionales para el SLA. Para obtener las instrucciones, consulte [“Especificación de opciones de SLA para trabajos de copia de seguridad de Kubernetes”](#) en la página 340

**Opcional: Interrupción de las copias de seguridad para una PVC:** Si ya no desea que una PVC participe en los trabajos de copia de seguridad de SLA, elimine la asignación de políticas de SLA de la PVC realizando las siguientes acciones:

1. En el panel **Copia de seguridad de Kubernetes**, examine la tabla de clústeres, seleccione la PVC para la que desea interrumpir las operaciones de copia de seguridad y pulse **Seleccionar una política de SLA**.
2. En la tabla **Política de SLA**, identifique las políticas de SLA asignadas a la PVC. Se seleccionan las casillas de verificación para los SLA asignados.
3. Desmarque la casilla de verificación para la política de SLA que desea eliminar.
4. Pulse **Guardar**. La política de SLA ya no se asigna a la PVC.

### Conceptos relacionados

[“Tipos de copia de seguridad y restauración”](#) en la página 330

Soporte de copia de seguridad de Kubernetes proporciona varios tipos de funciones de copia de seguridad y restauración. Puede utilizar la interfaz de usuario de IBM Spectrum Protect Plus o la línea de mandatos de Kubernetes para iniciar las operaciones de copia de seguridad y restauración.


[“Políticas de SLA”](#) en la página 331

Las políticas de acuerdo de nivel de servicio (SLA) definen la frecuencia con la que se ejecutan las operaciones de copia de seguridad de copia y de copia de seguridad de instantánea y durante cuánto tiempo se retienen las copias de seguridad de copia y de instantánea. Puede configurar SLA personalizados que cumplan los requisitos operativos.

### Especificación de opciones de SLA para trabajos de copia de seguridad de Kubernetes

Después de seleccionar un acuerdo de nivel de servicio (SLA) para su trabajo de copia de seguridad, puede configurar más opciones para ese SLA. Las opciones de SLA adicionales incluyen la ejecución de scripts, la exclusión de recursos de la operación de copia de seguridad y la ejecución forzosa de una copia de seguridad de base de datos completa.

### Procedimiento

1. En el panel de navegación, haga clic en **Gestionar protección > Contenedores > Kubernetes**.
2. En la columna **Opciones de política** de la tabla **Estado de la política de SLA**, haga clic en el icono de portapapeles  para una política de SLA y establezca las opciones siguientes:

#### Script anterior

Seleccione esta casilla de verificación para ejecutar un script antes de que se ejecute un trabajo. Las máquinas basadas en Windows admiten scripts batch y PowerShell mientras que las máquinas basadas en Linux admiten scripts de shell. Realice 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 la casilla de verificación **Utilizar servidor de scripts** y elija un servidor de aplicaciones de la lista **Servidor de aplicaciones**.

Los scripts y servidores de script se configuran mediante la página **Configuración del sistema > Script**.

#### **Script posterior**

Seleccione esta casilla de verificación para ejecutar un script después de que se ejecute un trabajo. Las máquinas basadas en Windows admiten scripts batch y PowerShell mientras que las máquinas basadas en Linux admiten scripts de shell. Realice 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 la casilla de verificación **Utilizar servidor de scripts** y elija un servidor de aplicaciones de la lista **Servidor de aplicaciones**.

Los scripts y servidores de script se configuran mediante la página **Configuración del sistema > Script**.

#### **Continuar trabajo/tarea en error de script**

Seleccione esta casilla de verificación para continuar ejecutando el trabajo cuando falla el script asociado con el trabajo.

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 el estado de la tarea de script anterior o de script posterior se notifica como COMPLETADO.

Cuando esta opción está inhabilitada, no se intenta realizar el trabajo de copia de seguridad o restauración y el estado de la tarea de script anterior o de script posterior se notifica como FALLIDO.

#### **Excluir recursos**

Se excluyen recursos específicos del trabajo de copia de seguridad utilizando uno o más patrones de exclusión. 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: - \_ \*

Separe varios con un punto y coma.

3. Pulse **Guardar**.

## **Restauración de datos de contenedor**

Puede utilizar la interfaz de usuario de IBM Spectrum Protect Plus para restaurar un volumen persistente desde una instantánea o copia de seguridad de copia. Una operación de restauración de instantánea suele ser el método más rápido para restaurar un volumen persistente.

#### **Antes de empezar**

Revise las restricciones siguientes:

- No puede restaurar una copia de seguridad de instantánea o de copia en un espacio de nombres o clúster distinto.
- No puede restaurar una copia de seguridad de instantánea o de copia en el volumen persistente original. Puede restaurar una copia de seguridad de instantánea o de copia solo en un volumen persistente nuevo. La reclamación de volumen persistente (PVC) para el nuevo volumen se crea automáticamente durante la operación de restauración.
- Para asegurarse de que una solicitud de restauración funciona correctamente, no suprima manualmente instantáneas de volúmenes protegidos por Soporte de copia de seguridad de Kubernetes.

## Acerca de esta tarea




Para crear el trabajo de restauración, utilice el asistente **Restaurar**. Puede crear trabajos bajo demanda que se ejecuten una vez después de la finalización del asistente.

## Procedimiento

Para restaurar los volúmenes persistentes de instantáneas o copias de seguridad de copia, defina un trabajo de restauración realizando los pasos siguientes:

1. En el panel de navegación, haga clic en **Gestionar protección > Contenedores > Kubernetes**.
2. Haga clic en **Crear trabajo** para ir a la página **Crear trabajo**.
3. En el panel **Restaurar**, haga clic en **Seleccionar** para abrir el asistente **Restaurar**.

### Sugerencias:

- También puede abrir el asistente **Restaurar** haciendo clic en **Trabajos y operaciones > Crear trabajo**. A continuación, haga clic en **Seleccionar** en el panel **Restaurar** y en **Kubernetes**.
  - Para obtener un resumen en ejecución de las selecciones en el asistente, pulse **Vista previa de restauración** en el panel de navegación del asistente.
  - El asistente se abre en la modalidad de configuración predeterminada. Para ejecutar el asistente en modalidad de configuración avanzada, establezca la modalidad en **Configuración avanzada**. Con la modalidad de configuración avanzada, puede establecer más opciones para el trabajo de restauración.
4. En la página **Seleccionar origen**, vaya a la tabla y seleccione la PVC que desee restaurar pulsando el icono de signo más  para la PVC.
- Los PVC seleccionados se muestran en la lista **Elemento**. Si necesita eliminar un elemento de la lista, haga clic en el icono de signo menos  al lado del elemento.
- De forma alternativa, puede buscar una PVC especificando todo o parte del nombre de PVC en el campo **Buscar** y haga clic en el icono de búsqueda .
5. En la página **Instantánea de origen**, utilice uno de los métodos siguientes para seleccionar el origen desde el que desea restaurar:
- Para restaurar una PVC desde una instantánea:
    - a. Haga clic en **Origen > Desde instantánea**.
    - b. Haga clic en **Tipo de restauración > Bajo demanda** para ejecutar una operación de restauración única. El trabajo de restauración se iniciará inmediatamente después de la finalización del asistente. La opción **Recurrente** no se aplica a operaciones de restauración de Kubernetes.
    - c. Haga clic en el campo de rango de fechas y especifique un rango de fechas para mostrar las copias de seguridad de instantáneas disponibles dentro de ese rango de fechas.
    - d. Si está restaurando una única PVC, seleccione una instantánea de la lista de elementos disponibles. Si está restaurando más de una PVC, seleccione un punto de restauración para cada PVC que aparezca en la lista.
    - e. Pulse **Siguiente** para continuar.
  - Para restaurar una PVC a partir de una copia de seguridad de copia:
    - a. Haga clic en **Origen > Desde copia**.
    - b. Haga clic en **Tipo de restauración > Bajo demanda** para ejecutar una operación de restauración única. El trabajo de restauración se iniciará inmediatamente después de la finalización del asistente. La opción **Recurrente** no se aplica a operaciones de restauración de Kubernetes.
    - c. En el menú **Tipo de ubicación de restauración**, seleccione un tipo de ubicación desde el que restaurar datos:

### Sitio

El sitio donde se hizo la copia de seguridad de datos. El sitio se define en el panel **Configuración del sistema > Sitio**.

### **Servicio en la nube**

El servicio en la nube donde se copiaron los datos. El servicio en la nube se define en **Configuración del sistema > Almacenamiento de copias de seguridad > Almacenamiento de objetos**.

### **Servidor de repositorio**

El servidor de repositorio donde se copiaron los datos. El servidor de repositorio se define en **Configuración del sistema > Almacenamiento de copias de seguridad > Servidor de repositorio**.

### **Archivado de servicio en la nube**

El servicio de archivado en la nube donde se copiaron los datos. El servicio en la nube se define en el panel **Configuración del sistema > Almacenamiento de copias de seguridad > Almacenamiento de objetos**.

### **Archivado de servidor de repositorio**

El servidor de repositorio donde los datos se han copiado en cintas. El servidor de repositorio se define en el panel **Configuración del sistema > Almacenamiento de copias de seguridad > Servidor de repositorio**.

d. En el menú **Seleccionar una ubicación**, realice una de las acciones siguientes:

- Si está restaurando datos desde un sitio, seleccione una de las siguientes ubicaciones de restauración:

#### **Demo**

El sitio de demostración desde el que restaurar copias de seguridad de copia.

#### **Primario**

El sitio primario desde el que restaurar copias de seguridad de copia.

#### **Secundario**

El sitio secundario desde el que restaurar copias de seguridad de copia.

- Si está restaurando datos desde un servidor de nube o de repositorio, seleccione un servidor en el menú **Seleccionar una ubicación**.

e. Haga clic en el campo de rango de fechas y especifique un rango de fechas para mostrar las copias de seguridad de copia disponibles en ese rango de fechas.

f. Si está restaurando una única PVC, seleccione una copia de seguridad de la lista de elementos disponibles. Si está restaurando más de una PVC, seleccione un punto de restauración para cada PVC que aparezca en la lista.

g. Pulse **Siguiente** para continuar.

6. En la página **Método de restauración**, escriba un nuevo nombre para la PVC restaurada.

Para designar una PVC nuevo, puede escribir hasta 221 caracteres para el nombre de PVC y un prefijo de 32 caracteres. Puede incluir caracteres alfanuméricos, puntos (.) y guiones (-). El nuevo nombre de la PVC no debe contener letras mayúsculas y no debe terminar con un guión o un punto. Por ejemplo, `restored-pvc1` es un nombre de PVC válido.

La PVC solo puede restaurarse en modalidad de producción en el espacio de nombres original.

Pulse **Siguiente** para continuar.

7. En la página **Opciones de trabajo**, configure opciones adicionales para el trabajo de restauración:

#### **Ejecutar la limpieza inmediatamente en caso de anomalía del trabajo**

Si la recuperación de PVC falla, limpie automáticamente los recursos asignados como parte del trabajo de restauración.

#### **Permitir la sobrescritura de sesión**

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.

### Continúe con las restauraciones de otros PVC seleccionados si uno falla

Si una PVC no se restaura correctamente, el trabajo de restauración continúa para todos los demás PVC que se están restaurando. Si esta opción no está habilitada, el trabajo de restauración se detiene cuando falla la recuperación de una PVC.

Pulse **Siguiente** para continuar.

8. Opcional: Si ejecuta el asistente en modalidad de configuración avanzada, en la página **Aplicar scripts**, especifique los scripts a ejecutar antes o después de que una operación se ejecute en el nivel de trabajo. Los scripts Batch y PowerShell están soportados.

#### Script anterior

Seleccione esta casilla de verificación para elegir un script cargado y un servidor de aplicaciones o scripts donde se ejecutará el script anterior. Para seleccionar el servidor de aplicaciones donde se ejecutará el script anterior, desmarque la casilla de verificación **Usar 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 el servidor de aplicaciones donde se ejecutará el script posterior, desmarque la casilla de verificación **Usar 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 esta casilla de verificación para continuar ejecutando el trabajo cuando falla el script asociado con el trabajo.

Cuando selecciona esta casilla de verificación, 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 o script posterior como COMPLETADO.

Si desmarca esta casilla de verificación, la operación de restauración no se intenta y el estado de la tarea del script anterior o del script posterior se notifica como FALLIDO.

9. En la página **Revisar**, revise los valores del trabajo de restauración y pulse **Enviar** para crear el trabajo.

### Resultados

En los trabajos bajo demanda, un trabajo 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 haciendo clic en **Descargar.zip**.

Todos los trabajos en ejecución se pueden visualizar en la página **Trabajos y operaciones > Trabajos en ejecución**.

#### Qué hacer a continuación

Para verificar si la PVC se ha restaurado, emita el mandato **kubect1** siguiente:

```
kubect1 get pvc restored_pvc -n namespace
```

donde *restored\_pvc* especifica el nombre de la PVC restaurada y *namespace* especifica el espacio de nombres de la PVC restaurada.

### Caducidad de las sesiones de trabajo de Kubernetes

Puede hacer que una sesión de trabajo de copia de seguridad de Kubernetes caduque para alterar temporalmente los valores de retención que se asignaron al crear una copia de seguridad de instantánea o de copia. Cuando caduca una sesión de trabajo, el punto de restauración (la copia de seguridad de instantánea o de copia) se eliminará durante el siguiente trabajo de mantenimiento.

## Acerca de esta tarea


Complete esta tarea si no desea esperar a que una sesión de trabajo caduque automáticamente según el valor de retención de la política de acuerdo de nivel de servicio asignada.

## Procedimiento

Para hacer que una sesión de trabajo de Kubernetes caduque, complete los pasos siguientes:

1. En el panel de navegación, haga clic en **Gestionar protección > IBM Spectrum Protect Plus > Restaurar punto de restauración**.
2. En la pestaña **Sesiones de copia de seguridad**, busque una sesión de trabajo o punto de restauración. De forma alternativa, en la ficha **Máquinas virtuales / Bases de datos**, seleccione **Aplicaciones** y busque una entrada de catálogo escribiendo el nombre.

Los nombres se pueden buscar escribiendo un texto parcial, usando un asterisco (\*) como carácter comodín o usando un signo de interrogación (?) para la coincidencia de patrón. Para obtener más información sobre la función de búsqueda, consulte [Apéndice A, “Directrices de búsqueda”, en la página 567](#).

3. Opcional: Si está buscando en la pestaña **Sesiones de copia de seguridad**, utilice filtros para limitar la búsqueda de copias de seguridad de instantáneas y de copia. También puede especificar el rango de fechas cuando se inicie el trabajo de copia de seguridad asociado.
  - a) En el campo **Tipo**, seleccione **Aplicación**.
  - b) En el campo **Tipo de subpolítica**, seleccione **Instantánea** para buscar copias de seguridad de instantáneas o seleccione **Copia de seguridad** para buscar copias de seguridad de copia.
  - c) Si es necesario, haga clic en el campo **Rango de tiempo de la copia de seguridad** y seleccione el rango de fechas que desea buscar.
4. Pulse el icono de búsqueda .
5. En los resultados de búsqueda, seleccione la sesión de trabajo que desea que caduque.
6. Si está en la pestaña **Sesiones de copia de seguridad**, en el menú **Acciones**, seleccione una de las siguientes opciones:
  - Para hacer que una sesión de trabajo única caduque, haga clic en **Caducar**.
  - Para hacer que caduquen todas las sesiones de trabajo no caducadas para el trabajo seleccionado, haga clic en **Caducar todas las sesiones de trabajo**.

Si está en la pestaña **Máquinas virtuales / Bases de datos**, haga clic en el icono de supresión  para el recurso que desea que caduque.

7. Siga las instrucciones de la ventana de confirmación y pulse **Aceptar**.

## Tareas relacionadas

“Gestión de puntos de restauración de IBM Spectrum Protect Plus” en la página 506

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.

## Supervisión de trabajos de Soporte de copia de seguridad de Kubernetes y ejecución de informes

Como administrador de copia de seguridad, puede utilizar la interfaz de usuario de IBM Spectrum Protect Plus para supervisar trabajos de Soporte de copia de seguridad de Kubernetes y crear informes que muestran el historial de copia de seguridad de los contenedores.

### Visualización de los registros de trabajo

Puede utilizar la ventana **Trabajos y operaciones** para supervisar los trabajos de Soporte de copia de seguridad de Kubernetes, revisar el historial de trabajos y ver los trabajos planificados.

## Acerca de esta tarea

Puede identificar los trabajos en las pestañas **Trabajos en ejecución** y **Historial de trabajos** de la siguiente manera:

- Los trabajos de inventario se identifican mediante la etiqueta `Inventario del servidor de aplicaciones`.
- Los trabajos de mantenimiento se identifican mediante la etiqueta `Mantenimiento`.
- Los nombres de trabajo de copia de seguridad se identifican mediante la etiqueta `k8s_sla_name`.

El tipo de trabajo se muestra en el campo `Tipo`. Por ejemplo, un trabajo de copia de seguridad de instantánea se identifica por `Tipo: Copia de seguridad - Instantánea`. Una copia de seguridad de copia se identifica por `Tipo: Copia de seguridad`.

- Los nombres del trabajo de restauración se identifican por la etiqueta `onDemandRestore_timestamp`. El tipo de trabajo es `Tipo: Restaurar`.

## Procedimiento

1. En el panel de navegación de IBM Spectrum Protect Plus, haga clic en **Trabajos y operaciones**.
2. Haga clic en la pestaña adecuada:

- Para visualizar los trabajos de inventario, copia de seguridad y restauración que están en ejecución, haga clic en **Trabajos en ejecución**.
- Para ver los trabajos que se han ejecutado correctamente, que el proceso se ha completado con advertencias o los trabajos que han fallado, haga clic en **Historial de trabajos**. Puede descargar un registro de trabajo de la página seleccionando el trabajo y pulsando **Descargar.zip**.

El archivo descargado tiene el siguiente convenio de denominación:

`JobLog_nombre;trabajo_indicación_fecha_hora.zip`

- Para ver el estado de los trabajos planificados, pulse **Planificar**.
- Para obtener un acceso directo para crear un trabajo de copia de seguridad ad hoc o un trabajo de restauración sin ir a la página **Kubernetes** en la sección **Gestionar protección**, haga clic en **Crear trabajo**.

## Conceptos relacionados

[“Creación de trabajos y planificaciones de trabajos” en la página 510](#)

El método para crear trabajos y planificaciones de trabajos depende del tipo de trabajo.

## Tareas relacionadas

[“Visualización de trabajos” en la página 512](#)

Vea información sobre el estado de los trabajos en ejecución y el estado general de los trabajos que se completaron correctamente o con fallos o advertencias.

## Creación de informes de historial de copia de seguridad para volúmenes persistentes

Puede ejecutar un informe para mostrar el historial de copia de seguridad de los volúmenes persistentes protegidos. Visualizando el historial de copia de seguridad, puede determinar si los trabajos de seguridad se están ejecutando según lo planeado.

## Antes de empezar

Si tiene previsto planificar un informe para que se ejecute en momentos específicos, asegúrese de configurar un servidor SMTP para las notificaciones de correo electrónico. Para obtener instrucciones, consulte [“Adición de un servidor SMTP” en la página 217](#).

## Acerca de esta tarea





Para cada reclamación de volumen persistente (PVC), el historial de copia de seguridad muestra información sobre las instantáneas de la Interfaz de almacenamiento de copias de seguridad (CSI) que se crearon en el entorno de Kubernetes y las copias de seguridad que se copiaron en el servidor vSnap de



IBM Spectrum Protect Plus. Puede ver información como la fecha y hora de la operación de copia de seguridad, el tamaño de la copia de seguridad y la duración de la operación de copia de seguridad. A partir de estos datos, puede verificar si las copias de seguridad planificadas se están ejecutando según la política de acuerdo de nivel de servicio (SLA) que establece para PVC.

## Procedimiento

1. En el panel de navegación de IBM Spectrum Protect Plus, haga clic en **Informes y registros > Informes**.
2. En la columna **Nombre (título de trabajo)**, localice la fila **Historial de copia de seguridad de volumen persistente de contenedor** y realice una de las siguientes acciones:

Acción	Pasos
Para ejecutar un informe inmediatamente	<ol style="list-style-type: none"> <li>a. Haga clic en el icono Ejecutar informe .</li> <li>b. En la ventana <b>Ejecutar informe</b>, modifique los parámetros según sea necesario y haga clic en <b>Ejecutar</b>.</li> </ol>
Para planificar un informe con los parámetros predeterminados	<ol style="list-style-type: none"> <li>a. Haga clic en el icono Planificar informe con parámetros predeterminados .</li> <li>b. En la ventana <b>Planificar informe con parámetros predeterminados</b>, especifique la frecuencia, la hora de inicio y la dirección de correo electrónico de un destinatario.</li> <li>c. Pulse <b>Planificar</b>.</li> </ol>
Para crear un informe personalizado	<ol style="list-style-type: none"> <li>a. Haga clic en el icono Crear informe personalizado . Se visualiza la ventana <b>Crear informe personalizado</b>.</li> <li>b. En la pestaña <b>Parámetros</b>, especifique un nombre y una descripción para el informe personalizado y modifique los parámetros de informe según sea necesario. El nombre del informe no debe contener espacios.</li> <li>c. Para planificar el informe para que se ejecute en momentos específicos, haga clic en la pestaña <b>Planificar</b> y seleccione <b>Definir planificación</b>.</li> <li>d. Especifique la frecuencia, la hora de inicio y la dirección de correo electrónico de un destinatario.</li> <li>e. Pulse <b>Guardar informe</b>.</li> </ol> <p>El informe personalizado se guarda en la pestaña <b>Informes personalizados</b> de la ventana <b>Informes</b>.</p>
Para ejecutar un informe personalizado	<ol style="list-style-type: none"> <li>a. Haga clic en la pestaña <b>Informes personalizados</b>.</li> <li>b. Identifique el informe que desea ejecutar y haga clic en el icono Ejecutar informe personalizado .</li> <li>c. En la ventana <b>Ejecutar informe personalizado</b>, haga clic en <b>Ejecutar</b>.</li> </ol>

## Resultados

Si ha ejecutado el informe inmediatamente, el informe del historial de copia de seguridad se muestra en la ventana **Historial de copia de seguridad de volumen persistente de contenedor**. Para descargar el informe, pulse **Descargar** y seleccione un formato de informe. Para volver a la ventana **Informes**, haga clic en **Volver a Informes**.

Si ha definido una planificación para el informe, el informe del historial de copia de seguridad se ejecuta a la hora planificada y se envía al destinatario que ha especificado.

Las descripciones de los datos notificados se muestran en la tabla siguiente:

Tabla 58. Detalles del informe del historial de copia de seguridad

Columna	Descripción
Política de SLA	La política de SLA que se utiliza para proteger una PVC.
Tiempo de protección	La fecha y hora cuando se completa cada uno de los trabajos de copia de seguridad.
Estado	El estado de cada trabajo de copia de seguridad. Si un trabajo de copia de seguridad falla, se proporciona un posible motivo.
¿Copia de seguridad de instantánea?	Una indicación de si la instancia de copia de seguridad es una copia de seguridad de instantánea. Se muestra una marca de selección en la columna para indicar que la instancia es una copia de seguridad de instantánea. Cuando se muestra una marca de selección, no se muestran datos en las columnas <b>Tamaño de copia de seguridad</b> y <b>Velocidad de copia de seguridad</b> .
Tamaño de la copia de seguridad	Para copias de seguridad de copia, la cantidad de datos de los que se ha hecho copia de seguridad en el servidor vSnap. Para las copias de seguridad de instantánea que se crearon en el entorno de Kubernetes o para las copias de seguridad que han fallado, no se muestra ningún tamaño.
Velocidad de copia de seguridad	La velocidad a la que se ha completado una copia de seguridad de copia. Para copias de seguridad de instantánea o copias de seguridad que han fallado, no se muestran datos.

#### Conceptos relacionados

“Gestión de informes y registros” en la página 521

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.

## Protección de contenedores utilizando la línea de mandatos

Como desarrollador de aplicaciones en un entorno de Kubernetes, puede utilizar la interfaz de línea de mandatos para hacer copia de seguridad y restaurar datos de contenedor, y para consultar el estado de las solicitudes de Soporte de copia de seguridad de Kubernetes.

Asegúrese de que el entorno de Kubernetes cumple los requisitos del sistema en “Requisitos de Soporte de copia de seguridad de Kubernetes” en la página 56.

### Solicitudes de Soporte de copia de seguridad de Kubernetes

Para proteger los datos de contenedor, puede enviar solicitudes de Soporte de copia de seguridad de Kubernetes mediante la interfaz de línea de mandatos de Kubernetes.

Una solicitud de Soporte de copia de seguridad de Kubernetes es un recurso personalizado de Kubernetes de tipo BaaSReq. Las solicitudes se especifican en los archivos de configuración *YAML Ain't Markup Language* (YAML). A continuación, se envía la solicitud utilizando la interfaz de línea de mandatos **kubect1**.

#### Tipos de solicitudes en Soporte de copia de seguridad de Kubernetes

La tabla siguiente muestra los tipos disponibles de solicitudes de Soporte de copia de seguridad de Kubernetes. Los tipos de solicitud se especifican como valores para la clave **requesttype** en el archivo YAML. También se proporcionan enlaces a instrucciones sobre la creación y el envío de solicitudes.

Tabla 59. Tipos de solicitudes de Soporte de copia de seguridad de Kubernetes

Tipo de solicitud	Descripción	Instrucciones
<b>Backup</b>	Planificar una operación de copia de seguridad para una reclamación de volumen persistente (PVC) (incluye copias de seguridad de instantánea y de copia)	<a href="#">“Planificación de copias de seguridad de volúmenes persistentes utilizando la línea de mandatos” en la página 350</a>
<b>BackupLabel</b>	Copia de seguridad de todos los PVC que tienen una etiqueta específica	<a href="#">“Copia de seguridad de volúmenes persistentes por etiqueta utilizando la línea de mandatos” en la página 355</a>
<b>BackupNamespace</b>	Copia de seguridad de todos los PVC que están en un espacio de nombres específico	<a href="#">“Copia de seguridad de volúmenes persistentes por espacio de nombres utilizando la línea de mandatos” en la página 358</a>
<b>OnDemandBackup</b>	Solicitar una copia de seguridad de instantánea inmediata de una PVC	<a href="#">“Copia de seguridad de un volumen persistente bajo demanda utilizando la línea de mandatos” en la página 353</a>
<b>Restore</b>	Restaurar una PVC desde una copia de seguridad de instantánea o una copia de seguridad de copia	<a href="#">“Restauración de datos de contenedor utilizando la línea de mandatos” en la página 360</a>
<b>Destroy</b>	Suprimir todas las copias de seguridad de instantánea y de copia y marcar el trabajo planificado como <b>destruido</b>	<a href="#">“Supresión de copias de seguridad de contenedor” en la página 366</a>

## Ejecución de una solicitud

Para iniciar una solicitud, cree un archivo de configuración YAML que especifique el tipo de solicitud y proporcione los parámetros necesarios. A continuación, envíe la solicitud ejecutando el mandato **kubect1 create**.

El siguiente archivo de ejemplo (baas-req.yaml) muestra el formato general de un archivo YAML:

```
#-----
# Filename: baas-req.yaml
#-----

apiVersion: "baas.io/v1alpha1"
kind: BaaSReq

metadata:
  name: nombre_solicitud
  namespace: espacio_nombres
spec:
  requesttype: tipo_solicitud
  sla: [politica_sla]
  volumesnapshotclass: nombre_clase_instantánea
```

donde:

### **nombre\_solicitud**

Especifica el nombre de la solicitud. Para las solicitudes de copia de seguridad planificadas, el nombre de la solicitud debe coincidir con el nombre de PVC.

### ***espacio\_nombres***

Especifica el espacio de nombres en el que existe el volumen persistente. Si no especifica un espacio de nombres, se utiliza el espacio de nombres predeterminado.

### ***tipo\_solicitud***

Especifica el tipo de solicitud. Para obtener la lista de tipos de solicitud disponibles, consulte [“Tipos de solicitudes en Soporte de copia de seguridad de Kubernetes”](#) en la página 348.

### ***[política\_sla]***

Especifica una o más políticas de acuerdo de nivel de servicio (SLA) que asigna a la solicitud. Para obtener información sobre las especificaciones para la política de SLA, consulte [“Planificación de copias de seguridad de volúmenes persistentes utilizando la línea de mandatos”](#) en la página 350.

### ***nombre\_clase\_instantánea***

Especifica la clase de instantánea para el volumen. Si no especifica la clase de instantánea, se utiliza la clase de instantánea predeterminada si el contenedor de sidecar `csi-snapshotter` de la clase de instantánea predeterminada coincide con el suministrador del volumen. De lo contrario, la solicitud de copia de seguridad no es válida.

Para iniciar la solicitud que se especifica en el archivo de ejemplo `baas-req.yaml`, emita el siguiente mandato:

```
kubectl create -f baas-req.yaml
```

Para comprobar el estado de una solicitud, utilice uno de los métodos siguientes:

- Para listar todas las solicitudes de Soporte de copia de seguridad de Kubernetes en todos los espacios de nombres a los que puede acceder, emita el mandato siguiente:

```
kubectl get baasreq --all-namespaces
```

- Para visualizar el estado de todas las solicitudes de Soporte de copia de seguridad de Kubernetes en un espacio de nombres especificado, emita el mandato siguiente:

```
kubectl describe baasreq -n namespace
```

donde *namespace* es el espacio de nombres del volumen persistente.

- Para visualizar el estado de una solicitud de Soporte de copia de seguridad de Kubernetes específica, emita el mandato siguiente:

```
kubectl describe baasreq nombre_solicitud -n espacio_nombres
```

donde *nombre\_solicitud* es el nombre de la solicitud y *espacio\_nombres* es el espacio de nombres del volumen persistente.

## **Copia de seguridad de los datos de contenedor**

Para proteger los volúmenes persistentes conectados a un contenedor, puede planificar operaciones de copia de seguridad para que se ejecuten como se especifica en las políticas de acuerdo de nivel de servicio (SLA). También puede crear instantáneas de volúmenes persistentes inmediatamente ejecutando solicitudes de copia de seguridad bajo demanda.

### **Planificación de copias de seguridad de volúmenes persistentes utilizando la línea de mandatos**

Mediante la línea de mandatos de Kubernetes, puede planificar solicitudes de copia de seguridad basadas en políticas de acuerdo de nivel de servicio (SLA). Las políticas de SLA especifican la frecuencia con la que se ejecutan las operaciones de copia de seguridad y la cantidad de copias de seguridad de copia y de instantánea que se retienen.

### **Antes de empezar**

Las solicitudes de copia de seguridad están dirigidas a reclamaciones de volumen persistente (PVC) para los volúmenes que desea proteger. Antes de planificar un trabajo de copia de seguridad, realice las acciones siguientes:

- Asegúrese de que la PVC existe en el espacio de nombres especificado.
- Asegúrese de que la PVC esté formateado. Los PVC deben formatearse antes de que se pueda hacer una copia de seguridad de ellos. Para que una PVC tenga el formato correcto, debe estar montado y grabado. No se admiten las operaciones de copia de seguridad de volúmenes de bloque en bruto.
- Determine qué política de SLA se asigna a los PVC. Para obtener instrucciones sobre la visualización de políticas de SLA disponibles, consulte [“Políticas de SLA” en la página 331](#).

### Acerca de esta tarea

Cuando se ejecuta un trabajo de copia de seguridad planificado, se ejecuta automáticamente un inventario de recursos de clúster y se crea una instantánea del volumen persistente con la frecuencia definida por el SLA. Si el SLA especifica una política de copia de seguridad de copia, la instantánea del volumen se copia en un servidor vSnap de IBM Spectrum Protect Plus.

Se planifican todos los trabajos de copia de seguridad, excepto los trabajos de copia de seguridad bajo demanda. Para planificar trabajos para una PVC, cree un archivo de configuración YAML con las especificaciones de trabajo y aplique la solicitud en la línea de mandatos en el entorno de Kubernetes .

Puede especificar una o más políticas de SLA por PVC.

### Procedimiento

1. Opcional: Visualice una lista de PVC en el espacio de nombres emitiendo el siguiente mandato:

```
kubect1 get pvc -n namespace
```

En la lista de PVC, identifique la PVC de la que desea hacer una copia de seguridad.

2. Cree un archivo YAML que defina la solicitud de una copia de seguridad planificada. El archivo YAML debe contener las propiedades siguientes:

```
#-----
# Filename: filename.yaml
#-----

apiVersion: "baas.io/v1alpha1"
kind: BaaSReq

metadata:
  name: nombre_solicitud
  namespace: espacio_nombres
spec:
  requesttype: Backup
  sla: [política_sla]
  volumesnapshotclass: nombre_clase_instantánea
```

donde:

#### **nombre\_archivo**

Especifica el nombre del archivo de configuración de YAML. El tipo de archivo es .yaml.

#### **nombre\_solicitud**

Especifica el nombre de la solicitud de copia de seguridad, que debe coincidir con el nombre de la PVC para el volumen al que desea hacer una copia de seguridad. Por ejemplo, para crear una solicitud de copia de seguridad para una PVC que se denomina dbvo1-01, el nombre de la solicitud debe ser dbvo1-01.

#### **espacio\_nombres**

Especifica el espacio de nombres en el que existe la PVC.

#### **[política\_sla]**

Especifica la política de SLA que determina la planificación para las operaciones de copia de seguridad. Puede especificar más de una política de SLA utilizando una lista separada por comas entre corchetes.

Por ejemplo, para asignar la política `daily` a una PVC, especifique la siguiente sentencia:

```
sla: [daily]
```

Para asignar las políticas `every4hours`, `daily_midnight` y `weekly` a PVC, especifique la siguiente sentencia en el archivo YAML:

```
sla: [every4hours,daily_midnight,weekly]
```

De forma alternativa, puede utilizar el formato siguiente para especificar una única política de SLA:

```
sla:  
- daily
```

O, puede utilizar el siguiente formato para especificar varias políticas de SLA:

```
sla:  
- every4hours  
- daily_midnight  
- weekly
```

Asegúrese de que utiliza el caso correcto cuando especifica el nombre de política de SLA. Los nombres de política distinguen entre mayúsculas y minúsculas en los archivos YAML.

Para eliminar todas las asignaciones de SLA de una PVC, suprima los nombres de políticas de SLA entre corchetes, tal como se muestran en la siguiente sentencia:

```
sla: []
```

Especificar los corchetes vacíos es el único método que puede utilizar para eliminar todas las asignaciones de SLA de la PVC.

### ***nombre\_clase\_instantánea***

Especifica la clase de instantánea para el volumen. Si no especifica la clase de instantánea, se utiliza la clase de instantánea predeterminada si el contenedor de sidecar `csi-snapshotter` de la clase de instantánea predeterminada coincide con el proveedor del volumen. De lo contrario, la solicitud de copia de seguridad no es válida.

3. Envíe la solicitud de copia de seguridad emitiendo el siguiente mandato:

```
kubectl create -f filename.yaml
```

donde *filename* es el nombre del archivo de configuración de YAML.

## **Resultados**

Después de enviar la solicitud de copia de seguridad, la primera operación de copia de seguridad planificada se iniciará en la ventana definida por la política de SLA. La hora de inicio de la copia de seguridad se registra en el estado de copia de seguridad.

## **Qué hacer a continuación**

Para ver información sobre la operación de copia de seguridad, emita el mandato **kubectl describe** utilizando el nombre de solicitud o el nombre de PVC. Para obtener instrucciones, consulte [“Visualización del estado de los trabajos de copia de seguridad y restauración”](#) en la página 363.

## **Modificación de parámetros en un archivo YAML:**

Una vez que se hayan iniciado los trabajos de copia de seguridad planificada, puede modificar los parámetros en el archivo YAML y aplicarlo a la misma PVC si es necesario. Por ejemplo:

- Para asignar una política de SLA distinta a la PVC o eliminar una asignación de SLA, edite los valores del campo **sla** en el archivo YAML. A continuación, aplique el archivo YAML utilizando la interfaz de línea de mandatos **kubectl**.

- Si ya no desea que la PVC participe en trabajos de copia de seguridad planificada, elimine las asignaciones de política de SLA actualizando el campo **sla** en el archivo YAML. Para eliminar la PVC de todos los SLA, modifique el campo **sla** de la siguiente manera:

```
sla: []
```

A continuación, aplique el archivo YAML utilizando la interfaz de línea de mandatos **kubect1**.

### Conceptos relacionados

[“Tipos de copia de seguridad y restauración” en la página 330](#)

Soporte de copia de seguridad de Kubernetes proporciona varios tipos de funciones de copia de seguridad y restauración. Puede utilizar la interfaz de usuario de IBM Spectrum Protect Plus o la línea de mandatos de Kubernetes para iniciar las operaciones de copia de seguridad y restauración.

[“Políticas de SLA” en la página 331](#)

Las políticas de acuerdo de nivel de servicio (SLA) definen la frecuencia con la que se ejecutan las operaciones de copia de seguridad de copia y de copia de seguridad de instantánea y durante cuánto tiempo se retienen las copias de seguridad de copia y de instantánea. Puede configurar SLA personalizados que cumplan los requisitos operativos.

[“Solicitudes de Soporte de copia de seguridad de Kubernetes” en la página 348](#)

Para proteger los datos de contenedor, puede enviar solicitudes de Soporte de copia de seguridad de Kubernetes mediante la interfaz de línea de mandatos de Kubernetes.

[“Resolución de problemas de Soporte de copia de seguridad de Kubernetes” en la página 550](#)

Para ayudar a resolver problemas con Soporte de copia de seguridad de Kubernetes, puede recopilar archivos de registro de depuración y ver los registros de rastreo. También puede seguir procedimientos para diagnosticar problemas.

### Copia de seguridad de un volumen persistente bajo demanda utilizando la línea de mandatos

Para crear una instantánea inmediatamente sin esperar a que se ejecute un trabajo de copia de seguridad planificada, ejecute un trabajo de copia de seguridad bajo demanda en la interfaz de línea de mandatos de Kubernetes.

### Antes de empezar

Las solicitudes de copia de seguridad están dirigidas a reclamaciones de volumen persistente (PVC) para los volúmenes que desea proteger. Antes de planificar un trabajo de copia de seguridad, realice las acciones siguientes:

- Asegúrese de que la PVC existe en el espacio de nombres especificado.
- Asegúrese de que la PVC esté formateado. Los PVC deben formatearse antes de que se pueda hacer una copia de seguridad de ellos. Para que una PVC tenga el formato correcto, debe estar montado y grabado. No se admiten las operaciones de copia de seguridad de volúmenes de bloque en bruto.
- Determine qué política de SLA se asigna a los PVC. Para obtener instrucciones sobre la visualización de políticas de SLA disponibles, consulte [“Políticas de SLA” en la página 331](#).

### Acerca de esta tarea

Durante una operación de copia de seguridad bajo demanda, solo se crea una instantánea. Después de que se completa una operación de copia de seguridad bajo demanda inicial, el volumen se protegerá de acuerdo con la política de SLA especificada.

A diferencia de una solicitud para copias de seguridad planificadas, el nombre de la solicitud bajo demanda debe ser exclusivo. En otras palabras, el nombre de la solicitud no debe ser el mismo que el nombre de la PVC.

### Procedimiento

1. Opcional: Visualice una lista de PVC en el espacio de nombres emitiendo el siguiente mandato:

```
kubectl get pvc -n namespace
```

En la lista de PVC, identifique la PVC de la que desea hacer una copia de seguridad.

2. Cree un archivo YAML que define la solicitud para una operación de copia de seguridad bajo demanda. El archivo YAML debe contener las propiedades siguientes:

```
#-----  
# Filename: filename.yaml  
#-----  
  
apiVersion: "baas.io/v1alpha1"  
kind: BaaSReq  
  
metadata:  
  name: nombre_solicitud  
  namespace: espacio_nombres  
spec:  
  requesttype: OnDemandBackup  
  pvcname: nombre_pvc  
  sla: [política_sla]  
  volumesnapshotclass: nombre_clase_instantánea
```

donde:

**nombre\_archivo**

Especifica el nombre del archivo de configuración de YAML. El tipo de archivo es .yaml.

**nombre\_solicitud**

Especifica el nombre de la solicitud de copia de seguridad bajo demanda. El nombre debe ser exclusivo y no debe coincidir con el nombre de la PVC.

Se debe crear una nueva solicitud de copia de seguridad bajo demanda para cada copia de seguridad bajo demanda posterior de la misma PVC. En otras palabras, para crear una segunda copia de seguridad bajo demanda de una PVC, cree una nueva solicitud y especifique un nombre de solicitud diferente (*nombre de solicitud*) en el archivo YAML.

**espacio\_nombres**

Especifica el espacio de nombres en el que existe la PVC.

**nombre\_pvc**

Especifica el nombre de la PVC para el volumen al que desea hacer la copia de seguridad.

**[política\_sla]**

Especifica la política de SLA que determina la planificación para las operaciones de copia de seguridad. Por ejemplo, para asignar la política *daily* a una PVC, especifique la siguiente sentencia:

```
sla: [daily]
```

Asegúrese de que utiliza el caso correcto cuando especifica el nombre de política de SLA. Los nombres de política distinguen entre mayúsculas y minúsculas en los archivos YAML.

Todos los SLA que no estén en la solicitud de copia de seguridad planificada correspondiente para la PVC se añadirán a la lista de SLA de dicha solicitud.

**nombre\_clase\_instantánea**

Especifica la clase de instantánea para el volumen. Si no especifica la clase de instantánea, se utiliza la clase de instantánea predeterminada si el contenedor de sidecar *csi-snapshotter* de la clase de instantánea predeterminada coincide con el proveedor del volumen. De lo contrario, la solicitud de copia de seguridad no es válida.

3. Inicie la operación de copia de seguridad bajo demanda emitiendo el siguiente mandato:

```
kubectl create -f filename.yaml
```

donde *filename* es el nombre del archivo de configuración de YAML.



## Resultados

Para ver información sobre la copia de seguridad, emita el mandato **kubectl describe** utilizando el nombre de solicitud o el nombre de PVC. Para obtener instrucciones, consulte [“Visualización del estado de los trabajos de copia de seguridad y restauración” en la página 363](#).

## Conceptos relacionados

[“Tipos de copia de seguridad y restauración” en la página 330](#)

Soporte de copia de seguridad de Kubernetes proporciona varios tipos de funciones de copia de seguridad y restauración. Puede utilizar la interfaz de usuario de IBM Spectrum Protect Plus o la línea de mandatos de Kubernetes para iniciar las operaciones de copia de seguridad y restauración.

[“Solicitudes de Soporte de copia de seguridad de Kubernetes” en la página 348](#)

Para proteger los datos de contenedor, puede enviar solicitudes de Soporte de copia de seguridad de Kubernetes mediante la interfaz de línea de mandatos de Kubernetes.

[“Resolución de problemas de Soporte de copia de seguridad de Kubernetes” en la página 550](#)

Para ayudar a resolver problemas con Soporte de copia de seguridad de Kubernetes, puede recopilar archivos de registro de depuración y ver los registros de rastreo. También puede seguir procedimientos para diagnosticar problemas.

## Copia de seguridad de volúmenes persistentes por etiqueta utilizando la línea de mandatos

Puede crear solicitudes de copia de seguridad para volúmenes persistentes especificando etiquetas. Las etiquetas son pares de valor clave adjuntas a objetos, como pods o PVC. Al especificar una o más etiquetas en una solicitud de copia de seguridad, puede realizar una copia de seguridad de todos los PVC que están asociados con dichas etiquetas.

## Antes de empezar

Las solicitudes de copia de seguridad están dirigidas a reclamaciones de volumen persistente (PVC) para los volúmenes que desea proteger. Antes de planificar un trabajo de copia de seguridad, realice las acciones siguientes:

- Asegúrese de que la PVC existe en el espacio de nombres especificado.
- Asegúrese de que la PVC esté formateado. Los PVC deben formatearse antes de que se pueda hacer una copia de seguridad de ellos. Para que una PVC tenga el formato correcto, debe estar montado y grabado. No se admiten las operaciones de copia de seguridad de volúmenes de bloque en bruto.
- Determine qué política de SLA se asigna a los PVC. Para obtener instrucciones sobre la visualización de políticas de SLA disponibles, consulte [“Políticas de SLA” en la página 331](#).

## Procedimiento

1. Opcional: Visualice una lista de PVC en un espacio de nombres especificado emitiendo el siguiente mandato:

```
kubectl get pvc -n espacio_nombres --show-labels
```

En la lista de PVC, identifique la etiqueta adjunta a los PVC a los que desea hacer copia de seguridad.

2. Cree un archivo YAML que defina la solicitud para la operación de copia de seguridad por etiqueta. El archivo YAML debe contener las propiedades siguientes:

```
#-----  
# Filename: filename.yaml  
#-----  
  
apiVersion: "baas.io/v1alpha1"  
kind: BaaSReq  
  
metadata:  
  name: nombre_solicitud  
  namespace: espacio_nombres  
spec:  
  requesttype: BackupLabel  
  sla: [política_sla]
```

```
volumesnapshotclass: nombre_clase_instantánea
backuplabels:
- clave_etiqueta: valor
```

donde:

***nombre\_archivo***

Especifica el nombre del archivo de configuración de YAML. El tipo de archivo es `.yaml`.

***nombre\_solicitud***

Especifica el nombre de la solicitud de copia de seguridad por etiqueta. El nombre debe ser exclusivo y no debe coincidir con el nombre de PVC.

***espacio\_nombres***

Especifica el espacio de nombres para la solicitud de copia de seguridad

***[política\_sla]***

Especifica la política de SLA que determina la planificación para las operaciones de copia de seguridad. Puede especificar más de una política de SLA utilizando una lista separada por comas entre corchetes.

Por ejemplo, para asignar la política `daily` a una PVC, especifique la siguiente sentencia:

```
sla: [daily]
```

Para asignar las políticas `every4hours`, `daily_midnight` y `weekly` a PVC, especifique la siguiente sentencia en el archivo YAML:

```
sla: [every4hours,daily_midnight,weekly]
```

De forma alternativa, puede utilizar el formato siguiente para especificar una única política de SLA:

```
sla:
- daily
```

O, puede utilizar el siguiente formato para especificar varias políticas de SLA:

```
sla:
- every4hours
- daily_midnight
- weekly
```

Asegúrese de que utiliza el caso correcto cuando especifica el nombre de política de SLA. Los nombres de política distinguen entre mayúsculas y minúsculas en los archivos YAML.

Para eliminar todas las asignaciones de SLA de una etiqueta, suprima los nombres de política de SLA entre corchetes, como se muestra en la siguiente sentencia:

```
sla: []
```

***nombre\_clase\_instantánea***

Especifica la clase de instantánea para el volumen. Si no especifica la clase de instantánea, se utiliza la clase de instantánea predeterminada si el contenedor de sidecar `csi-snapshotter` de la clase de instantánea predeterminada coincide con el suministrador del volumen. De lo contrario, la solicitud de copia de seguridad no es válida.

***clave\_etiqueta: valor***

Especifica el par clave-valor para la etiqueta adjunta a los PVC a los que desea hacer copia de seguridad. Puede especificar más de una etiqueta.

Después de asignar una política de SLA en el nivel de etiqueta, los PVC nuevos que crea con esa etiqueta se asignarán automáticamente al SLA.

Por ejemplo, para hacer copia de seguridad de todos los PVC asociados con la etiqueta `color: red` y la etiqueta `department: sales`, especifique las siguientes sentencias:

```
backuplabels:  
- color: red  
- department: sales
```

### Restricciones:

- Las etiquetas de PVC son pares de valor clave. Las claves duplicadas con valores diferentes se sobrescriben con el último par de clave-valor.
- La operación de copia de seguridad por etiqueta se aplica a todos los PVC que tienen una etiqueta específica en el clúster. Si alguno de los PVC a los que ha realizado copia de seguridad pertenece a un espacio de nombres al que no tiene acceso, no podrá restaurar esos PVC utilizando la línea de mandatos. Sin embargo, los PVC se pueden restaurar mediante la interfaz de usuario de IBM Spectrum Protect Plus, independientemente del espacio de nombres al que pertenezca. Para obtener más información, consulte [“Restauración de datos de contenedor” en la página 341](#).

3. Envíe la solicitud de copia de seguridad emitiendo el siguiente mandato:

```
kubectl create -f filename.yaml
```

donde *filename* es el nombre del archivo de configuración de YAML.

### Resultados

Después de enviar la solicitud de copia de seguridad, la primera operación de copia de seguridad planificada se iniciará en la ventana definida por la política de SLA. La hora de inicio de la copia de seguridad se registra en el estado de copia de seguridad.

### Qué hacer a continuación

Para ver información sobre la solicitud de copia de seguridad, emita el mandato **kubectl describe** utilizando el nombre de solicitud. Por ejemplo, para ver información sobre una solicitud de copia de seguridad denominada `backup-red-label` en el espacio de nombres `baas`, emita el mandato siguiente:

```
kubectl describe baasreq backup-red-label -n baas
```

Para obtener instrucciones, consulte [“Visualización del estado de los trabajos de copia de seguridad y restauración” en la página 363](#).

### Modificación de parámetros en un archivo YAML:

Una vez que se han iniciado los trabajos de copia de seguridad por etiqueta planificada, puede modificar el parámetro de SLA en el archivo YAML y aplicarlo a la misma etiqueta si es necesario. Por ejemplo:

- Para asignar una política de SLA diferente a la etiqueta o eliminar una asignación de SLA, edite los valores del campo **sla** en el archivo YAML. A continuación, aplique el archivo YAML utilizando la interfaz de línea de mandatos **kubectl**.
- Si ya no desea que los PVC asociados con la etiqueta participen en trabajos de copia de seguridad planificada, elimine las asignaciones de política de SLA actualizando el campo **sla** en el archivo YAML. Para eliminar la etiqueta de todos los SLA, modifique el campo **sla** de la siguiente manera:

```
sla: []
```

A continuación, aplique el archivo YAML utilizando la interfaz de línea de mandatos **kubectl**.

- Si desea modificar cualquier otro parámetro, debe crear una solicitud nueva y especificar un nombre de solicitud diferente (*nombre\_solicitud*) en el archivo YAML.

### Conceptos relacionados

[“Tipos de copia de seguridad y restauración” en la página 330](#)

Soporte de copia de seguridad de Kubernetes proporciona varios tipos de funciones de copia de seguridad y restauración. Puede utilizar la interfaz de usuario de IBM Spectrum Protect Plus o la línea de mandatos de Kubernetes para iniciar las operaciones de copia de seguridad y restauración.

#### “Políticas de SLA” en la página 331

Las políticas de acuerdo de nivel de servicio (SLA) definen la frecuencia con la que se ejecutan las operaciones de copia de seguridad de copia y de copia de seguridad de instantánea y durante cuánto tiempo se retienen las copias de seguridad de copia y de instantánea. Puede configurar SLA personalizados que cumplan los requisitos operativos.

#### “Solicitudes de Soporte de copia de seguridad de Kubernetes” en la página 348

Para proteger los datos de contenedor, puede enviar solicitudes de Soporte de copia de seguridad de Kubernetes mediante la interfaz de línea de mandatos de Kubernetes.

#### “Resolución de problemas de Soporte de copia de seguridad de Kubernetes” en la página 550

Para ayudar a resolver problemas con Soporte de copia de seguridad de Kubernetes, puede recopilar archivos de registro de depuración y ver los registros de rastreo. También puede seguir procedimientos para diagnosticar problemas.

### **Copia de seguridad de volúmenes persistentes por espacio de nombres utilizando la línea de mandatos**

Puede crear solicitudes de copia de seguridad para volúmenes persistentes especificando un espacio de nombres. Un clúster físico se puede dividir en clústeres virtuales que se denominan espacios de nombres. Al especificar un espacio de nombres en una solicitud de copia de seguridad, puede realizar copia de seguridad de todos los PVC de dicho espacio de nombres

#### **Antes de empezar**

Las solicitudes de copia de seguridad están dirigidas a reclamaciones de volumen persistente (PVC) para los volúmenes que desea proteger. Antes de planificar un trabajo de copia de seguridad, realice las acciones siguientes:

- Asegúrese de que la PVC existe en el espacio de nombres especificado.
- Asegúrese de que la PVC esté formateado. Los PVC deben formatearse antes de que se pueda hacer una copia de seguridad de ellos. Para que una PVC tenga el formato correcto, debe estar montado y grabado. No se admiten las operaciones de copia de seguridad de volúmenes de bloque en bruto.
- Determine qué política de SLA se asigna a los PVC. Para obtener instrucciones sobre la visualización de políticas de SLA disponibles, consulte “Políticas de SLA” en la página 331.

#### **Procedimiento**

1. Opcional: Visualice la lista de los PVC del espacio de nombres a los que desee hacer copia de seguridad emitiendo el mandato siguiente:

```
kubectl get pvc -n namespace
```

2. Cree un archivo YAML que defina la solicitud para la operación de copia de seguridad por espacio de nombres. El archivo YAML debe contener las propiedades siguientes:

```
#-----  
# Filename: filename.yaml  
#-----  
  
apiVersion: "baas.io/v1alpha1"  
kind: BaaSReq  
  
metadata:  
  name: nombre_solicitud  
  namespace: espacio_nombres  
spec:  
  requesttype: BackupNamespace  
  sla: [politica_sla]  
  volumesnapshotclass: nombre_clase_instantanea
```

donde:

**nombre\_archivo**

Especifica el nombre del archivo de configuración de YAML. El tipo de archivo es `.yaml`.

**nombre\_solicitud**

Especifica el nombre de la solicitud de copia de seguridad por espacio de nombres. El nombre debe ser exclusivo y no debe coincidir con el nombre de PVC.

**espacio\_nombres**

Especifica el espacio de nombres al que desea asignar una política de acuerdo de nivel de servicio (SLA).

Después de asignar el SLA en el nivel de espacio de nombres, cualquier PVC que crea en ese espacio de nombres se asignará automáticamente al SLA.

**[política\_sla]**

Especifica la política de SLA que determina la planificación para las operaciones de copia de seguridad. Puede especificar más de una política de SLA utilizando una lista separada por comas entre corchetes.

Por ejemplo, para asignar la política `daily` a una PVC, especifique la siguiente sentencia:

```
sla: [daily]
```

Para asignar las políticas `every4hours`, `daily_midnight` y `weekly` a PVC, especifique la siguiente sentencia en el archivo YAML:

```
sla: [every4hours,daily_midnight,weekly]
```

De forma alternativa, puede utilizar el formato siguiente para especificar una única política de SLA:

```
sla:  
- daily
```

O, puede utilizar el siguiente formato para especificar varias políticas de SLA:

```
sla:  
- every4hours  
- daily_midnight  
- weekly
```

Asegúrese de que utiliza el caso correcto cuando especifica el nombre de política de SLA. Los nombres de política distinguen entre mayúsculas y minúsculas en los archivos YAML.

Para eliminar todas las asignaciones de SLA de un espacio de nombres, suprima los nombres de políticas de SLA entre corchetes, tal como se muestran en la siguiente sentencia:

```
sla: []
```

**nombre\_clase\_instantánea**

Especifica la clase de instantánea para el volumen. Si no especifica la clase de instantánea, se utiliza la clase de instantánea predeterminada si el contenedor de sidecar `csi-snapshotter` de la clase de instantánea predeterminada coincide con el proveedor del volumen. De lo contrario, la solicitud de copia de seguridad no es válida.

- Envíe la solicitud de copia de seguridad emitiendo el siguiente mandato:

```
kubectl create -f filename.yaml
```

donde *filename* es el nombre del archivo de configuración de YAML.

**Resultados**

Después de enviar la solicitud de copia de seguridad, la primera operación de copia de seguridad planificada se iniciará en la ventana definida por la política de SLA. La hora de inicio de la copia de seguridad se registra en el estado de copia de seguridad.

## Qué hacer a continuación

Para ver información sobre la solicitud de copia de seguridad, emita el mandato **kubectl describe** utilizando el nombre de solicitud. Por ejemplo, para ver información sobre una solicitud de copia de seguridad denominada backup-namespace1 en el espacio de nombres baas, emita el mandato siguiente:

```
kubectl describe baasreq backup-namespace1 -n baas
```

Para obtener instrucciones, consulte [“Visualización del estado de los trabajos de copia de seguridad y restauración”](#) en la página 363.

## Modificación de parámetros en un archivo YAML:

Una vez que se hayan iniciado los trabajos de copia de seguridad por espacio de nombres planificada, puede modificar los parámetros en el archivo YAML y aplicarlo al mismo espacio de nombres si es necesario. Por ejemplo:

- Para asignar una política de SLA distinta al espacio de nombres o eliminar una asignación de SLA, edite los valores del campo **sla** en el archivo YAML. A continuación, aplique el archivo YAML utilizando la interfaz de línea de mandatos **kubectl**.
- Si ya no desea que los PVC de un espacio de nombres participen en trabajos de copia de seguridad planificada, elimine las asignaciones de política de SLA actualizando el campo **sla** en el archivo YAML. Para eliminar el espacio de nombres de todos los SLA, modifique el campo **sla** de la siguiente manera:

```
sla: []
```

A continuación, aplique el archivo YAML utilizando la interfaz de línea de mandatos **kubectl**.

- Si desea modificar cualquier otro parámetro, debe crear una solicitud nueva y especificar un nombre de solicitud diferente (*nombre\_solicitud*) en el archivo YAML.

## Conceptos relacionados

[“Tipos de copia de seguridad y restauración”](#) en la página 330

Soporte de copia de seguridad de Kubernetes proporciona varios tipos de funciones de copia de seguridad y restauración. Puede utilizar la interfaz de usuario de IBM Spectrum Protect Plus o la línea de mandatos de Kubernetes para iniciar las operaciones de copia de seguridad y restauración.

[“Políticas de SLA”](#) en la página 331

Las políticas de acuerdo de nivel de servicio (SLA) definen la frecuencia con la que se ejecutan las operaciones de copia de seguridad de copia y de copia de seguridad de instantánea y durante cuánto tiempo se retienen las copias de seguridad de copia y de instantánea. Puede configurar SLA personalizados que cumplan los requisitos operativos.

[“Solicitudes de Soporte de copia de seguridad de Kubernetes”](#) en la página 348

Para proteger los datos de contenedor, puede enviar solicitudes de Soporte de copia de seguridad de Kubernetes mediante la interfaz de línea de mandatos de Kubernetes.

[“Resolución de problemas de Soporte de copia de seguridad de Kubernetes”](#) en la página 550

Para ayudar a resolver problemas con Soporte de copia de seguridad de Kubernetes, puede recopilar archivos de registro de depuración y ver los registros de rastreo. También puede seguir procedimientos para diagnosticar problemas.

## Restauración de datos de contenedor utilizando la línea de mandatos

Puede utilizar la interfaz de línea de mandatos de Kubernetes para restaurar un volumen persistente desde una copia de seguridad de instantánea o una copia de seguridad de copia. Una operación de restauración de instantánea suele ser más rápida que una operación de restauración de copia.

### Antes de empezar

Revise las restricciones siguientes:

- En cualquier tipo de operación de restauración, no puede restaurar un volumen en un nombre de espacios o clúster diferente.
- Puede restaurar una copia de seguridad de instantánea o de copia solo en un volumen persistente nuevo. La reclamación de volumen persistente (PVC) para el nuevo volumen se crea automáticamente cuando restaura una copia de seguridad de instantánea o de copia.
- Para asegurarse de que una solicitud de restauración funciona correctamente, no suprima manualmente instantáneas de volúmenes protegidos por Soporte de copia de seguridad de Kubernetes.

### Acerca de esta tarea

En función del objetivo de tiempo de recuperación y del objetivo de punto de recuperación, puede ejecutar una operación de restauración rápida o una operación de restauración de copia:

- Para restaurar un volumen en el menor tiempo posible, ejecute una operación de restauración rápida para restaurar una instantánea. Si hay otra operación en curso en el mismo volumen, la operación de restauración rápida puede tardar más tiempo en completarse.
- Para restaurar un volumen desde un punto específico en el tiempo desde el servidor vSnap de IBM Spectrum Protect Plus, ejecute una operación de restauración de copia.

### Procedimiento

1. Para ver los puntos de restauración que están disponibles para una PVC, consulte todas las copias de seguridad de la PVC ejecutando el siguiente mandato:

```
kubectl describe BaaSReq pvc_name -n namespace
```

Los puntos de restauración se identifican a través de la indicación de fecha y hora de la copia de seguridad de instantánea o de copia.

2. En la salida de estado que se visualiza, identifique la indicación de fecha y hora de la copia de seguridad de instantánea y de copia que desea restaurar. Las indicaciones de fecha y hora se muestran en la sección Estado de la salida antes del tipo de copia de seguridad.

Por ejemplo, la salida siguiente muestra las indicaciones de fecha y hora para los diferentes tipos de copias de seguridad:

```
Status:
Timestamp: 2019-05-30 13:27:21
Type:      FAST
Timestamp: 2019-05-30 13:32:21
Type:      COPY
```

donde:

#### RÁPIDO

Denota el tipo de copia de seguridad para la instantánea que se hace durante la operación de copia de seguridad de instantánea.

#### COPIA

Denota el tipo de copia de seguridad para una copia de seguridad de copia que se almacena en un servidor vSnap de IBM Spectrum Protect Plus.

3. Para especificar la solicitud de restauración, cree un archivo YAML con las propiedades siguientes. Inserte la indicación de fecha y hora para la instantánea de origen en el parámetro **restorepoint**.

```
#-----
# Filename: filename.yaml
#-----

apiVersion: "baas.io/v1alpha1"
kind: BaaSReq

metadata:
  name: nombre_solicitud_restauración
  namespace: espacio_nombres
```

```
spec:
  requesttype: restore
  pvcname: nombre_pvc
  targetvolume: volumen_destino_para_restauración
  storageclass: clase_almacenamiento_de_volumen_destino
  restorepoint: indicación_fecha_hora_de_copia_seguridad
  restoretype: fast | copy
```

donde:

***nombre\_archivo***

Especifica el nombre del archivo de configuración de YAML.

***nombre\_solicitud\_restauración***

Especifica el nombre de la solicitud para el trabajo de restauración. El nombre debe ser exclusivo y no debe coincidir con el nombre de la PVC.

Se debe crear una nueva solicitud de restauración para cada restauración posterior de la misma PVC. En otras palabras, para restaurar una PVC de nuevo, cree una nueva solicitud y especifique un nombre de solicitud diferente (*nombre\_solicitud*) en el archivo YAML.

***espacio\_nombres***

Especifica el espacio de nombres para la solicitud.

***nombre\_pvc***

Especifica el nombre de la PVC que desea restaurar.

***volumen\_destino\_para\_restauración***

Especifica el nombre de la PVC donde desea restaurar el volumen.

En las restauraciones rápidas o restauraciones de copia, el volumen siempre se restaura en una PVC nueva. En este caso, proporcione el nombre de la nueva PVC.

***clase\_almacenamiento\_de\_volumen\_destino***

Especifica la clase de almacenamiento definida para el volumen de destino.

En las operaciones de restauración rápida, se ignora la clase de almacenamiento. Se utiliza la clase de almacenamiento de la PVC original.

En las operaciones de restauración de copia, puede especificar una clase de almacenamiento que sea la misma que la PVC original o especificar una clase de almacenamiento diferente. Si no especifica la clase de almacenamiento, se utiliza la clase de almacenamiento de la PVC original.

Si especifica una clase de almacenamiento pero no especifica el tipo de restauración con el parámetro **restoretype**, se produce una operación de restauración de copia.

***indicación\_fecha\_hora\_de\_copia\_seguridad***

Especifica la indicación de fecha y hora de la copia de seguridad de copia o de instantánea de origen desde la que desea restaurar. La indicación de fecha y hora está en formato UTC (Hora universal coordinada).

Si no especifica una indicación de fecha y hora, se restaura la copia de seguridad de instantánea o de copia más reciente.

***restoretype: fast | copy***

Especifica el tipo de operación de restauración que se va a utilizar.

***rápida***

Restaura un volumen desde una copia de seguridad de instantánea.

***reserva***

Restaura un volumen desde una copia de seguridad de copia.

Este parámetro es opcional. Si no especifica un tipo de restauración, el tipo de restauración se determina automáticamente. Si existe una instantánea en la indicación de fecha y hora especificada, se ejecuta una restauración rápida para restaurar la instantánea. Si solo hay disponible una copia de seguridad de copia en el momento especificado, se ejecuta una restauración de copia para restaurar la copia de seguridad de copia.

4. Inicie la solicitud de restauración emitiendo el mandato siguiente:



```
kubectl create -f filename.yaml
```

donde *filename* es el nombre del archivo de configuración de YAML.

### Qué hacer a continuación

Si ha restaurado los datos en un volumen persistente nuevo, vuelva a configurar el contenedor de aplicaciones para montar el nuevo volumen después de que se restaure la copia de seguridad de instantánea o de copia.

Para gestionar de forma más eficaz las solicitudes de Soporte de copia de seguridad de Kubernetes, suprima las solicitudes completadas emitiendo el mandato siguiente:

```
kubectl delete baasreq nombre_solicitud_restauración -n espacio_nombres
```

Al suprimir las solicitudes completadas, obtendrá las ventajas siguientes:

- El tamaño de la base de datos etcd se reduce y puede volver a utilizar el nombre de una solicitud para otra operación.
- Se simplifica el proceso de resolución de problemas.
- Se simplifica el seguimiento de solicitudes de copia de seguridad y de restauración. En cualquier momento, puede obtener una lista precisa de solicitudes que se están ejecutando en el clúster cuando emite el siguiente mandato:

```
kubectl get baasreq -n namespace
```

### Conceptos relacionados

[“Tipos de copia de seguridad y restauración” en la página 330](#)

Soporte de copia de seguridad de Kubernetes proporciona varios tipos de funciones de copia de seguridad y restauración. Puede utilizar la interfaz de usuario de IBM Spectrum Protect Plus o la línea de mandatos de Kubernetes para iniciar las operaciones de copia de seguridad y restauración.

[“Solicitudes de Soporte de copia de seguridad de Kubernetes” en la página 348](#)

Para proteger los datos de contenedor, puede enviar solicitudes de Soporte de copia de seguridad de Kubernetes mediante la interfaz de línea de mandatos de Kubernetes.

[“Resolución de problemas de Soporte de copia de seguridad de Kubernetes” en la página 550](#)

Para ayudar a resolver problemas con Soporte de copia de seguridad de Kubernetes, puede recopilar archivos de registro de depuración y ver los registros de rastreo. También puede seguir procedimientos para diagnosticar problemas.

### Tareas relacionadas

[“Visualización del estado de los trabajos de copia de seguridad y restauración” en la página 363](#)

Después de enviar una solicitud de copia de seguridad o restauración, puede utilizar los mandatos **kubectl get** y **kubectl describe** para mostrar información sobre la solicitud.

## Gestión de trabajos de copia de seguridad y restauración de contenedor

Puede consultar la información sobre los trabajos de copia de seguridad y restauración, y suprimir las copias de seguridad de copia y de instantánea que ya no necesita.

### Visualización del estado de los trabajos de copia de seguridad y restauración

Después de enviar una solicitud de copia de seguridad o restauración, puede utilizar los mandatos **kubectl get** y **kubectl describe** para mostrar información sobre la solicitud.

### Procedimiento

1. Para mostrar un listado de todas las solicitudes de Soporte de copia de seguridad de Kubernetes en un espacio de nombres, emita el mandato **kubectl get** de la siguiente manera:

```
kubectl get baasreq -n espacio_nombres
```

Por ejemplo, para mostrar todas las solicitudes en el espacio de nombres `production-01`, emita el siguiente mandato:

```
kubectl get baasreq -n production-01
```

La salida es similar a la que se muestra en el ejemplo siguiente:

NAME	AGE
vol08-adhoc	17d
inv-adhoc2	17d
db-vol08	18d
db-vol09	17d

Los nombres de solicitud se listan en la columna `NAME` de la salida.

2. Utilizando los resultados del Paso “1” en la [página 363](#), emita el mandato **kubectl describe** para mostrar el estado de un trabajo. Por ejemplo:

- Para mostrar la lista de todas las copias de seguridad para cualquier solicitud, incluidas las copias de seguridad de solicitudes de copia de seguridad planificadas y bajo demanda, especifique el nombre de la solicitud y el espacio de nombres en el siguiente mandato:

```
kubectl describe baasreq nombre_solicitud -n espacio_nombres
```

donde *nombre\_solicitud* es el nombre de la solicitud. Para copias de seguridad bajo demanda, utilice el nombre de PVC como el nombre de solicitud.

Por ejemplo, para mostrar todas las copias de seguridad para PVC `db-vol08` en el espacio de nombres `production-01`, emita el siguiente mandato:

```
kubectl describe baasreq db-vol08 -n production-01
```

La salida es similar a la que se muestra en el ejemplo siguiente:

```
kubectl describe baasreq db-vol08 -n production-01
Name:          db-vol08
Namespace:     production-01
Labels:        <none>
Annotations:   <none>
API Version:   baas.io/v1alpha1
Backupstatus:  Ready
Kind:          BaaSReq
Metadata:
  CreationTimestamp:  2020-05-20T20:28:33Z
  Generation:         9
  Resource Version:   2955966
  Self Link:          /apis/baas.io/v1alpha1/namespaces/production-01/baasreqs/db-vol08
  UID:                0e8d4412-522f-44b3-932c-1e6239f7bf8e
Spec:
  Inprogress:    None
  Instanceid:    e05c400868ab9151e3c792d28edfbb18
  Origreqtype:   backup
  Requesttype:   backup
  Size:          1073741824
  Sla:
    joanne-copy2
  Spppvcname:    cluster01:production-01:db-vol08
  Volumesnapshotclass:  cirrus-csi-rbdplugin-snapclass
Status:
  Snapshotname:   spp-1005-2161-172342eb32d
  Timestamp:      2020-05-20 22:24:25
  Type:           FAST
  Snapshotname:   2000.snapshot.824
  Timestamp:      2020-05-20 21:13:27
  Type:           COPY
  Snapshotname:   spp-1005-2161-17233c4e7a0
  Timestamp:      2020-05-20 20:28:14
  Type:           FAST
```

- Para mostrar información sobre un trabajo de restauración, emita el mandato siguiente:

```
kubectl describe baasreq nombre_solicitud -n espacio_nombres
```

donde *nombre\_solicitud* es el nombre de solicitud del trabajo de restauración y *espacio\_nombres* es el espacio de nombres de la PVC que se ha restaurado.

## Resultados

En la salida del mandato, el campo **Backupstatus** muestra el estado de un trabajo de copia de seguridad. Para los trabajos de restauración, el campo **Restorestatus** muestra el estado del trabajo de restauración. Para obtener más información, consulte el apartado [“Estado de los trabajos de copia de seguridad y restauración”](#) en la página 365.

El campo **instanceid** contiene una serie generada aleatoriamente que identifica de forma exclusiva un volumen en IBM Spectrum Protect Plus.

El campo **Spppvname** muestra el nombre de la PVC que se notifica en la ventana de IBM Spectrum Protect Plus **Trabajos y operaciones**. El formato *espacio\_nombres:nombre\_pvc* se utiliza para identificar la PVC. Los valores para los campos **instanceid** y **Spppvname** identifica de manera exclusiva una copia de seguridad en IBM Spectrum Protect Plus.

En las solicitudes de copia de seguridad, la sección **Estado** muestra la lista de copias de seguridad que se han completado. Para cada copia de seguridad, se lista la indicación de fecha y hora de la copia de seguridad, seguida del tipo de copia de seguridad que se ha ejecutado. Los tipos de copias de seguridad se definen de la siguiente manera:

### RÁPIDO

Denota el tipo de copia de seguridad para la instantánea que se hace durante la operación de copia de seguridad de instantánea.

### COPIA

Denota el tipo de copia de seguridad para una copia de seguridad de copia que se almacena en un servidor vSnap de IBM Spectrum Protect Plus.

### Estado de los trabajos de copia de seguridad y restauración

Cuando utiliza el mandato **kubectl describe** para mostrar información sobre los trabajos de copia de seguridad y restauración, el estado de los trabajos de copia de seguridad y restauración se muestra en la salida del mandato .

Para visualizar el estado de una solicitud de Soporte de copia de seguridad de Kubernetes específica, escriba el mandato siguiente:

```
kubectl describe baasreq nombre_solicitud -n espacio_nombres
```

donde *nombre\_solicitud* es el nombre de la solicitud y *espacio\_nombres* es el espacio de nombres en el que existe el volumen persistente. Para obtener más información, consulte el apartado [“Visualización del estado de los trabajos de copia de seguridad y restauración”](#) en la página 363.

### Estado de copia de seguridad notificado

El estado de un trabajo de copia de seguridad se muestra en el campo Backupstatus en la salida del mandato. La tabla siguiente muestra los estados posibles de una solicitud de copia de seguridad:

Tabla 60. Estado de los trabajos de copia de seguridad	
Estado de copia de seguridad	Descripción
<b>Ninguno</b>	No se han iniciado trabajos de copia de seguridad para esta planificación.
<b>Solicitado</b>	Se ha iniciado un trabajo de copia de seguridad para esta planificación.

Tabla 60. Estado de los trabajos de copia de seguridad (continuación)

Estado de copia de seguridad	Descripción
<b>Listo</b>	Se ha completado al menos un trabajo de copia de seguridad para esta planificación.
<b>Destruído</b>	Se han suprimido todas las copias de seguridad de copia y de instantánea de una reclamación de volumen persistente.
<b>No válido</b>	Se ha producido un problema con la solicitud. Se muestra una explicación posible en el campo <b>Errmsg</b> .

### Estado de restauración notificado

El estado de un trabajo de restauración se muestra en el campo **Restoestatus** en la salida del mandato. La tabla siguiente muestra los estados posibles de un trabajo de restauración:

Tabla 61. Estado de los trabajos de restauración

Estado de restauración	Descripción
<b>Ninguno</b>	No se han solicitado trabajos de restauración.
<b>Solicitado</b>	Se solicita un trabajo de restauración de copia de seguridad de copia o de instantánea.
<b>Restaurado</b>	Se ha restaurado correctamente una copia de seguridad de copia o de instantánea.
<b>No válido</b>	Se ha producido un problema con la solicitud. Se muestra una explicación posible en el campo <b>Errmsg</b> .

### Supresión de copias de seguridad de contenedor

Puede marcar para eliminación las copias de seguridad de instantánea y de copia de una reclamación de volumen persistente (PVC) enviando una solicitud **destroy**.

### Antes de empezar

Antes de enviar una solicitud **destroy** para suprimir copias de seguridad de contenedor, tenga en cuenta las siguientes consecuencias:

- Se suprimen todas las instantáneas de PVC cuando se alcanzan sus fechas de caducidad tal como define la política de acuerdo de nivel de servicio (SLA) para la PVC.
- Las copias de seguridad de instantánea y de copia en el servidor vSnap de IBM Spectrum Protect Plus se marcarán para supresión. IBM Spectrum Protect Plus gestiona la supresión.
- La solicitud de copia de seguridad original no se suprimirá mediante la solicitud **destroy**. Debe ejecutar el mandato **kubect1 delete** para suprimirlo.
- La solicitud **destroy** no se admite para copias de seguridad bajo demanda. Utilice el mandato **kubect1 delete** para suprimir una solicitud de copia de seguridad bajo demanda. Se suprime una instantánea bajo demanda cuando caduca la instantánea o cuando se destruye la copia de seguridad planificada.

### Procedimiento

1. Cree un archivo YAML para la solicitud **destroy** que contiene las propiedades siguientes:

```
#-----
# Filename: filename.yaml
```

```
#-----
apiVersion: "baas.io/v1alpha1"
kind: BaaSReq

metadata:
  name: request_name
  namespace: espacio_nombres
spec:
  requesttype: Destroy
```

donde:

**nombre\_archivo**

El nombre del archivo de configuración de YAML.

**nombre\_solicitud**

El nombre de la solicitud, que debe coincidir con el nombre de la PVC de la que se ha hecho copia de seguridad. Por ejemplo, si desea suprimir todas las copias de seguridad de instantáneas y copia para la PVC llamada db-vo101, el nombre de la solicitud también debe ser db-vo101.

**espacio\_nombres**

El espacio de nombres en el que existe la PVC.

- Envíe la solicitud **destroy** especificando el mandato siguiente en la línea de mandatos:

```
kubectl apply -f filename.yaml
```

donde *filename* es el nombre del archivo de configuración de YAML.

- Para comprobar que se suprimen las copias de seguridad de instantáneas y de copia para una PVC, emita el siguiente mandato:

```
kubectl describe baasreq request_name -n namespace | grep Backupstatus
```

donde *request\_name* es el nombre de la PVC de la que se ha hecho copia de seguridad.

En la salida del mandato, el siguiente estado muestra que se han suprimido las copias de seguridad:

```
Backupstatus: Destroyed
```

## Qué hacer a continuación

Como práctica recomendada, suprima la solicitud completada emitiendo el siguiente mandato:

```
kubectl delete baasreq request_name -n namespace
```

donde *request\_name* es el nombre de la PVC de la que se ha hecho copia de seguridad.

Al suprimir las solicitudes completadas, obtendrá las ventajas siguientes:

- El tamaño de la base de datos etcd se reduce y puede volver a utilizar el nombre de una solicitud para otra operación.
- Se simplifica el proceso de resolución de problemas.
- Se simplifica el seguimiento de solicitudes de copia de seguridad y de restauración. En cualquier momento, puede obtener una lista precisa de solicitudes que se están ejecutando en el clúster cuando emite el siguiente mandato:

```
kubectl get baasreq -n namespace
```

Si suprime la solicitud de copia de seguridad sin destruir primero la copia de seguridad, la solicitud de copia de seguridad continuará ejecutándose y las copias de seguridad se realizarán según la política de SLA especificada hasta que se reinicie Soporte de copia de seguridad de Kubernetes.

## Información relacionada

[“Tipos de solicitudes en Soporte de copia de seguridad de Kubernetes” en la página 348](#)



## Capítulo 13. Protección de datos en sistemas en nube

Los sistemas en nube como Microsoft Office 365 se pueden registrar con IBM Spectrum Protect Plus para que pueda comenzar a proteger los datos. Registre Office 365 con IBM Spectrum Protect Plus para poder configurar los trabajos de copia de seguridad o las políticas de acuerdo de nivel de servicio (SLA) planificadas regularmente.

Si decide proteger Microsoft Office 365 con IBM Spectrum Protect Plus, necesita comprar IBM Spectrum Protect Plus for Microsoft Office 365 Entity ID Monthly License, Part Number D25ZELL. Para obtener más información sobre esta titularidad, consulte la carta de anuncio de [IBM Spectrum Protect Plus V10.1.5](#).

### Microsoft Office 365

Para proteger el correo electrónico, los calendarios, contactos y datos de Microsoft Office 365 en el almacenamiento en la nube de OneDrive, primero debe registrarse en la aplicación Office 365 con Azure Active Directory. A continuación, despliegue el servidor de aplicaciones y regístrelo con IBM Spectrum Protect Plus. Después de eso, debe añadir los arrendatarios de Office 365 y definir una política de acuerdo de nivel de servicio (SLA) para crear trabajos de copia de seguridad.

Puede utilizar IBM Spectrum Protect Plus para registrar y probar datos de Office 365 en un entorno no productivo. Si decide proteger Microsoft Office 365 en un entorno productivo con IBM Spectrum Protect Plus, necesita adquirir IBM Spectrum Protect Plus for Microsoft Office 365 Entity ID Monthly License, Part Number D25ZELL. Para obtener más información sobre esta titularidad, consulte la carta de anuncio de [IBM Spectrum Protect Plus V10.1.5](#). Tenga en cuenta que se trata de un enlace externo.

### Registro con Azure Active Directory

Para proteger una aplicación de Office 365, debe registrar la aplicación con Azure Active Directory y otorgar los permisos adecuados. Cuando registra una aplicación nueva con Azure Active Directory, las credenciales de aplicación, como el ID de aplicación y el secreto de aplicación están disponibles en el portal de Azure Active Directory.

#### Antes de empezar

Realice las acciones siguientes:

- Asegúrese de que tiene una suscripción a Office 365 activa.
- Asegúrese de tener un ID de usuario de administración y una contraseña de Office 365.

#### Procedimiento

1. Vaya a la página de bienvenida de Office 365 e inicie sesión en su cuenta de Microsoft utilizando el ID de usuario de administración y la contraseña de Office 365.
2. Para abrir el centro de administración de Azure Active Directory, en el panel izquierdo, haga clic en los puntos suspensivos para expandir el menú **Mostrar todo** y, a continuación, haga clic en **Centros de administración > Azure Active Directory**.
3. Para abrir el panel de instrumentos de arrendatario, en el panel izquierdo del centro de administración de Azure Active Directory, haga clic en **Azure Active Directory**.
4. En el menú del panel de instrumentos de arrendatario, haga clic en **Registros de aplicación** y, a continuación, haga clic en **Nuevo registro**.
5. Para especificar un nombre para el usuario para la aplicación Office 365, en la página "Registrar una aplicación", escriba un nombre en el campo **Nombre**.
6. Utilice las opciones predeterminadas para los campos restantes y pulse **Registrar**. El registro de la aplicación se configura con el nombre de usuario que ha especificado.
7. Para obtener la serie del ID de aplicación (cliente) y el ID de directorio (arrendatario), haga clic en **Azure Active Directory > arrendatario: registros de la aplicación > Nombre de aplicación**. A

continuación, copie la serie ID de aplicación e ID de directorio. Estas series serán necesarias más tarde, cuando registra la aplicación Office 365 con IBM Spectrum Protect Plus.

8. Para crear un secreto de cliente para este ID de aplicación, haga clic en **Certificados y secretos > Nuevo secreto de cliente**.
9. En el panel "Añadir un secreto cliente", especifique cualquier nombre de usuario en el campo **Descripción** y haga clic en **Añadir**. Se genera un secreto de cliente y el valor se visualiza en el panel Secretos de cliente.
10. Copie el secreto de cliente en el portapapeles utilizando el recurso de copia junto al campo **Valor del secreto de cliente**. Esta serie de caracteres también se utiliza para el registro con IBM Spectrum Protect Plus.
11. Para añadir permisos para este ID de aplicación, haga clic en **Permisos de API > Añadir permisos**.
12. Especifique permisos para cada API en la tabla siguiente realizando las siguientes acciones. Seleccione el nombre de API, por ejemplo, Azure Active Directory Graph.
  - a) En el nombre de permiso User.Read.All, seleccione el tipo **Permisos delegados**.
  - b) En los permisos restantes, seleccione el tipo **Permisos de aplicación** para cada uno de los nombres de permiso para la API de la tabla.

API	Nombre de permiso
Azure Active Directory Graph	User.Read.All
Azure Active Directory Graph	Directory.Read.All
Exchange	full_access_as_app
Microsoft Graph	calendars.ReadWrite
Microsoft Graph	Contacts.ReadWrite
Microsoft Graph	Files.ReadWrite.All
Microsoft Graph	Mail.ReadWrite
Microsoft Graph	Sites.Read.All
Microsoft Graph	User.Read
Microsoft Graph	User.Read.all

13. Para guardar los permisos seleccionados, haga clic en **Otorgar consentimiento de administrador para <nombre de su organización>**.

#### Qué hacer a continuación

Siga las instrucciones que se indican en [“Registro del arrendatario de Office 365 con IBM Spectrum Protect Plus”](#) en la página 370.

## Registro del arrendatario de Office 365 con IBM Spectrum Protect Plus

Para asegurarse de que el agente de IBM Spectrum Protect Plus puede conectarse al arrendatario de Office 365, debe registrar las credenciales de arrendatario de Office 365 y el servidor de host de proxy con IBM Spectrum Protect Plus. Este procedimiento es necesario para garantizar que se puede hacer copia de seguridad de los datos de Office 365 en IBM Spectrum Protect Plus.

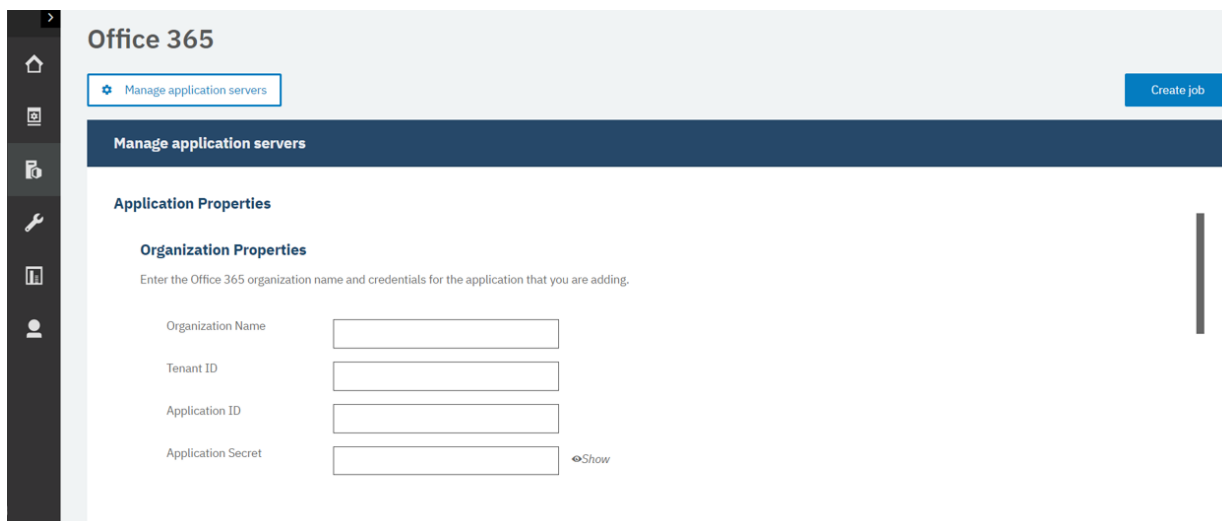
#### Antes de empezar

Asegúrese de que tiene un sistema Linux que pueda actuar como máquina proxy en la nube. IBM Spectrum Protect Plus despliega el agente de copia de seguridad en esta máquina. Para obtener más información sobre los requisitos, consulte [Requisitos de Office 365](#). Asegúrese de que la aplicación Office 365 esté registrada en Azure Active Directory. Para obtener instrucciones, consulte [“Registro con Azure Active Directory”](#) en la página 369.



## Procedimiento

1. En el panel de navegación, expanda **Gestionar protección > Cloud Management > Office 365**.



The screenshot shows the 'Office 365' interface. On the left is a dark sidebar with navigation icons. The top bar has 'Office 365' and a 'Manage application servers' tab. Below the top bar is a dark blue header with 'Manage application servers'. The main content area is titled 'Application Properties' and 'Organization Properties'. It contains a text prompt: 'Enter the Office 365 organization name and credentials for the application that you are adding.' Below this are four input fields: 'Organization Name', 'Tenant ID', 'Application ID', and 'Application Secret'. A 'Show' button is next to the 'Application Secret' field. A 'Create job' button is in the top right corner.

2. En la página de Office 365, haga clic en **Gestionar servidores de aplicaciones** y, a continuación, haga clic en **Añadir servidor de aplicaciones**.
3. En la página Propiedades de la organización, complete los campos siguientes:
  - a. En el campo **Nombre de la organización**, especifique el nombre de la organización que ha configurado en el centro de administración de Azure Active Directory.

**Nota:** Este es el nombre de la Organización/Arrendatario como *tenantname.onmicrosoft.com* y no se puede ver cuando está registrando la aplicación Azure.
  - b. En el campo **ID de arrendatario**, especifique la serie del campo **ID de directorio (arrendatario)** en el registro de la aplicación Azure Active Directory.
  - c. En el campo **ID de aplicación**, especifique la serie del campo **ID de aplicación (cliente)** en el registro de la aplicación Azure Active Directory.
  - d. En el campo **Secreto de aplicación**, especifique la serie de contraseña que se ha generado durante el registro de la aplicación Azure Active Directory.
4. En la página Propiedades de proxy, complete los campos siguientes:
  - a. En el campo **Direcciones de host**, especifique el nombre de host o IP del servidor Linux que se está utilizando como host de proxy.
  - b. Para la autenticación de servidor de host, seleccione una de las opciones siguientes:
    - **Usuario:** seleccione un usuario existente o escriba un ID de usuario y la contraseña asociada.
    - **Clave SSH:** seleccione una clave de Secure Shell (SSH) de la lista desplegable.
5. Pulse **Guardar**.

## Resultados

Cuando se registra un host de proxy en IBM Spectrum Protect Plus, se ejecuta automáticamente un inventario en la organización de Office 365, que devuelve los usuarios de Office 365 en dicho recurso.

## Registros de procesos detallados

El registro de procesos detallado es un archivo de registro de procesos de Microsoft O365 adicional que ayuda a la hora de resolver problemas. Este registro se recopila para realizar el seguimiento de todos los procesos de copia de seguridad y de restauración para ayudar a la resolución de problemas y a la realización del seguimiento

Un registro de procesos detallado realiza el seguimiento de los procesos para cada elemento de Office 365 protegido. Cuando descarga el archivo .zip del registro de trabajo, puede ver el archivo de registro de procesos detallado junto con los archivos de diagnóstico estándar.

**Nota:** Para encontrar el registro, descargue el archivo `joblog.zip`. Cuando descomprima los archivos `diag.tar.gz`, encontrará el archivo `Audit.log`. Este es el archivo con la información de proceso de Office 365.

### Contenido del registro de proceso detallado y ejemplo

Un archivo de registro de proceso detallado incluye la siguiente información:

- Fecha y hora de la operación.
- Tipo de operación.
- Cuenta asociada con la operación.
- Indicación de si el suceso está relacionado con OneDrive, un mensaje, un suceso o un contacto.
- Mensajes informativos:
  - Para OneDrive, se lista la vía de acceso y el nombre de archivo del objeto procesado. Si la operación es una operación de restauración redirigida, es decir, indicada.
  - Para mensajes, se lista la fecha y hora del mensaje. Si la operación es una operación de restauración redirigida, se listan todos los mensajes asociados.
  - Para sucesos, se lista el asunto del suceso.
  - Para contactos, se lista el nombre del contacto.

### Ejemplo de registro de proceso detallado

La información del registro de proceso detallado se proporciona en el formato siguiente:

```
[date time] [operation] [account] [relation] [message1] optional: [message2]
```

Por ejemplo,

```
2020-02-13 19:15:27.805 Backup Completed username@example.com OneDrive
"my_new_document.pdf"
2020-02-13 19:13:46.754 Backup Completed username@example.com Message "1/20/2020 10:52:01
PM +01:00" "Welcome!"
2020-02-13 19:16:14.196 Backup Completed username@example.com Contact "John Smith"
2020-02-13 19:14:48.847 Backup Completed username@example.com Event "Monday meeting"
2020-02-13 19:18:22.544 Backup Failed username@example.com OneDrive "my_folder
\inventory.pdf"
2020-02-13 19:15:27.805 Restore Completed username@example.com OneDrive
"my_new_document.pdf" "my_new_document_2020-02-11_19_15.pdf"
2020-02-13 19:22:28.238 Backup Failed username@example.com OneDrive "my_folder\inv
\inventory.pdf"
```

## Copia de seguridad de datos de Office 365

Después de que la organización de Office 365 se registra con IBM Spectrum Protect Plus, puede aplicar una política de acuerdo de nivel de servicio (SLA) para empezar a proteger los datos de Office 365.

### Procedimiento

1. En el panel de navegación de IBM Spectrum Protect Plus, expanda **Gestionar protección > Cloud Management > Office 365**.
2. Seleccione la casilla de verificación para la organización.
3. Pulse **Seleccionar una política de SLA** y elija una política de SLA.  
Para obtener más información sobre las políticas de SLA, consulte [“Crear políticas de copia de seguridad” en la página 169](#).
4. Guarde su selección. Para definir un nuevo SLA o editar una política existente con periodos de retención personalizados o tasas de frecuencia de copia de seguridad, haga clic en **Gestionar**

**protección > Descripción general de política.** En el panel "Políticas de SLA", pulse **Añadir política de SLA** y defina las preferencias de política.

**Nota:** Algunas opciones del campo **Opciones de política** en la sección **Estado de la política de SLA** difieren en la disponibilidad basada en el tipo de copia de seguridad.

5. Para ejecutar la política fuera del trabajo planificado, realice las acciones siguientes.
  - a. Para hacer copia de seguridad de todos los datos de organización, seleccione el casilla de verificación de la organización.
  - b. Para hacer copia de seguridad de una cuenta, haga clic en Organización y seleccione el casilla de verificación para el nombre de usuario asociado con la cuenta.
  - c. Para hacer copia de seguridad de correos electrónicos, calendarios, contactos o datos de OneDrive para una cuenta, haga clic en Organización y, a continuación, haga clic en el nombre de usuario y seleccione la casilla de verificación para el correo electrónico, calendario, contactos o OneDrive.
6. Pulse **Ejecutar**. El estado cambia a **En ejecución** para el SLA elegido y puede seguir el progreso del trabajo en el registro.

### **Copia de seguridad incremental para siempre para Office 365**

IBM Spectrum Protect Plus proporciona una estrategia de copia de seguridad denominada *incremental para siempre*. En lugar de planificar trabajos de copia de seguridad completa periódicos, esta solución de copia de seguridad requiere solo una copia de seguridad completa inicial. 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 objetos nuevos o 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 hace copia de seguridad de todos los datos de las cuentas de Office 365 seleccionadas.
2. Todos los trabajos de copia de seguridad posteriores solo hacen copia de seguridad de los datos nuevos o que han cambiado de las cuentas seleccionadas.

## **Restauración de datos de Office 365**

Puede restaurar datos de Office 365 desde copias de seguridad en servidores vSnap o almacenamiento remoto. Cuando esté preparado para restaurar un buzón en Office 365, puede completar la tarea en IBM Spectrum Protect Plus.

### **Antes de empezar**

Al menos un trabajo de copia de seguridad de Office 365 debe haberse ejecutado correctamente. Para obtener instrucciones sobre la configuración de un trabajo de copia de seguridad, consulte [“Copia de seguridad de datos de Office 365”](#) en la página 372.



### **Acerca de esta tarea**

Se admiten las siguientes modalidades de restauración:

- Restaurar datos en la cuenta original
- Restaurar datos en otra cuenta
- Restaurar datos en una vía de acceso especificada

### **Procedimiento**

1. En el panel de navegación, expanda **Gestionar protección > Cloud Management > Office 365**.

2. Pulse **Crear trabajo**.
3. Seleccione **Restaurar**.
4. En el panel **Seleccionar origen**, complete los pasos siguientes:
  - a) Haga clic en un origen de la lista para mostrar los datos que se pueden restaurar para la organización seleccionada. También puede utilizar la función de búsqueda para buscar datos disponibles y conmutar los datos visualizados utilizando el filtro **Ver**.
  - b) Para seleccionar los datos a restaurar, haga clic en el icono Añadir a la lista de restauración  junto a los datos. Es posible seleccionar varios elementos en la lista. Se añaden los elementos seleccionados a la lista de restauración. Para eliminar un elemento de la lista de origen, haga clic en el icono Eliminar de la lista de restauración  junto a los datos.
  - c) Pulse **Siguiente** para continuar.
5. En la página "Instantánea de origen", seleccione el tipo de restauración y la hora a la que se ha realizado la copia de seguridad de los datos que se van a restaurar. A continuación, pulse **Siguiente** para continuar.
6. En la página "Seleccionar destino", complete los siguientes campos y pulse **Siguiente** para continuar.

Opción	Descripción
<b>Seleccionar un destino</b>	<p>Seleccione la ubicación donde se deben restaurar los datos:</p> <p><b>Restaurar en la cuenta original</b> Restaura los datos en la cuenta de Office 365 original</p> <p><b>Restaurar en otra cuenta</b> Restaura los datos en otra cuenta de Office 365</p>
<b>Restaurar vía de acceso</b>	Restaura los datos en la vía de acceso de directorio seleccionada en la cuenta de Office 365

7. En la página **Opciones de trabajo**, si desea ejecutar operaciones de restauración en streams paralelos, especifique un valor en el campo **Máximo de streams paralelos**. A continuación, pulse **Siguiente** para continuar.
8. En la página Revisar, revise los valores del trabajo de restauración.
9. Para iniciar el trabajo de restauración, pulse **Enviar**.

## Resultados

Unos instantes después de que pulse **Enviar**, se añade el trabajo de restauración bajo demanda a la pestaña Trabajos en ejecución en la página Trabajos y operaciones. Puede pulsar el registro de trabajo para visualizar los detalles de la operación. También puede descargar el archivo de registro comprimido pulsando **Descargar.zip**.

Se puede encontrar el nombre de cuenta para los datos restaurados en el archivo de registro para la operación de restauración. Para localizar los registros para una operación de restauración, en el panel de navegación, haga clic en **Trabajos y operaciones** y, a continuación, en la pestaña **Trabajos en ejecución**.

---

## Capítulo 14. Protección de bases de datos

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.

**Restricción:** IBM Spectrum Protect Plus puede crear carpetas en servidores de aplicaciones cuando las aplicaciones están registradas con IBM Spectrum Protect Plus. Las carpetas creadas por IBM Spectrum Protect Plus deben permanecer para que el producto funcione correctamente. Sin embargo, si debe eliminar una carpeta creada por IBM Spectrum Protect Plus, anule el registro de la aplicación y IBM Spectrum Protect Plus borrará las carpetas asociadas con el registro.

No asigne más de una aplicación por máquina como servidor de aplicaciones a un grupo de recursos. Por ejemplo, si Microsoft SQL Server y Microsoft Exchange Server ocupan la misma máquina y ambos están registrados en IBM Spectrum Protect Plus, solo uno de ellos puede añadirse como servidor de aplicaciones a un determinado grupo de recursos.

### 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 62](#).

**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 378](#).

Se debe poder acceder a la dirección IP desde el servidor IBM Spectrum Protect Plus y desde el servidor vSnap. Ambos deben tener un servicio de gestión remota de Windows que esté a la escucha en el puerto 5985.

Se debe poder resolver y redirigir el nombre de dominio completo desde el servidor de dispositivo IBM Spectrum Protect Plus y desde el servidor vSnap.

### Requisitos previos para Db2

Se deben cumplir todos los requisitos previos para Servidor de aplicaciones de IBM Spectrum Protect Plus Db2 antes de empezar a proteger los recursos de Db2 con IBM Spectrum Protect Plus.

Los requisitos para Servidor de aplicaciones de IBM Spectrum Protect Plus Db2 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 378.
- 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.

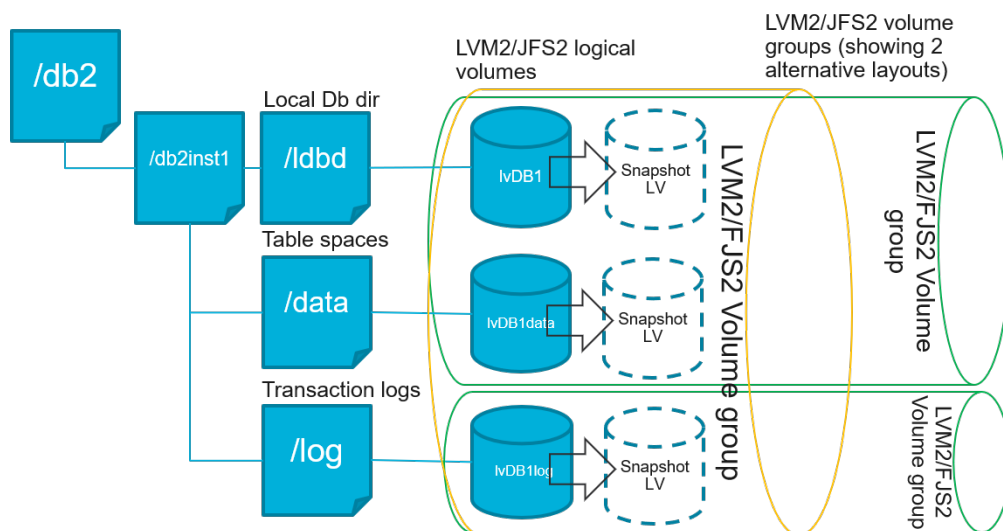


Figura 35. Ejemplos de diseño de volúmenes lógicos

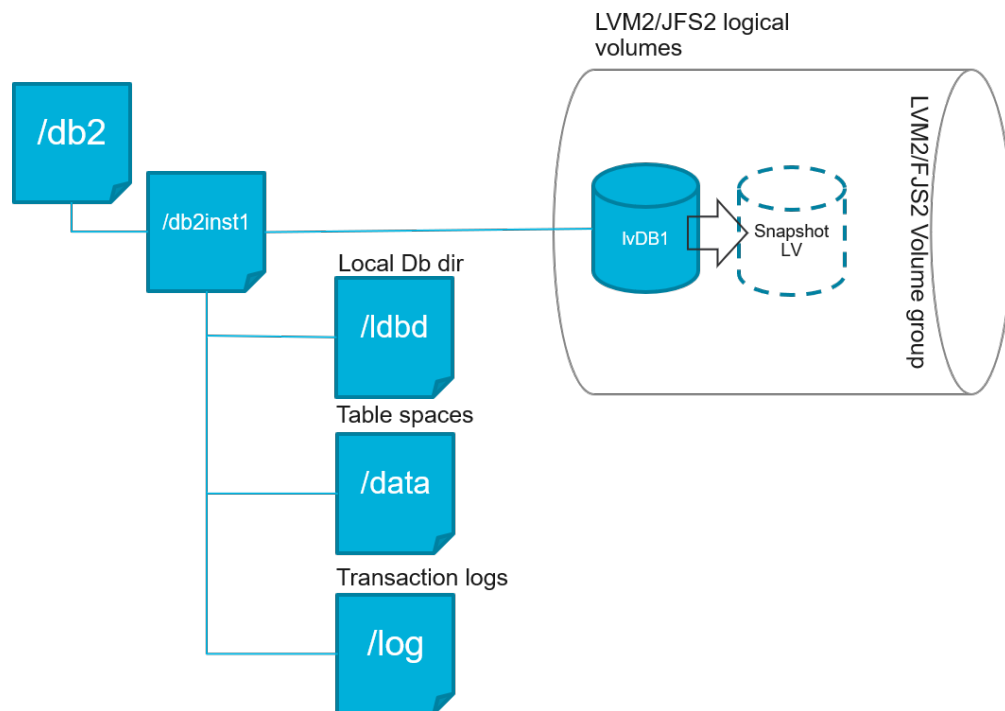


Figura 36. Ejemplo de diseño de volumen lógico único

- 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 37. 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.

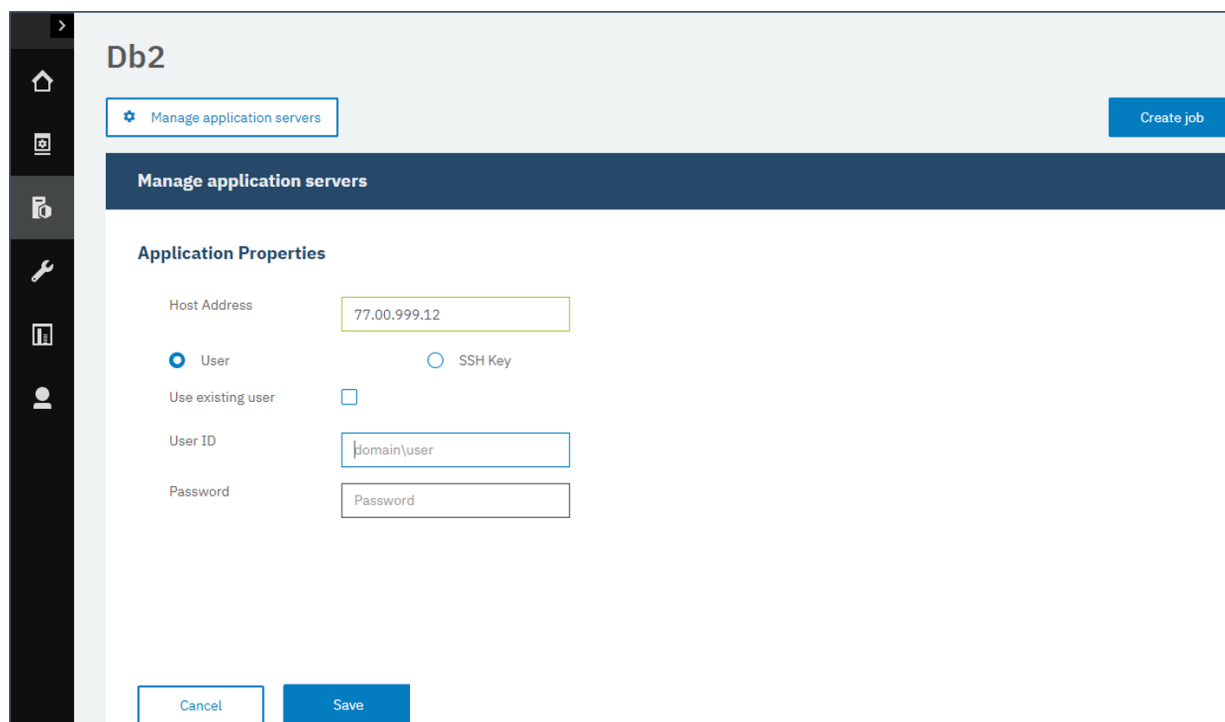


Figura 38. Gestión de usuarios agentes

### 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**.

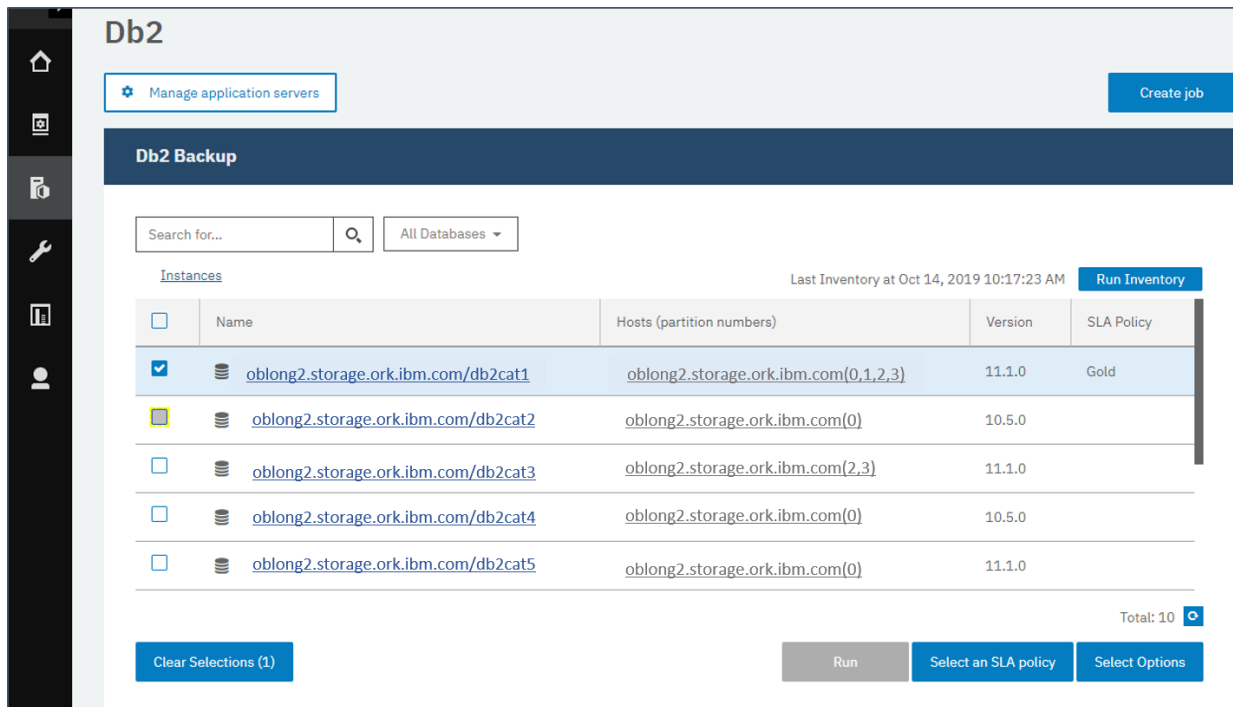


Figura 39. Detección de recursos de Db2

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](#).

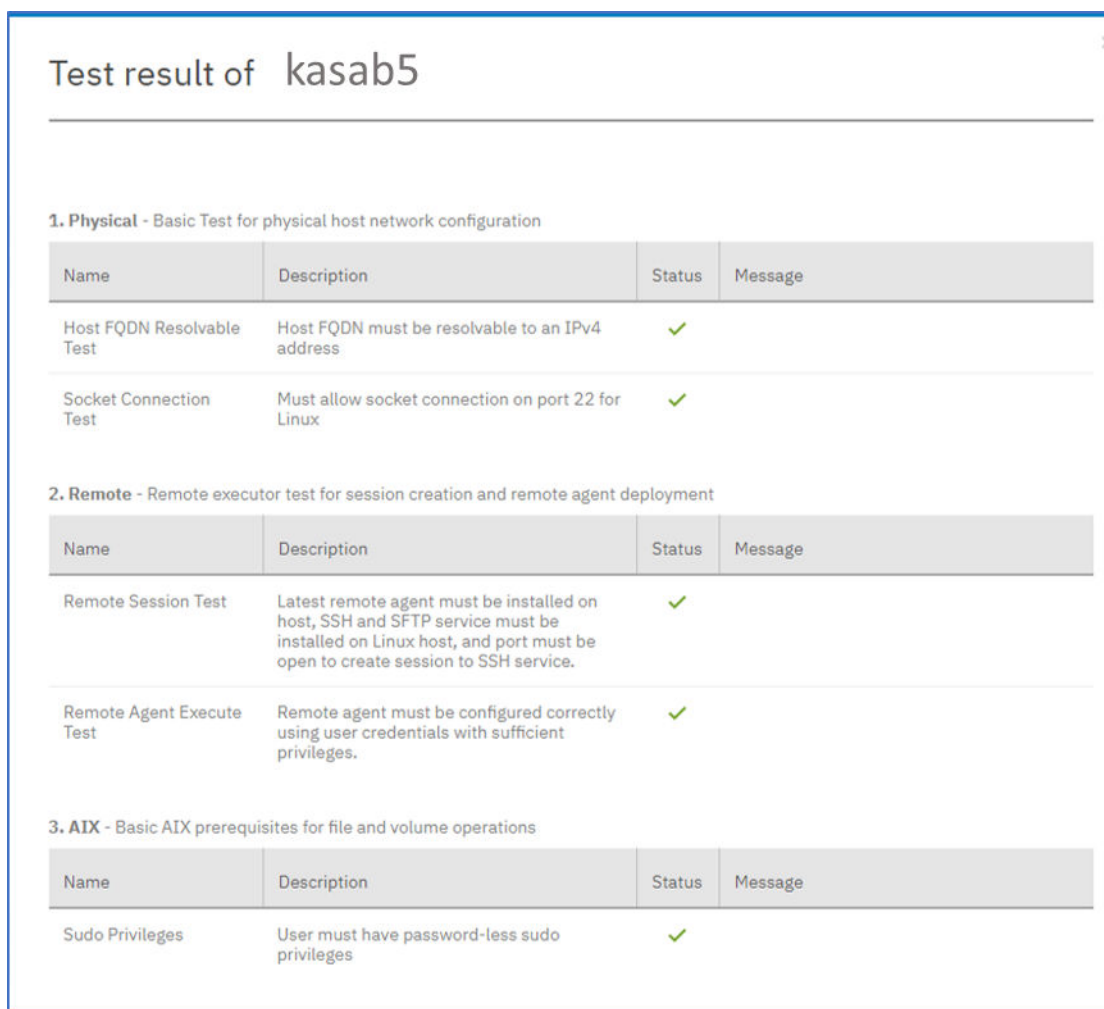
### Prueba de conexión de Db2

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**.

- 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.
- Pulse **Acciones** y seleccione **Probar** para iniciar las pruebas de verificación de las conexiones y los valores físicos, remotos y operativos del sistema.



**Test result of kasab5**

**1. Physical** - Basic Test for physical host network configuration

Name	Description	Status	Message
Host FQDN Resolvable Test	Host FQDN must be resolvable to an IPv4 address	✓	
Socket Connection Test	Must allow socket connection on port 22 for Linux	✓	

**2. Remote** - Remote executor test for session creation and remote agent deployment

Name	Description	Status	Message
Remote Session Test	Latest remote agent must be installed on host, SSH and SFTP service must be installed on Linux host, and port must be open to create session to SSH service.	✓	
Remote Agent Execute Test	Remote agent must be configured correctly using user credentials with sufficient privileges.	✓	

**3. AIX** - Basic AIX prerequisites for file and volume operations

Name	Description	Status	Message
Sudo Privileges	User must have password-less sudo privileges	✓	

Figura 40. 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.

- 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 [Capítulo 18, “Gestión del acceso de usuarios”](#), en la [página 533](#).
- 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 del registro 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 del registro habilitada, una copia de seguridad del 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.

### Acerca de esta tarea

Los pasos siguientes describen cómo hacer copia de seguridad de los recursos asignados a una política de SLA. Para ejecutar un trabajo de copia de seguridad bajo demanda para uno o más recursos independientemente de si esos recursos ya están asociados a una política de SLA, haga clic en **Crear trabajo**, seleccione **Copia de seguridad ad hoc** y siga las instrucciones en [“Ejecución de un trabajo de copia de seguridad ad hoc”](#) en la [página 517](#).

### Procedimiento

1. En el panel de navegación, expanda **Gestionar protección > Aplicaciones > Db2**
2. Seleccione un recurso para realizar una copia de seguridad.
  - Seleccione una instancia completa en el panel **Instancias** pulsando el recuadro de selección del 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.
3. Pulse **Seleccionar opciones** para habilitar o inhabilitar la copia de seguridad del 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 del registro de Db2, consulte [Copias de seguridad de registro](#).

**Options**

☐ Enable Log Backup

Maximum Parallel Streams per Database

**Save**

Figura 41. Panel Copia de seguridad con la opción Habilitar copia de seguridad del registro

Si un trabajo bajo demanda se ejecuta con la opción **Habilitar copia de seguridad del registro** habilitada, se realiza la copia de seguridad del registro. Sin embargo, cuando el trabajo se ejecuta de nuevo en una planificación, la opción se inhabilita para que la ejecución del trabajo impida la posible pérdida de segmentos en una cadena de copias de seguridad.

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, puede ejecutar una copia de seguridad bajo demanda en cualquier momento pulsando **Acciones** para esa 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.

Puede hacer copia de seguridad de una instancia entera con todos sus datos asociados, o hacer copia de seguridad de una o más bases de datos.

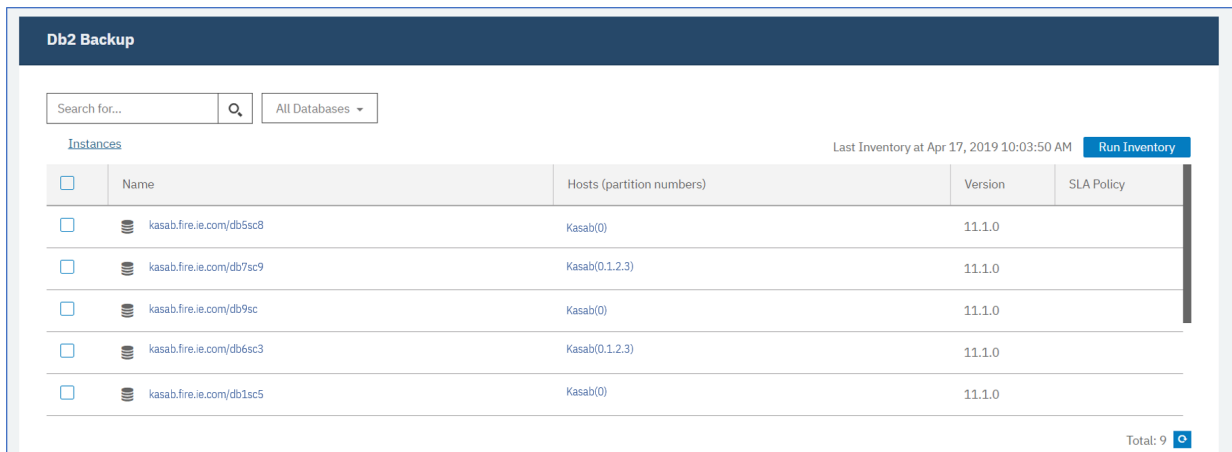


Figura 42. Panel de copia de seguridad de Db2 que instancias

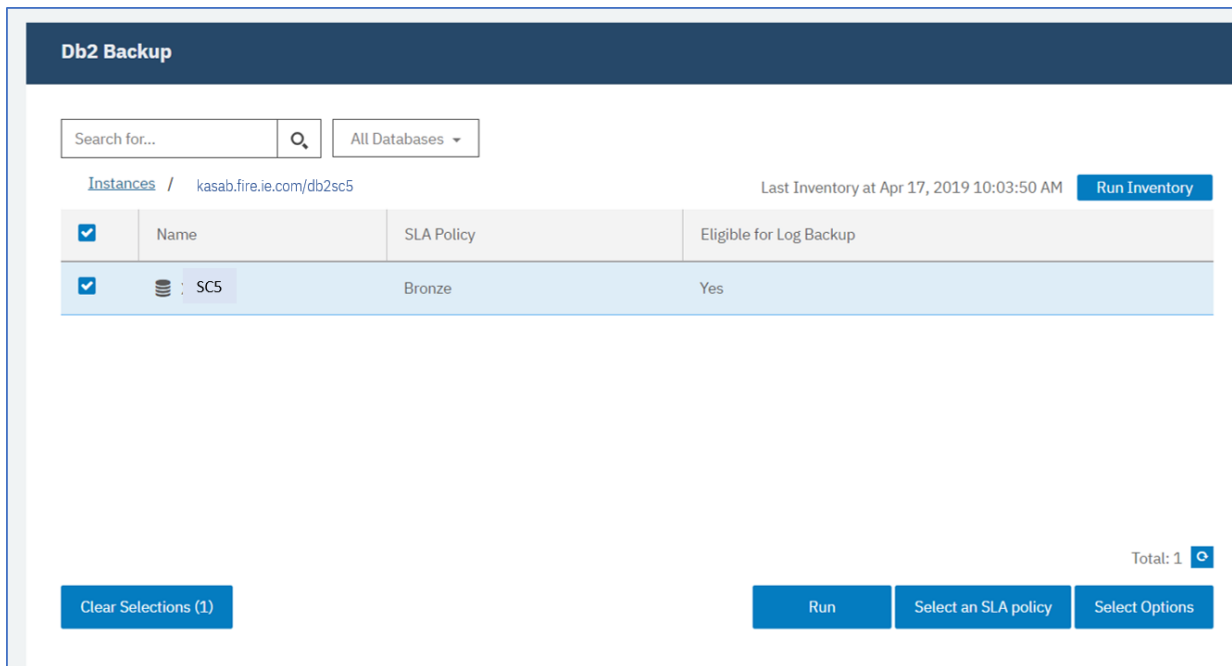


Figura 43. Panel de copia de seguridad de Db2 que muestra bases de datos en una instancia

- Haga clic en **Seleccionar política de SLA** y seleccione una política de SLA: **Oro**, **Plata** o **Bronce**. Guarde su selección.

Las políticas Oro, Plata y Bronce predefinidas tienen diferentes frecuencias y tasas de retención. Puede crear una política de SLA personalizada o editar una política existente navegando a **Descripción general de políticas > Políticas de SLA**.

- Pulse **Seleccionar opciones** para definir opciones para la copia de seguridad, como por ejemplo, habilitar las copias de seguridad del 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.

SLA Policy Status								
					Filter Job Log:	INFO ✕ WARN ✕ ERROR ✕ SUMMARY ✕		
Policy	Frequency	Total	Succeeded	Failed	Next Run	Status	Policy Options	
> Demo	Every 1 Days at 6:05:00 AM	0	0	0	Apr 24, 2019 6:05:00 AM	IDLE		Actions ▾
> Bronze	Every 1 Days at 6:10:00 AM	0	0	0	Apr 24, 2019 6:10:00 AM	IDLE		Actions ▾
> Silver	Every 1 Days at 6:10:00 AM	0	0	0	Apr 24, 2019 6:10:00 AM	IDLE		Actions ▾
> Gold	Every 4 Hours	0	0	0	Apr 23, 2019 2:05:00 PM	IDLE		Actions ▾
								Total: 4
Auto Refresh								

Figura 44. Opciones de copia de seguridad y políticas de SLA

- 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 387.

- Para ejecutar la política fuera del trabajo planificado, seleccione la instancia o 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.

SLA Policy Status								
					Filter Job Log:	INFO ✕ WARN ✕ ERROR ✕ SUMMARY ✕		
Policy	Frequency	Total	Succeeded	Failed	Next Run	Status	Policy Options	
> Demo	Every 1 Days at 6:05:00 AM	0	0	0	Apr 24, 2019 6:05:00 AM	IDLE		Actions ▾
> Bronze	Every 1 Days at 6:10:00 AM	0	0	0	Apr 24, 2019 6:10:00 AM	IDLE		Actions ▾
> Silver	Every 1 Days at 6:10:00 AM	0	0	0	Apr 24, 2019 6:10:00 AM	IDLE		Start Pause Schedule
> Gold	Every 4 Hours	0	0	0	Apr 23, 2019 2:05:00 PM	IDLE		Actions ▾
								Total: 4
Auto Refresh								

Figura 45. Políticas de SLA

**Consejo:** Cuando se ejecuta un trabajo para la política de SLA seleccionada, todos los recursos asociados con esa política de SLA se incluyen en la operación de copia de seguridad. Para hacer copia de seguridad únicamente de los recursos seleccionados, puede ejecutar un trabajo bajo demanda. Un trabajo bajo demanda ejecuta inmediatamente la operación de copia de seguridad.

- Para ejecutar un trabajo de copia de seguridad bajo demanda par un único recurso, seleccione el recurso y haga clic en **Ejecutar**. Si el recurso no está asociado con una política de SLA, el botón **Ejecutar** no está disponible.
- Para ejecutar un trabajo de copia de seguridad bajo demanda para uno o más recursos, haga clic en **Crear trabajo**, seleccione **Copia de seguridad ad hoc** y siga las instrucciones en [“Ejecución de un trabajo de copia de seguridad ad hoc”](#) en la página 517.




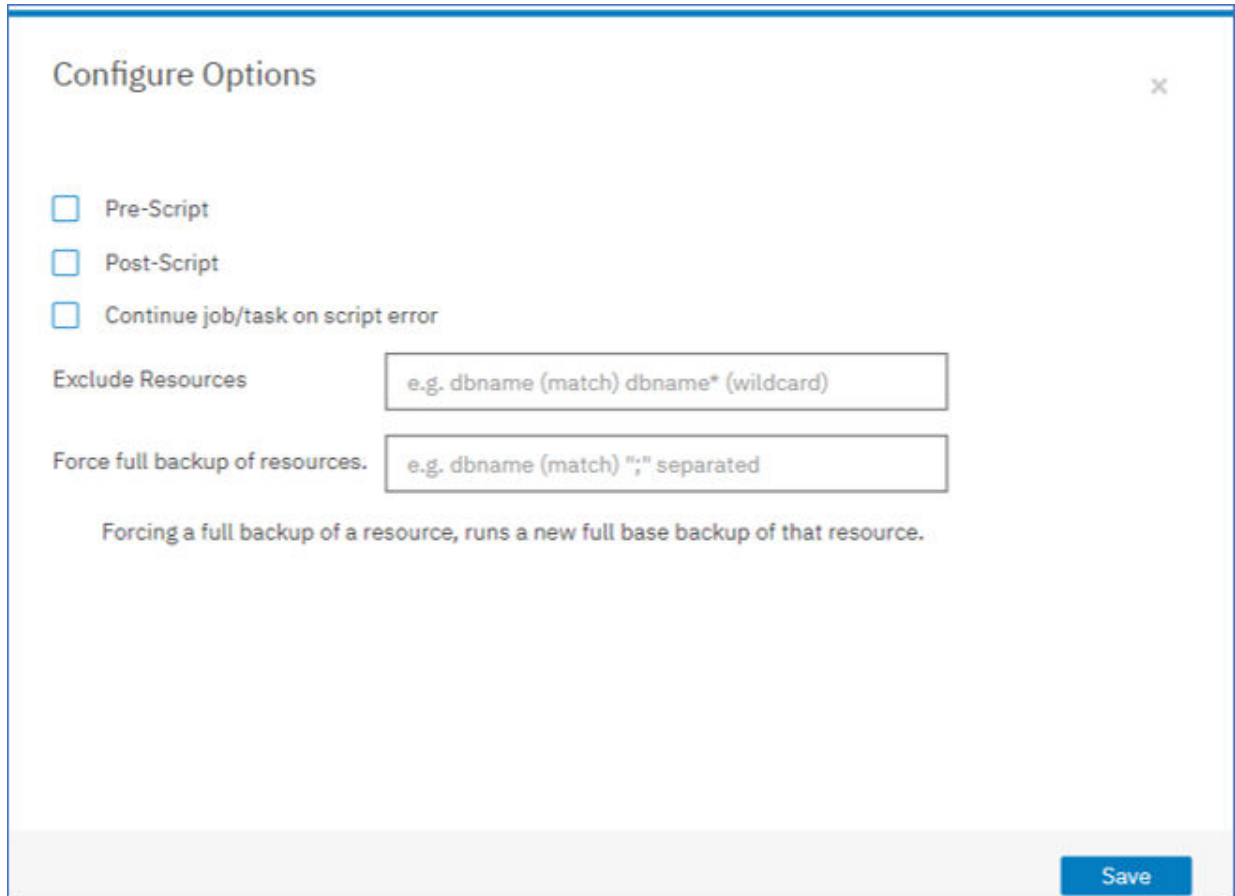
Para poner en pausa la planificación de un SLA, pulse **Acciones** y seleccione **Pausar planificación**.  
Para cancelar un trabajo una vez que se haya iniciado, pulse **Acciones** > **Cancelar**.

### 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 de base de datos 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.



La imagen muestra una ventana de configuración titulada "Configure Options" con un botón de cerrar "x" en la esquina superior derecha. Dentro de la ventana, hay tres opciones de configuración con casillas de verificación: "Pre-Script", "Post-Script" y "Continue job/task on script error". Debajo de estas, hay dos campos de texto. El primero, etiquetado "Exclude Resources", contiene el ejemplo "e.g. dbname (match) dbname\* (wildcard)". El segundo, etiquetado "Force full backup of resources.", contiene el ejemplo "e.g. dbname (match) ';' separated". Debajo de estos campos, hay un texto explicativo: "Forcing a full backup of a resource, runs a new full base backup of that resource." En la esquina inferior derecha de la ventana, hay un botón azul con el texto "Save".

Figura 46. 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 del registro 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 deselectione 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 del registro 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 del registro 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 del registro.

**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 del registro.

**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 del registro. 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 del registro 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 384.](#)

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 382.](#)
- 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 18, “Gestión del acceso de usuarios”, en la página 533.](#)
- 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 pulse **Crear trabajo > Restaurar**.

Se abre el asistente Restaurar.

2. Opcional: Si ha iniciado el asistente de restauración desde la página **Trabajos y operaciones**, pulse **Db2** como tipo de origen y, a continuación, **Siguiente**.

### Sugerencias:

- Para obtener un resumen en ejecución de las selecciones en el asistente, pulse **Vista previa de restauración** en el panel de navegación del asistente.
  - El asistente se abre en la modalidad de configuración predeterminada. Para ejecutar el asistente en modalidad de configuración avanzada, seleccione **Configuración avanzada**. Con la modalidad de configuración avanzada, puede establecer más opciones para el trabajo de restauración.
3. En la página **Seleccionar origen**, haga clic 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  para ese nombre de 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 desde una copia de seguridad de la base de datos de un punto en el tiempo. 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. Complete los campos de la página **Instantánea de origen** y pulse **Siguiente** para continuar.

Los campos que se muestran dependen del número de elementos seleccionados en la página **Seleccionar origen** y en el tipo de restauración. Algunos campos tampoco se muestran hasta que se selecciona un campo relacionado.

**Campos que se muestran para una instantánea bajo demanda, una única restauración de recursos**

Opción	Descripción
<b>Rango de fechas</b>	Especifique un rango de fechas para mostrar las instantáneas disponibles dentro de ese intervalo.
<b>Tipo de almacenamiento de copias de seguridad</b>	<p>Todas las copias de seguridad del rango de fechas seleccionado se listan en filas que muestran la hora a la que se ha realizado la operación de copia de seguridad y la política de acuerdo de nivel de servicio (SLA) para la copia de seguridad. Seleccione la fila que contiene la hora de la copia de seguridad y la política de SLA que desea y, a continuación, realice una de las siguientes acciones:</p> <ul style="list-style-type: none"> <li>Haga clic en el tipo de almacenamiento de copia de seguridad desde el que desea restaurar. Los tipos de almacenamiento que se muestran dependen de los tipos disponibles en el entorno y se muestran en el orden siguiente: <ul style="list-style-type: none"> <li><b>Copia de seguridad</b> Restaura los datos de los que se ha hecho copia de seguridad en un servidor vSnap.</li> <li><b>Réplica</b> Restaura datos que se replican en un servidor vSnap.</li> <li><b>Almacenamiento de objetos</b> Restaura los datos que se copian en un servicio en la nube o en un servidor de repositorio.</li> <li><b>Archivado</b> Restaura los datos que se copian en un archivo de servicio en la nube o en un archivo de servidor de repositorio (cinta).</li> </ul> </li> <li>Haga clic en cualquier sitio en la fila. El primer tipo de copia de seguridad que se muestra secuencialmente desde la izquierda de la fila se selecciona de forma predeterminada. Por ejemplo, si se muestran los tipos de almacenamiento <b>Copia de seguridad</b>, <b>Réplica</b> y <b>Archivado</b>, <b>Copia de seguridad</b> se selecciona de forma predeterminada.</li> </ul>
<b>Utilizar el servidor vSnap alternativo para el trabajo de restauración</b>	<p>Si restaura datos desde un servicio en la nube o un servidor de repositorio, seleccione este recuadro para especificar un servidor vSnap alternativo y, a continuación, seleccione un servidor desde el menú <b>Seleccionar vSnap alternativo</b>.</p> <p>Cuando restaura datos desde un punto de restauración que se ha copiado en 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 copia. Para reducir la carga en el servidor vSnap, puede seleccionar un servidor vSnap alternativo para que sirva como pasarela.</p>

**Campos que se muestran para una instantánea bajo demanda, restauración de varios recursos; restauración de punto en el tiempo o restauración recurrente**

Opción	Descripción
<b>Tipo de ubicación de restauración</b>	<p>Seleccione un tipo de ubicación desde donde se restauran los datos:</p> <p><b>Sitio</b> El sitio en que se ha realizado la copia de seguridad de instantáneas. El sitio se define en el panel <b>Configuración del sistema &gt; Sitio</b>.</p>

Opción	Descripción
	<p><b>Servicio en la nube</b> El servicio en la nube en el que se han copiado las instantáneas. El servicio en la nube se define en el panel <b>Configuración del sistema</b> &gt; <b>Almacenamiento de copias de seguridad</b> &gt; <b>Almacenamiento de objetos</b>.</p> <p><b>Servidor de repositorio</b> El servidor de repositorio en el que se han copiado las instantáneas. El servidor de repositorio se define en el panel <b>Configuración del sistema</b> &gt; <b>Almacenamiento de copias de seguridad</b> &gt; <b>Servidor de repositorio</b>.</p> <p><b>Archivado de servicio en la nube</b> El servicio de archivado en la nube en el que se copiaron las instantáneas. El servicio en la nube se define en el panel <b>Configuración del sistema</b> &gt; <b>Almacenamiento de copias de seguridad</b> &gt; <b>Almacenamiento de objetos</b>.</p> <p><b>Archivado de servidor de repositorio</b> El servidor de repositorio en el que se han copiado las instantáneas en cintas. El servidor de repositorio se define en el panel <b>Configuración del sistema</b> &gt; <b>Almacenamiento de copias de seguridad</b> &gt; <b>Servidor de repositorio</b>.</p>
<b>Seleccionar una ubicación</b>	<p>Si está restaurando datos desde un sitio, seleccione una de las siguientes ubicaciones de restauración:</p> <p><b>Demo</b> El sitio de demostración desde el que se restauran las instantáneas.</p> <p><b>Primario</b> El sitio primario desde el que se restauran las instantáneas.</p> <p><b>Secundario</b> El sitio secundario desde el que se restauran las instantáneas.</p> <p>Si está restaurando datos desde un servidor de nube o de repositorio, seleccione un servidor en el menú <b>Seleccionar una ubicación</b>.</p>
<b>Selector de fecha</b>	Para las operaciones de restauración bajo demanda, especifique un rango de fechas para mostrar las instantáneas disponibles dentro de ese rango.
<b>Punto de restauración</b>	Para las operaciones de restauración bajo demanda, seleccione una instantánea en la lista de instantáneas disponibles en el rango de fechas seleccionado.
<b>Utilizar el servidor vSnap alternativo para el trabajo de restauración</b>	<p>Si restaura datos desde un servicio en la nube o un servidor de repositorio, seleccione este recuadro para especificar un servidor vSnap alternativo y, a continuación, seleccione un servidor desde el menú <b>Seleccionar vSnap alternativo</b>.</p> <p>Cuando restaura datos desde un punto de restauración que se ha copiado en un servicio en la nube o un servidor de repositorio, se utiliza un servidor vSnap como pasarela para completar esta 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 copia. Para reducir la carga en el servidor vSnap, puede seleccionar un servidor vSnap alternativo para que sirva como pasarela.</p>

6. 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](#).

7. 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.

8. 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 del 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**.

9. 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.
10. 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.
11. 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.
12. 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.
13. 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 382.
- 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 18, “Gestión del acceso de usuarios”](#), en la página 533.
- 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 pulse **Crear trabajo > Restaurar**.  
Se abre el asistente Restaurar.
2. Opcional: Si ha iniciado el asistente de restauración desde la página **Trabajos y operaciones**, pulse **Db2** como tipo de origen y, a continuación, **Siguiente**.

### Sugerencias:

- Para obtener un resumen en ejecución de las selecciones en el asistente, pulse **Vista previa de restauración** en el panel de navegación del asistente.
  - El asistente se abre en la modalidad de configuración predeterminada. Para ejecutar el asistente en modalidad de configuración avanzada, seleccione **Configuración avanzada**. Con la modalidad de configuración avanzada, puede establecer más opciones para el trabajo de restauración.
3. En la página **Seleccionar origen**, haga clic 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  para ese nombre de 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 desde una copia de seguridad de la base de datos de un punto en el tiempo. 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. Complete los campos de la página **Instantánea de origen** y pulse **Siguiente** para continuar.

Los campos que se muestran dependen del número de elementos seleccionados en la página **Seleccionar origen** y en el tipo de restauración. Algunos campos tampoco se muestran hasta que se selecciona un campo relacionado.

### Campos que se muestran para una instantánea bajo demanda, una única restauración de recursos

Opción	Descripción
<b>Rango de fechas</b>	Especifique un rango de fechas para mostrar las instantáneas disponibles dentro de ese intervalo.
<b>Tipo de almacenamiento de copias de seguridad</b>	Todas las copias de seguridad del rango de fechas seleccionado se listan en filas que muestran la hora a la que se ha realizado la operación de copia de seguridad y la política de acuerdo de nivel de servicio (SLA) para la copia de seguridad. Seleccione la fila que contiene la hora de la copia de seguridad y la política de SLA que desea y, a continuación, realice una de las siguientes acciones: <ul style="list-style-type: none"><li>• Haga clic en el tipo de almacenamiento de copia de seguridad desde el que desea restaurar. Los tipos de almacenamiento que se muestran dependen de los tipos disponibles en el entorno y se muestran en el orden siguiente:</li></ul>

Opción	Descripción
	<p><b>Copia de seguridad</b> Restaura los datos de los que se ha hecho copia de seguridad en un servidor vSnap.</p> <p><b>Réplica</b> Restaura datos que se replican en un servidor vSnap.</p> <p><b>Almacenamiento de objetos</b> Restaura los datos que se copian en un servicio en la nube o en un servidor de repositorio.</p> <p><b>Archivado</b> Restaura los datos que se copian en un archivo de servicio en la nube o en un archivo de servidor de repositorio (cinta).</p> <ul style="list-style-type: none"> <li>Haga clic en cualquier sitio en la fila. El primer tipo de copia de seguridad que se muestra secuencialmente desde la izquierda de la fila se selecciona de forma predeterminada. Por ejemplo, si se muestran los tipos de almacenamiento <b>Copia de seguridad</b>, <b>Réplica</b> y <b>Archivado</b>, <b>Copia de seguridad</b> se selecciona de forma predeterminada.</li> </ul>
<b>Utilizar el servidor vSnap alternativo para el trabajo de restauración</b>	<p>Si restaura datos desde un servicio en la nube o un servidor de repositorio, seleccione este recuadro para especificar un servidor vSnap alternativo y, a continuación, seleccione un servidor desde el menú <b>Seleccionar vSnap alternativo</b>.</p> <p>Cuando restaura datos desde un punto de restauración que se ha copiado en 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 copia. Para reducir la carga en el servidor vSnap, puede seleccionar un servidor vSnap alternativo para que sirva como pasarela.</p>

**Campos que se muestran para una instantánea bajo demanda, restauración de varios recursos; restauración de punto en el tiempo o restauración recurrente**

Opción	Descripción
<b>Tipo de ubicación de restauración</b>	<p>Seleccione un tipo de ubicación desde donde se restauran los datos:</p> <p><b>Sitio</b> El sitio en que se ha realizado la copia de seguridad de instantáneas. El sitio se define en el panel <b>Configuración del sistema &gt; Sitio</b>.</p> <p><b>Servicio en la nube</b> El servicio en la nube en el que se han copiado las instantáneas. El servicio en la nube se define en el panel <b>Configuración del sistema &gt; Almacenamiento de copias de seguridad &gt; Almacenamiento de objetos</b>.</p> <p><b>Servidor de repositorio</b> El servidor de repositorio en el que se han copiado las instantáneas. El servidor de repositorio se define en el panel <b>Configuración del sistema &gt; Almacenamiento de copias de seguridad &gt; Servidor de repositorio</b>.</p> <p><b>Archivado de servicio en la nube</b> El servicio de archivado en la nube en el que se copiaron las instantáneas. El servicio en la nube se define en el panel <b>Configuración del sistema &gt; Almacenamiento de copias de seguridad &gt; Almacenamiento de objetos</b>.</p>

Opción	Descripción
	<b>Archivado de servidor de repositorio</b> El servidor de repositorio en el que se han copiado las instantáneas en cintas. El servidor de repositorio se define en el panel <b>Configuración del sistema &gt; Almacenamiento de copias de seguridad &gt; Servidor de repositorio</b> .
<b>Seleccionar una ubicación</b>	Si está restaurando datos desde un sitio, seleccione una de las siguientes ubicaciones de restauración: <b>Demo</b> El sitio de demostración desde el que se restauran las instantáneas. <b>Primario</b> El sitio primario desde el que se restauran las instantáneas. <b>Secundario</b> El sitio secundario desde el que se restauran las instantáneas. Si está restaurando datos desde un servidor de nube o de repositorio, seleccione un servidor en el menú <b>Seleccionar una ubicación</b> .
<b>Selector de fecha</b>	Para las operaciones de restauración bajo demanda, especifique un rango de fechas para mostrar las instantáneas disponibles dentro de ese rango.
<b>Punto de restauración</b>	Para las operaciones de restauración bajo demanda, seleccione una instantánea en la lista de instantáneas disponibles en el rango de fechas seleccionado.
<b>Utilizar el servidor vSnap alternativo para el trabajo de restauración</b>	Si restaura datos desde un servicio en la nube o un servidor de repositorio, seleccione este recuadro para especificar un servidor vSnap alternativo y, a continuación, seleccione un servidor desde el menú <b>Seleccionar vSnap alternativo</b> . Cuando restaura datos desde un punto de restauración que se ha copiado en un servicio en la nube o un servidor de repositorio, se utiliza un servidor vSnap como pasarela para completar esta 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 copia. Para reducir la carga en el servidor vSnap, puede seleccionar un servidor vSnap alternativo para que sirva como pasarela.

6. 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.

7. 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.
8. Elija las opciones como se describe en [“Restauración de datos de Db2”](#) en la página 389.
9. 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.

10. 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 382.
- 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 18, “Gestión del acceso de usuarios”](#), en la página 533.
- 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 pulse **Crear trabajo > Restaurar**.  
Se abre el asistente Restaurar.
2. Opcional: Si ha iniciado el asistente de restauración desde la página **Trabajos y operaciones**, pulse **Db2** como tipo de origen y, a continuación, **Siguiente**.

#### Sugerencias:

- Para obtener un resumen en ejecución de las selecciones en el asistente, pulse **Vista previa de restauración** en el panel de navegación del asistente.
  - El asistente se abre en la modalidad de configuración predeterminada. Para ejecutar el asistente en modalidad de configuración avanzada, seleccione **Configuración avanzada**. Con la modalidad de configuración avanzada, puede establecer más opciones para el trabajo de restauración.
3. En la página **Seleccionar origen**, haga clic 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  para ese nombre de 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 desde una copia de seguridad de la base de datos de un punto en el tiempo. 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. Complete los campos de la página **Instantánea de origen** y pulse **Siguiente** para continuar.  
Los campos que se muestran dependen del número de elementos seleccionados en la página **Seleccionar origen** y en el tipo de restauración. Algunos campos tampoco se muestran hasta que se selecciona un campo relacionado.

#### Campos que se muestran para una instantánea bajo demanda, una única restauración de recursos

Opción	Descripción
Rango de fechas	Especifique un rango de fechas para mostrar las instantáneas disponibles dentro de ese intervalo.
Tipo de almacenamiento	Todas las copias de seguridad del rango de fechas seleccionado se listan en filas que muestran la hora a la que se ha realizado la operación de copia de

Opción	Descripción
<b>de copias de seguridad</b>	<p>seguridad y la política de acuerdo de nivel de servicio (SLA) para la copia de seguridad. Seleccione la fila que contiene la hora de la copia de seguridad y la política de SLA que desea y, a continuación, realice una de las siguientes acciones:</p> <ul style="list-style-type: none"> <li>Haga clic en el tipo de almacenamiento de copia de seguridad desde el que desea restaurar. Los tipos de almacenamiento que se muestran dependen de los tipos disponibles en el entorno y se muestran en el orden siguiente: <ul style="list-style-type: none"> <li><b>Copia de seguridad</b> Restaura los datos de los que se ha hecho copia de seguridad en un servidor vSnap.</li> <li><b>Réplica</b> Restaura datos que se replican en un servidor vSnap.</li> <li><b>Almacenamiento de objetos</b> Restaura los datos que se copian en un servicio en la nube o en un servidor de repositorio.</li> <li><b>Archivado</b> Restaura los datos que se copian en un archivo de servicio en la nube o en un archivo de servidor de repositorio (cinta).</li> </ul> </li> <li>Haga clic en cualquier sitio en la fila. El primer tipo de copia de seguridad que se muestra secuencialmente desde la izquierda de la fila se selecciona de forma predeterminada. Por ejemplo, si se muestran los tipos de almacenamiento <b>Copia de seguridad</b>, <b>Réplica</b> y <b>Archivado</b>, <b>Copia de seguridad</b> se selecciona de forma predeterminada.</li> </ul>
<b>Utilizar el servidor vSnap alternativo para el trabajo de restauración</b>	<p>Si restaura datos desde un servicio en la nube o un servidor de repositorio, seleccione este recuadro para especificar un servidor vSnap alternativo y, a continuación, seleccione un servidor desde el menú <b>Seleccionar vSnap alternativo</b>.</p> <p>Cuando restaura datos desde un punto de restauración que se ha copiado en 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 copia. Para reducir la carga en el servidor vSnap, puede seleccionar un servidor vSnap alternativo para que sirva como pasarela.</p>

**Campos que se muestran para una instantánea bajo demanda, restauración de varios recursos; restauración de punto en el tiempo o restauración recurrente**

Opción	Descripción
<b>Tipo de ubicación de restauración</b>	<p>Seleccione un tipo de ubicación desde donde se restauran los datos:</p> <p><b>Sitio</b> El sitio en que se ha realizado la copia de seguridad de instantáneas. El sitio se define en el panel <b>Configuración del sistema &gt; Sitio</b>.</p> <p><b>Servicio en la nube</b> El servicio en la nube en el que se han copiado las instantáneas. El servicio en la nube se define en el panel <b>Configuración del sistema &gt; Almacenamiento de copias de seguridad &gt; Almacenamiento de objetos</b>.</p>

Opción	Descripción
	<p><b>Servidor de repositorio</b> El servidor de repositorio en el que se han copiado las instantáneas. El servidor de repositorio se define en el panel <b>Configuración del sistema &gt; Almacenamiento de copias de seguridad &gt; Servidor de repositorio</b>.</p> <p><b>Archivado de servicio en la nube</b> El servicio de archivado en la nube en el que se copiaron las instantáneas. El servicio en la nube se define en el panel <b>Configuración del sistema &gt; Almacenamiento de copias de seguridad &gt; Almacenamiento de objetos</b>.</p> <p><b>Archivado de servidor de repositorio</b> El servidor de repositorio en el que se han copiado las instantáneas en cintas. El servidor de repositorio se define en el panel <b>Configuración del sistema &gt; Almacenamiento de copias de seguridad &gt; Servidor de repositorio</b>.</p>
<b>Seleccionar una ubicación</b>	<p>Si está restaurando datos desde un sitio, seleccione una de las siguientes ubicaciones de restauración:</p> <p><b>Demo</b> El sitio de demostración desde el que se restauran las instantáneas.</p> <p><b>Primario</b> El sitio primario desde el que se restauran las instantáneas.</p> <p><b>Secundario</b> El sitio secundario desde el que se restauran las instantáneas.</p> <p>Si está restaurando datos desde un servidor de nube o de repositorio, seleccione un servidor en el menú <b>Seleccionar una ubicación</b>.</p>
<b>Selector de fecha</b>	Para las operaciones de restauración bajo demanda, especifique un rango de fechas para mostrar las instantáneas disponibles dentro de ese rango.
<b>Punto de restauración</b>	Para las operaciones de restauración bajo demanda, seleccione una instantánea en la lista de instantáneas disponibles en el rango de fechas seleccionado.
<b>Utilizar el servidor vSnap alternativo para el trabajo de restauración</b>	<p>Si restaura datos desde un servicio en la nube o un servidor de repositorio, seleccione este recuadro para especificar un servidor vSnap alternativo y, a continuación, seleccione un servidor desde el menú <b>Seleccionar vSnap alternativo</b>.</p> <p>Cuando restaura datos desde un punto de restauración que se ha copiado en un servicio en la nube o un servidor de repositorio, se utiliza un servidor vSnap como pasarela para completar esta 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 copia. Para reducir la carga en el servidor vSnap, puede seleccionar un servidor vSnap alternativo para que sirva como pasarela.</p>

6. 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.
7. 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 la 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.
8. Elija las opciones como se describe en “Restauración de datos de Db2” en la página 389.
9. 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.
10. 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 operaciones** **Ejecución de trabajos**.

## Exchange Server

Una vez que haya registrado correctamente un servidor de aplicaciones de 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 el servidor de Exchange

Asegúrese de que todos los requisitos previos de la aplicación Microsoft Exchange se cumplan antes de empezar a proteger las bases de datos de Exchange con IBM Spectrum Protect Plus.

Para obtener más información, consulte “Requisitos de Microsoft Exchange Server” en la página 68.

## Soporte de virtualización

IBM Spectrum Protect Plus da soporte a Exchange Server que se ejecuta en un servidor (bare metal) físico así 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 ayudar a garantizar que un agente de Exchange puede trabajar en el entorno de IBM Spectrum Protect Plus, debe configurar los privilegios adecuados para la cuenta de usuario de Exchange.

## Control de acceso basado en roles

Debe registrar Exchange Server con IBM Spectrum Protect Plus con un usuario de Exchange que tenga privilegios de administrador y los permisos correctos del Control de acceso basado en roles (RBAC).

Además, para las operaciones de restauración granulares, debe utilizar un usuario de Exchange que tiene privilegios de administrador local y los permisos de RBAC correctos.

Para cumplir los requisitos mínimos de un usuario de Exchange, complete los pasos siguientes:

1. Verifique que el usuario de Exchange es miembro de un grupo de administradores locales y que tiene 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 de administración de la organización de Exchange, debe añadir manualmente la cuenta de usuario al grupo de administradores locales realizando una de las siguientes acciones:

- En el sistema del miembro de dominio, pulse **Herramientas administrativas > Gestión de sistemas > Herramienta de usuarios y grupos locales**.
- En un sistema controlador de dominio que no tiene un grupo de administradores locales o una herramienta de de usuario y grupos locales, añada manualmente la cuenta de usuario al grupo de administradores en el dominio: Haga clic en **Herramientas administrativas > Herramienta Usuarios y sistemas de Active Directory**.

2. Establezca el rol y el ámbito.

- Verifique que el usuario de Exchange tiene los permisos de RBAC correctos.

Debe asignar los siguientes roles de gestión a cada usuario de Exchange que completará las operaciones 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

Coloque los usuarios que completan las tareas de restauración de buzón en un grupo de roles de Exchange Server que contiene esos roles.

El servidor de Exchange incluye varios grupos de rol incorporados. El grupo de roles Gestión de la organización contiene, de forma predeterminada, la mayoría, si no todos, los roles listados.

Coloque los usuarios que deben completar varias tareas de restauración de buzón en el grupo de roles Gestión de la organización (asegurándose de que el grupo contiene todos los roles listados).

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. Un usuario cuyo nombre no se encuentra en el grupo o subgrupos de roles de Exchange Organization Management puede experimentar un rendimiento más lento durante las operaciones de restauración.

**Importante:** Puede gestionar los grupos de roles de Exchange mediante 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 de roles de gestión

Asegúrese de que los objetos de Exchange siguientes están en el ámbito de rol de gestión para el usuario de Exchange:

- El Exchange Server que contiene los datos necesarios
- La base de datos de recuperación creada por 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 realiza la operación de restauración

### 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.

### Certificados de Exchange

Los certificados digitales de Exchange se deben instalar y configurar para que el navegador de buzón funcione durante una operación de restauración granular. Asegúrese de que los certificados de Exchange actuales estén instalados y configurados correctamente en el entorno.

**Nota:** Con Exchange 2016 y Exchange 2019, Exchange Server está configurado para utilizar la Seguridad de la capa de transporte (TSL) de forma predeterminada. Esta seguridad TLS cifra la comunicación entre los servidores de Exchange internos y entre los servicios de Exchange en el servidor local.

## Adición de un servidor de aplicaciones de Exchange

Al registrar un servidor de Exchange, 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 los informes.

### Acerca de esta tarea

Para registrar un servidor de aplicaciones de Exchange, necesita la dirección IP o el nombre de host.

### Procedimiento

Para añadir un servidor de aplicaciones de Exchange, complete los pasos siguientes:

1. En el panel de navegación, expanda **Gestionar protección > Bases de datos > 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 403.
5. En el campo **Máximo de bases de datos simultáneas**, establezca el número máximo de bases de datos por política de acuerdo de nivel de servicio (SLA) de las que puede hacer una copia de seguridad simultáneamente. El valor predeterminado es 10. Los valores válidos son 1-99.

Este valor puede ser mayor o menor que el número de bases de datos que están asociadas con una política de SLA. Por ejemplo, si una política de SLA tiene 10 bases de datos asociadas y este valor se establece en 2, se realiza una operación de copia de seguridad para únicamente 2 de las 10 bases de datos al mismo tiempo. Cuando se completan las operaciones de copia de seguridad, se inicia una segunda operación de copia de seguridad hasta que se haya realizado copia de seguridad de todas las bases de datos. Si una política de SLA tiene 5 bases de datos asociadas y este valor se establece en 10, las operaciones de copia de seguridad de las 5 bases de datos se realizarán al mismo tiempo.

Esta opción se aplica únicamente a las políticas de SLA asociadas con varias bases de datos. Para las políticas de SLA asociadas con una sola base de datos, esta opción no proporciona ninguna función.

El número máximo de operaciones de copia de seguridad de base de datos simultáneas está limitado por el entorno. Algunas cosas que se deben tener en cuenta son la configuración del servidor vSnap, el ancho de banda de red y la configuración de disco físico del servidor de IBM Spectrum Protect Plus.

Para obtener directrices sobre el ajuste del entorno de IBM Spectrum Protect Plus para mejorar el rendimiento, consulte [Blueprints de IBM Spectrum Protect Plus](#).

6. 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 Exchange en 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 Exchange ejecutando un inventario”](#) en la página 406. 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 407.

### Detección de bases de datos de Exchange ejecutando un inventario

Cuando añade instancias de Exchange Server a IBM Spectrum Protect Plus, se ejecuta automáticamente un inventario. 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 Exchange”](#) en la página 405.

### Procedimiento

1. En el panel de navegación, expanda **Gestionar protección > Bases de datos > 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 de la lista **Instancias**, compruebe el servidor de aplicaciones de 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 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 > Bases de datos > 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.

## Copia de seguridad de bases de datos de Exchange

Para proteger las bases de datos de 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 los servidores de aplicaciones que contienen bases de datos de Exchange de las que desea realizar copia de de seguridad están registrados con IBM Spectrum Protect Plus. Para obtener más información, consulte [“Adición de un servidor de aplicaciones de Exchange”](#) en la página 405.

### Procedimiento

1. En el panel de navegación, expanda **Gestionar protección > Bases de datos > 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 a 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 del 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.

Para ejecutar un trabajo de copia de seguridad bajo demanda para varias bases de datos asociadas con una política de SLA, haga clic en **Crear trabajo**, seleccione **Copia de seguridad ad hoc** y siga las instrucciones en [“Ejecución de un trabajo de copia de seguridad ad hoc”](#) en la página 517.

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 407.

### Definición de un trabajo de copia de seguridad de Acuerdo de nivel de servicio

Cuando las bases de datos de Exchange se listan para cada una de las instancias de Exchange Server, 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 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 > Bases de datos > 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 para hipervisores, bases de datos y sistemas de archivos”](#) en la página 244.
4. Pulse **Seleccionar opciones** para definir opciones para la copia de seguridad, como por ejemplo, habilitar las copias de seguridad del 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 408.
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 de base de datos 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 Exchange

Puede realizar una copia de seguridad de los registros de transacciones de la base de datos para las bases de datos de Exchange. Las copias de seguridad del registro de Exchange se planifican utilizando el Programador de tareas de Windows. Cuando las copias de seguridad del 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 del 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 > Bases de datos > Exchange**.
2. Pulse la instancia de Exchange Server 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 del registro. Si se registra una base de datos como no apta para la copia de seguridad del registro, se ofrece una explicación de ayuda contextual.

3. Pulse **Seleccionar opciones** y, a continuación, seleccione **Habilitar copia de seguridad de registro**.

Si un trabajo bajo demanda se ejecuta con la opción **Habilitar copia de seguridad del registro** habilitada, se realiza la copia de seguridad del registro. Sin embargo, cuando el trabajo se ejecuta de nuevo en una planificación, la opción se inhabilita para que la ejecución del trabajo impida la posible pérdida de segmentos en una cadena de copias de seguridad.

4. **Restricción:** Los días de la semana para la opción **Semanas** está disponible solo si instala el arreglo temporal de IBM Spectrum Protect Plus 10.1.6 eFix2 o posterior.

Elija la frecuencia de las copias de seguridad de registro en **Minutos, Horas, Días, Semanas, Meses o Años**. Cuando se selecciona **Semanas**, puede seleccionar uno o más días de la semana. La **Hora de inicio** se aplicará a los días seleccionados de la semana.

5. seleccione la hora de inicio de las copias de seguridad del registro y, a continuación, pulse **Guardar**. Elija la **Hora de inicio**.



## 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. Solo una instancia de Exchange Server a la vez puede grabar copias de seguridad del registro en el servidor vSnap.

Los problemas de copia de seguridad del 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 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 > Bases de datos > 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 Exchange que desea ver y, a continuación, seleccione las bases de datos para realizar una 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, solo 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 Exchange

Si los datos de una base de datos Exchange se pierden o se dañan, puede restaurarlos desde una copia de seguridad. Utilice el asistente **Restaurar** 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 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 407](#).
- 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 18, “Gestión del acceso de usuarios”, en la página 533](#).
- 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 datos en una base de datos de Exchange, realice 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 Exchange en la instancia original

Restaure una base de datos de 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 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 18, “Gestión del acceso de usuarios”](#), en la página 533.

### 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, haga clic en **Gestionar protección > Bases de datos > Exchange > Crear trabajo** y, a continuación, seleccione **Restaurar** para abrir el asistente **Restaurar**.

#### Sugerencias:

- También puede abrir el asistente pulsando **Trabajos y operaciones > Crear trabajo > Restaurar > Exchange**.
  - Para obtener un resumen en ejecución de las selecciones en el asistente, pulse **Vista previa de restauración** en el panel de navegación del asistente.
  - El asistente se abre en la modalidad de configuración predeterminada. Para ejecutar el asistente en modalidad de configuración avanzada, seleccione **Configuración avanzada**. Con la modalidad de configuración avanzada, puede establecer más opciones para el trabajo de restauración.
2. En la página **Seleccionar origen**, realice las acciones 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**, seleccione el tipo de trabajo de restauración que desea crear:

#### Bajo demanda: instantánea

Ejecuta una operación de restauración puntual. 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.

4. Complete los campos de la página **Instantánea de origen** y pulse **Siguiente** para continuar.  
Los campos que se muestran dependen del número de elementos seleccionados en la página **Seleccionar origen** y en el tipo de restauración. Algunos campos tampoco se muestran hasta que se selecciona un campo relacionado.

#### Campos que se muestran para una instantánea bajo demanda, una única restauración de recursos

Opción	Descripción
<b>Rango de fechas</b>	Especifique un rango de fechas para mostrar las instantáneas disponibles dentro de ese intervalo.
<b>Tipo de almacenamiento de copias de seguridad</b>	<p>Todas las copias de seguridad del rango de fechas seleccionado se listan en filas que muestran la hora a la que se ha realizado la operación de copia de seguridad y la política de acuerdo de nivel de servicio (SLA) para la copia de seguridad. Seleccione la fila que contiene la hora de la copia de seguridad y la política de SLA que desea y, a continuación, realice una de las siguientes acciones:</p> <ul style="list-style-type: none"> <li>Haga clic en el tipo de almacenamiento de copia de seguridad desde el que desea restaurar. Los tipos de almacenamiento que se muestran dependen de los tipos disponibles en el entorno y se muestran en el orden siguiente: <ul style="list-style-type: none"> <li><b>Copia de seguridad</b> Restaura los datos de los que se ha hecho copia de seguridad en un servidor vSnap.</li> <li><b>Réplica</b> Restaura datos que se replican en un servidor vSnap.</li> <li><b>Almacenamiento de objetos</b> Restaura los datos que se copian en un servicio en la nube o en un servidor de repositorio.</li> <li><b>Archivado</b> Restaura los datos que se copian en un archivo de servicio en la nube o en un archivo de servidor de repositorio (cinta).</li> </ul> </li> <li>Haga clic en cualquier sitio en la fila. El primer tipo de copia de seguridad que se muestra secuencialmente desde la izquierda de la fila se selecciona de forma predeterminada. Por ejemplo, si se muestran los tipos de almacenamiento <b>Copia de seguridad</b>, <b>Réplica</b> y <b>Archivado</b>, <b>Copia de seguridad</b> se selecciona de forma predeterminada.</li> </ul>
<b>Utilizar el servidor vSnap alternativo para el trabajo de restauración</b>	<p>Si restaura datos desde un servicio en la nube o un servidor de repositorio, seleccione este recuadro para especificar un servidor vSnap alternativo y, a continuación, seleccione un servidor desde el menú <b>Seleccionar vSnap alternativo</b>.</p> <p>Cuando restaura datos desde un punto de restauración que se ha copiado en 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 copia. Para reducir la carga en el servidor vSnap, puede seleccionar un servidor vSnap alternativo para que sirva como pasarela.</p>

**Campos que se muestran para una instantánea bajo demanda, restauración de varios recursos; restauración de punto en el tiempo o restauración recurrente**

Opción	Descripción
<b>Tipo de ubicación de restauración</b>	<p>Seleccione un tipo de ubicación desde donde se restauran los datos:</p> <p><b>Sitio</b> El sitio en que se ha realizado la copia de seguridad de instantáneas. El sitio se define en el panel <b>Configuración del sistema &gt; Sitio</b>.</p>

Opción	Descripción
	<p><b>Servicio en la nube</b> El servicio en la nube en el que se han copiado las instantáneas. El servicio en la nube se define en el panel <b>Configuración del sistema</b> &gt; <b>Almacenamiento de copias de seguridad</b> &gt; <b>Almacenamiento de objetos</b>.</p> <p><b>Servidor de repositorio</b> El servidor de repositorio en el que se han copiado las instantáneas. El servidor de repositorio se define en el panel <b>Configuración del sistema</b> &gt; <b>Almacenamiento de copias de seguridad</b> &gt; <b>Servidor de repositorio</b>.</p> <p><b>Archivado de servicio en la nube</b> El servicio de archivado en la nube en el que se copiaron las instantáneas. El servicio en la nube se define en el panel <b>Configuración del sistema</b> &gt; <b>Almacenamiento de copias de seguridad</b> &gt; <b>Almacenamiento de objetos</b>.</p> <p><b>Archivado de servidor de repositorio</b> El servidor de repositorio en el que se han copiado las instantáneas en cintas. El servidor de repositorio se define en el panel <b>Configuración del sistema</b> &gt; <b>Almacenamiento de copias de seguridad</b> &gt; <b>Servidor de repositorio</b>.</p>
<b>Seleccionar una ubicación</b>	<p>Si está restaurando datos desde un sitio, seleccione una de las siguientes ubicaciones de restauración:</p> <p><b>Demo</b> El sitio de demostración desde el que se restauran las instantáneas.</p> <p><b>Primario</b> El sitio primario desde el que se restauran las instantáneas.</p> <p><b>Secundario</b> El sitio secundario desde el que se restauran las instantáneas.</p> <p>Si está restaurando datos desde un servidor de nube o de repositorio, seleccione un servidor en el menú <b>Seleccionar una ubicación</b>.</p>
<b>Selector de fecha</b>	Para las operaciones de restauración bajo demanda, especifique un rango de fechas para mostrar las instantáneas disponibles dentro de ese rango.
<b>Punto de restauración</b>	Para las operaciones de restauración bajo demanda, seleccione una instantánea en la lista de instantáneas disponibles en el rango de fechas seleccionado.
<b>Utilizar el servidor vSnap alternativo para el trabajo de restauración</b>	<p>Si restaura datos desde un servicio en la nube o un servidor de repositorio, seleccione este recuadro para especificar un servidor vSnap alternativo y, a continuación, seleccione un servidor desde el menú <b>Seleccionar vSnap alternativo</b>.</p> <p>Cuando restaura datos desde un punto de restauración que se ha copiado en un servicio en la nube o un servidor de repositorio, se utiliza un servidor vSnap como pasarela para completar esta 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 copia. Para reducir la carga en el servidor vSnap, puede seleccionar un servidor vSnap alternativo para que sirva como pasarela.</p>

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 de recuperación 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 416.

6. En la página **Establecer destino**, seleccione **Restaurar a la instancia original** y pulse **Siguiente**.
7. 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

Restaura 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 del registro están habilitadas, esta opción restaura la base de datos y aplica registros del volumen de copia de seguridad del 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.

8. 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.
9. 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**.
10. 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 Exchange a su instancia original, pero en una ubicación nueva 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, haga clic en **Gestionar protección > Bases de datos > Exchange > Crear trabajo** y, a continuación, seleccione **Restaurar** para abrir el asistente **Restaurar**.

#### **Sugerencias:**

- También puede abrir el asistente pulsando **Trabajos y operaciones > Crear trabajo > Restaurar > Exchange**.
  - Para obtener un resumen en ejecución de las selecciones en el asistente, pulse **Vista previa de restauración** en el panel de navegación del asistente.
  - El asistente se abre en la modalidad de configuración predeterminada. Para ejecutar el asistente en modalidad de configuración avanzada, seleccione **Configuración avanzada**. Con la modalidad de configuración avanzada, puede establecer más opciones para el trabajo de restauración.
2. En la página **Seleccionar origen**, realice las acciones 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**, seleccione el tipo de trabajo de restauración que desea crear:

#### **Bajo demanda: instantánea**

Ejecuta una operación de restauración puntual. 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.

4. Complete los campos de la página **Instantánea de origen** y pulse **Siguiente** para continuar.

Los campos que se muestran dependen del número de elementos seleccionados en la página **Seleccionar origen** y en el tipo de restauración. Algunos campos tampoco se muestran hasta que se selecciona un campo relacionado.

### Campos que se muestran para una instantánea bajo demanda, una única restauración de recursos

Opción	Descripción
<b>Rango de fechas</b>	Especifique un rango de fechas para mostrar las instantáneas disponibles dentro de ese intervalo.
<b>Tipo de almacenamiento de copias de seguridad</b>	<p>Todas las copias de seguridad del rango de fechas seleccionado se listan en filas que muestran la hora a la que se ha realizado la operación de copia de seguridad y la política de acuerdo de nivel de servicio (SLA) para la copia de seguridad. Seleccione la fila que contiene la hora de la copia de seguridad y la política de SLA que desea y, a continuación, realice una de las siguientes acciones:</p> <ul style="list-style-type: none"><li>Haga clic en el tipo de almacenamiento de copia de seguridad desde el que desea restaurar. Los tipos de almacenamiento que se muestran dependen de los tipos disponibles en el entorno y se muestran en el orden siguiente: <b>Copia de seguridad</b> Restaura los datos de los que se ha hecho copia de seguridad en un servidor vSnap. <b>Réplica</b> Restaura datos que se replican en un servidor vSnap. <b>Almacenamiento de objetos</b> Restaura los datos que se copian en un servicio en la nube o en un servidor de repositorio. <b>Archivado</b> Restaura los datos que se copian en un archivo de servicio en la nube o en un archivo de servidor de repositorio (cinta).</li><li>Haga clic en cualquier sitio en la fila. El primer tipo de copia de seguridad que se muestra secuencialmente desde la izquierda de la fila se selecciona de forma predeterminada. Por ejemplo, si se muestran los tipos de almacenamiento <b>Copia de seguridad</b>, <b>Réplica</b> y <b>Archivado</b>, <b>Copia de seguridad</b> se selecciona de forma predeterminada.</li></ul>
<b>Utilizar el servidor vSnap alternativo para el trabajo de restauración</b>	<p>Si restaura datos desde un servicio en la nube o un servidor de repositorio, seleccione este recuadro para especificar un servidor vSnap alternativo y, a continuación, seleccione un servidor desde el menú <b>Seleccionar vSnap alternativo</b>.</p> <p>Cuando restaura datos desde un punto de restauración que se ha copiado en 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 copia. Para reducir la carga en el servidor vSnap, puede seleccionar un servidor vSnap alternativo para que sirva como pasarela.</p>

### Campos que se muestran para una instantánea bajo demanda, restauración de varios recursos; restauración de punto en el tiempo o restauración recurrente

Opción	Descripción
<b>Tipo de ubicación de restauración</b>	<p>Seleccione un tipo de ubicación desde donde se restauran los datos:</p> <p><b>Sitio</b> El sitio en que se ha realizado la copia de seguridad de instantáneas. El sitio se define en el panel <b>Configuración del sistema &gt; Sitio</b>.</p> <p><b>Servicio en la nube</b> El servicio en la nube en el que se han copiado las instantáneas. El servicio en la nube se define en el panel <b>Configuración del sistema &gt; Almacenamiento de copias de seguridad &gt; Almacenamiento de objetos</b>.</p> <p><b>Servidor de repositorio</b> El servidor de repositorio en el que se han copiado las instantáneas. El servidor de repositorio se define en el panel <b>Configuración del sistema &gt; Almacenamiento de copias de seguridad &gt; Servidor de repositorio</b>.</p> <p><b>Archivado de servicio en la nube</b> El servicio de archivado en la nube en el que se copiaron las instantáneas. El servicio en la nube se define en el panel <b>Configuración del sistema &gt; Almacenamiento de copias de seguridad &gt; Almacenamiento de objetos</b>.</p> <p><b>Archivado de servidor de repositorio</b> El servidor de repositorio en el que se han copiado las instantáneas en cintas. El servidor de repositorio se define en el panel <b>Configuración del sistema &gt; Almacenamiento de copias de seguridad &gt; Servidor de repositorio</b>.</p>
<b>Seleccionar una ubicación</b>	<p>Si está restaurando datos desde un sitio, seleccione una de las siguientes ubicaciones de restauración:</p> <p><b>Demo</b> El sitio de demostración desde el que se restauran las instantáneas.</p> <p><b>Primario</b> El sitio primario desde el que se restauran las instantáneas.</p> <p><b>Secundario</b> El sitio secundario desde el que se restauran las instantáneas.</p> <p>Si está restaurando datos desde un servidor de nube o de repositorio, seleccione un servidor en el menú <b>Seleccionar una ubicación</b>.</p>
<b>Selector de fecha</b>	Para las operaciones de restauración bajo demanda, especifique un rango de fechas para mostrar las instantáneas disponibles dentro de ese rango.
<b>Punto de restauración</b>	Para las operaciones de restauración bajo demanda, seleccione una instantánea en la lista de instantáneas disponibles en el rango de fechas seleccionado.
<b>Utilizar el servidor vSnap alternativo para el trabajo de restauración</b>	<p>Si restaura datos desde un servicio en la nube o un servidor de repositorio, seleccione este recuadro para especificar un servidor vSnap alternativo y, a continuación, seleccione un servidor desde el menú <b>Seleccionar vSnap alternativo</b>.</p> <p>Cuando restaura datos desde un punto de restauración que se ha copiado en un servicio en la nube o un servidor de repositorio, se utiliza un servidor vSnap como pasarela para completar esta 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 copia. Para reducir la carga en el servidor vSnap, puede seleccionar un servidor vSnap alternativo para que sirva como pasarela.</p>

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**, especifique la nueva ubicación de directorio para el archivo de base de datos en el servidor, incluido el nombre .edb y la ubicación de los registros.



**Aviso:** Los directorios de destino que especifica en el campo **Vía de acceso de destino** ya deben existir en el host de aplicación. Si no es así, cree los directorios necesarios en el servidor antes de completar la operación de restauración.

Por ejemplo, para una base de datos denominada Database\_A, especifique  
C:\<new\_destination\_path>\Database\_A.edb, para la ubicación de los registros, especifique  
C:\<new\_logs\_path>.

6. En la página **Establecer destino**, seleccione **Restaurar a la instancia original** y pulse **Siguiente**.
7. 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

Restaura 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 del registro están habilitadas, esta opción restaura la base de datos y aplica registros del volumen de copia de seguridad del 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.

8. 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.
9. 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**.
10. 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 en una instancia alternativa

Puede seleccionar una copia de seguridad de base de datos de Microsoft Exchange y restaurarla en 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, haga clic en **Gestionar protección** > **Bases de datos** > **Exchange** > **Crear trabajo** y, a continuación, seleccione **Restaurar** para abrir el asistente **Restaurar**.

##### Sugerencias:

- También puede abrir el asistente pulsando **Trabajos y operaciones** > **Crear trabajo** > **Restaurar** > **Exchange**.
  - Para obtener un resumen en ejecución de las selecciones en el asistente, pulse **Vista previa de restauración** en el panel de navegación del asistente.
  - El asistente se abre en la modalidad de configuración predeterminada. Para ejecutar el asistente en modalidad de configuración avanzada, seleccione **Configuración avanzada**. Con la modalidad de configuración avanzada, puede establecer más opciones para el trabajo de restauración.
2. En la página **Seleccionar origen**, realice las acciones 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**, seleccione el tipo de trabajo de restauración que desea crear:

**Bajo demanda: instantánea**

Ejecuta una operación de restauración puntual. 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.

4. Complete los campos de la página **Instantánea de origen** y pulse **Siguiente** para continuar.

Los campos que se muestran dependen del número de elementos seleccionados en la página

**Seleccionar origen** y en el tipo de restauración. Algunos campos tampoco se muestran hasta que se selecciona un campo relacionado.

**Campos que se muestran para una instantánea bajo demanda, una única restauración de recursos**

Opción	Descripción
<b>Rango de fechas</b>	Especifique un rango de fechas para mostrar las instantáneas disponibles dentro de ese intervalo.
<b>Tipo de almacenamiento de copias de seguridad</b>	<p>Todas las copias de seguridad del rango de fechas seleccionado se listan en filas que muestran la hora a la que se ha realizado la operación de copia de seguridad y la política de acuerdo de nivel de servicio (SLA) para la copia de seguridad. Seleccione la fila que contiene la hora de la copia de seguridad y la política de SLA que desea y, a continuación, realice una de las siguientes acciones:</p> <ul style="list-style-type: none"> <li>Haga clic en el tipo de almacenamiento de copia de seguridad desde el que desea restaurar. Los tipos de almacenamiento que se muestran dependen de los tipos disponibles en el entorno y se muestran en el orden siguiente: <ul style="list-style-type: none"> <li><b>Copia de seguridad</b> Restaura los datos de los que se ha hecho copia de seguridad en un servidor vSnap.</li> <li><b>Réplica</b> Restaura datos que se replican en un servidor vSnap.</li> <li><b>Almacenamiento de objetos</b> Restaura los datos que se copian en un servicio en la nube o en un servidor de repositorio.</li> <li><b>Archivado</b> Restaura los datos que se copian en un archivo de servicio en la nube o en un archivo de servidor de repositorio (cinta).</li> </ul> </li> <li>Haga clic en cualquier sitio en la fila. El primer tipo de copia de seguridad que se muestra secuencialmente desde la izquierda de la fila se selecciona de forma predeterminada. Por ejemplo, si se muestran los tipos de almacenamiento <b>Copia de seguridad</b>, <b>Réplica</b> y <b>Archivado</b>, <b>Copia de seguridad</b> se selecciona de forma predeterminada.</li> </ul>
<b>Utilizar el servidor vSnap alternativo para el trabajo de restauración</b>	<p>Si restaura datos desde un servicio en la nube o un servidor de repositorio, seleccione este recuadro para especificar un servidor vSnap alternativo y, a continuación, seleccione un servidor desde el menú <b>Seleccionar vSnap alternativo</b>.</p> <p>Cuando restaura datos desde un punto de restauración que se ha copiado en un recurso de nube o servidor de repositorio, se utiliza un servidor vSnap como</p>

Opción	Descripción
	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 copia. Para reducir la carga en el servidor vSnap, puede seleccionar un servidor vSnap alternativo para que sirva como pasarela.

**Campos que se muestran para una instantánea bajo demanda, restauración de varios recursos; restauración de punto en el tiempo o restauración recurrente**

Opción	Descripción
<b>Tipo de ubicación de restauración</b>	<p>Seleccione un tipo de ubicación desde donde se restauran los datos:</p> <p><b>Sitio</b> El sitio en que se ha realizado la copia de seguridad de instantáneas. El sitio se define en el panel <b>Configuración del sistema &gt; Sitio</b>.</p> <p><b>Servicio en la nube</b> El servicio en la nube en el que se han copiado las instantáneas. El servicio en la nube se define en el panel <b>Configuración del sistema &gt; Almacenamiento de copias de seguridad &gt; Almacenamiento de objetos</b>.</p> <p><b>Servidor de repositorio</b> El servidor de repositorio en el que se han copiado las instantáneas. El servidor de repositorio se define en el panel <b>Configuración del sistema &gt; Almacenamiento de copias de seguridad &gt; Servidor de repositorio</b>.</p> <p><b>Archivado de servicio en la nube</b> El servicio de archivado en la nube en el que se copiaron las instantáneas. El servicio en la nube se define en el panel <b>Configuración del sistema &gt; Almacenamiento de copias de seguridad &gt; Almacenamiento de objetos</b>.</p> <p><b>Archivado de servidor de repositorio</b> El servidor de repositorio en el que se han copiado las instantáneas en cintas. El servidor de repositorio se define en el panel <b>Configuración del sistema &gt; Almacenamiento de copias de seguridad &gt; Servidor de repositorio</b>.</p>
<b>Seleccionar una ubicación</b>	<p>Si está restaurando datos desde un sitio, seleccione una de las siguientes ubicaciones de restauración:</p> <p><b>Demo</b> El sitio de demostración desde el que se restauran las instantáneas.</p> <p><b>Primario</b> El sitio primario desde el que se restauran las instantáneas.</p> <p><b>Secundario</b> El sitio secundario desde el que se restauran las instantáneas.</p> <p>Si está restaurando datos desde un servidor de nube o de repositorio, seleccione un servidor en el menú <b>Seleccionar una ubicación</b>.</p>
<b>Selector de fecha</b>	Para las operaciones de restauración bajo demanda, especifique un rango de fechas para mostrar las instantáneas disponibles dentro de ese rango.
<b>Punto de restauración</b>	Para las operaciones de restauración bajo demanda, seleccione una instantánea en la lista de instantáneas disponibles en el rango de fechas seleccionado.
<b>Utilizar el servidor vSnap</b>	Si restaura datos desde un servicio en la nube o un servidor de repositorio, seleccione este recuadro para especificar un servidor vSnap alternativo y, a

Opción	Descripción
<b>alternativo para el trabajo de restauración</b>	<p>continuación, seleccione un servidor desde el menú <b>Seleccionar vSnap alternativo</b>.</p> <p>Cuando restaura datos desde un punto de restauración que se ha copiado en un servicio en la nube o un servidor de repositorio, se utiliza un servidor vSnap como pasarela para completar esta 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 copia. Para reducir la carga en el servidor vSnap, puede seleccionar un servidor vSnap alternativo para que sirva como pasarela.</p>

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 de recuperación 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) Expandir el nombre de la base de datos para ver la información de la vía de acceso de origen y de destino. En el campo **Vía de acceso de destino**, especifique la ubicación del directorio del archivo de base de datos de Exchange en el host alternativo, incluido el nombre .edb y la ubicación de los registros.



**Aviso:** Los directorios de destino que especifica en el campo **Vía de acceso de destino** ya deben existir en el host alternativo. Si no es así, cree los directorios necesarios en el host alternativo antes de completar la operación de restauración.

Por ejemplo, para una base de datos denominada Database\_A.edb, especifique C:\<new\_destination\_path>\Database\_A.edb, y para la ubicación de los registros, especifique c:\<new\_logs\_path>.

6. 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**.
7. 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

Restaura 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 del registro están habilitadas, esta opción restaura la base de datos y aplica registros del volumen de copia de seguridad del 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.

8. 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.
9. 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**.
10. 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 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 403](#)) o bien puede ejecutar el asistente de configuración de IBM Spectrum Protect Plus para configurar automáticamente los permisos (véase el paso [“15” en la página 428](#)).

#### 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, haga clic en **Gestionar protección > Bases de datos > Exchange > Crear trabajo** y, a continuación, seleccione **Restaurar** para abrir el asistente **Restaurar**.

### Sugerencias:

- También puede abrir el asistente pulsando **Trabajos y operaciones > Crear trabajo > Restaurar > Exchange**.
  - Para obtener un resumen en ejecución de las selecciones en el asistente, pulse **Vista previa de restauración** en el panel de navegación del asistente.
  - El asistente se abre en la modalidad de configuración predeterminada. Para ejecutar el asistente en modalidad de configuración avanzada, seleccione **Configuración avanzada**. Con la modalidad de configuración avanzada, puede establecer más opciones para el trabajo de restauración.
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**, seleccione el tipo de trabajo de restauración que desea crear:

#### Bajo demanda: instantánea

Ejecuta una operación de restauración puntual. 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.

4. Complete los campos de la página **Instantánea de origen** y pulse **Siguiente** para continuar. Los campos que se muestran dependen del número de elementos seleccionados en la página **Seleccionar origen** y en el tipo de restauración. Algunos campos tampoco se muestran hasta que se selecciona un campo relacionado.

#### Campos que se muestran para una instantánea bajo demanda, una única restauración de recursos

Opción	Descripción
<b>Rango de fechas</b>	Especifique un rango de fechas para mostrar las instantáneas disponibles dentro de ese intervalo.
<b>Tipo de almacenamiento de copias de seguridad</b>	<p>Todas las copias de seguridad del rango de fechas seleccionado se listan en filas que muestran la hora a la que se ha realizado la operación de copia de seguridad y la política de acuerdo de nivel de servicio (SLA) para la copia de seguridad. Seleccione la fila que contiene la hora de la copia de seguridad y la política de SLA que desea y, a continuación, realice una de las siguientes acciones:</p> <ul style="list-style-type: none"> <li>Haga clic en el tipo de almacenamiento de copia de seguridad desde el que desea restaurar. Los tipos de almacenamiento que se muestran dependen de los tipos disponibles en el entorno y se muestran en el orden siguiente: <ul style="list-style-type: none"> <li><b>Copia de seguridad</b> Restaura los datos de los que se ha hecho copia de seguridad en un servidor vSnap.</li> <li><b>Réplica</b> Restaura datos que se replican en un servidor vSnap.</li> <li><b>Almacenamiento de objetos</b> Restaura los datos que se copian en un servicio en la nube o en un servidor de repositorio.</li> <li><b>Archivado</b> Restaura los datos que se copian en un archivo de servicio en la nube o en un archivo de servidor de repositorio (cinta).</li> </ul> </li> <li>Haga clic en cualquier sitio en la fila. El primer tipo de copia de seguridad que se muestra secuencialmente desde la izquierda de la fila se selecciona de forma predeterminada. Por ejemplo, si se muestran los tipos de almacenamiento <b>Copia de seguridad</b>, <b>Réplica</b> y <b>Archivado</b>, <b>Copia de seguridad</b> se selecciona de forma predeterminada.</li> </ul>
<b>Utilizar el servidor vSnap alternativo para el trabajo de restauración</b>	<p>Si restaura datos desde un servicio en la nube o un servidor de repositorio, seleccione este recuadro para especificar un servidor vSnap alternativo y, a continuación, seleccione un servidor desde el menú <b>Seleccionar vSnap alternativo</b>.</p> <p>Cuando restaura datos desde un punto de restauración que se ha copiado en 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 copia. Para reducir la carga en el servidor vSnap, puede seleccionar un servidor vSnap alternativo para que sirva como pasarela.</p>

**Campos que se muestran para una instantánea bajo demanda, restauración de varios recursos; restauración de punto en el tiempo o restauración recurrente**

Opción	Descripción
<b>Tipo de ubicación de restauración</b>	<p>Seleccione un tipo de ubicación desde donde se restauran los datos:</p> <p><b>Sitio</b> El sitio en que se ha realizado la copia de seguridad de instantáneas. El sitio se define en el panel <b>Configuración del sistema &gt; Sitio</b>.</p>



Opción	Descripción
	<p><b>Servicio en la nube</b> El servicio en la nube en el que se han copiado las instantáneas. El servicio en la nube se define en el panel <b>Configuración del sistema</b> &gt; <b>Almacenamiento de copias de seguridad</b> &gt; <b>Almacenamiento de objetos</b>.</p> <p><b>Servidor de repositorio</b> El servidor de repositorio en el que se han copiado las instantáneas. El servidor de repositorio se define en el panel <b>Configuración del sistema</b> &gt; <b>Almacenamiento de copias de seguridad</b> &gt; <b>Servidor de repositorio</b>.</p> <p><b>Archivado de servicio en la nube</b> El servicio de archivado en la nube en el que se copiaron las instantáneas. El servicio en la nube se define en el panel <b>Configuración del sistema</b> &gt; <b>Almacenamiento de copias de seguridad</b> &gt; <b>Almacenamiento de objetos</b>.</p> <p><b>Archivado de servidor de repositorio</b> El servidor de repositorio en el que se han copiado las instantáneas en cintas. El servidor de repositorio se define en el panel <b>Configuración del sistema</b> &gt; <b>Almacenamiento de copias de seguridad</b> &gt; <b>Servidor de repositorio</b>.</p>
<b>Seleccionar una ubicación</b>	<p>Si está restaurando datos desde un sitio, seleccione una de las siguientes ubicaciones de restauración:</p> <p><b>Demo</b> El sitio de demostración desde el que se restauran las instantáneas.</p> <p><b>Primario</b> El sitio primario desde el que se restauran las instantáneas.</p> <p><b>Secundario</b> El sitio secundario desde el que se restauran las instantáneas.</p> <p>Si está restaurando datos desde un servidor de nube o de repositorio, seleccione un servidor en el menú <b>Seleccionar una ubicación</b>.</p>
<b>Selector de fecha</b>	Para las operaciones de restauración bajo demanda, especifique un rango de fechas para mostrar las instantáneas disponibles dentro de ese rango.
<b>Punto de restauración</b>	Para las operaciones de restauración bajo demanda, seleccione una instantánea en la lista de instantáneas disponibles en el rango de fechas seleccionado.
<b>Utilizar el servidor vSnap alternativo para el trabajo de restauración</b>	<p>Si restaura datos desde un servicio en la nube o un servidor de repositorio, seleccione este recuadro para especificar un servidor vSnap alternativo y, a continuación, seleccione un servidor desde el menú <b>Seleccionar vSnap alternativo</b>.</p> <p>Cuando restaura datos desde un punto de restauración que se ha copiado en un servicio en la nube o un servidor de repositorio, se utiliza un servidor vSnap como pasarela para completar esta 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 copia. Para reducir la carga en el servidor vSnap, puede seleccionar un servidor vSnap alternativo para que sirva como pasarela.</p>


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. En la página **Establecer destino**, seleccione **Restaurar a la instancia original** y pulse **Siguiente**.

7. 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.
8. 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.
9. 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**.
10. 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**.
11. 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.
12. 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**.
13. En la GUI MMC de IBM Spectrum Protect Plus, pulse el nodo **Proteger y recuperar datos** y seleccione **Exchange Server**.
14. 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.
15. 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**.
16. 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 62. Vista previa y filtrado de elementos de buzón

Tarea	Acción
Vista previa de elementos de buzón	<p>a. Seleccione un elemento de buzón, como por ejemplo <b>Bandeja de entrada</b>, para visualizar su contenido en el panel de vista previa.</p> <p>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.</p> <p>c. Si un elemento contiene un archivo adjunto, pulse el icono de archivo adjunto para obtener una vista previa de su contenido.</p>
Filtrar elementos de buzón	<p>Utilice las opciones de filtro para reducir la lista de carpetas y mensajes para restaurar:</p> <p>a. Pulse <b>Mostrar opciones de filtro y Añadir fila</b>.</p> <p>b. Pulse la tecla de flecha abajo en el campo <b>Nombre de columna</b> y seleccione un elemento para el filtro. Puede filtrar por el nombre de carpeta, el texto de asunto y otras opciones.</p> <p><b>Restricción:</b> Puede filtrar carpetas de buzón públicas únicamente por la columna <b>Nombre de carpeta</b>.</p> <p>Cuando selecciona <b>Todo el contenido</b>, los elementos del buzón se filtran por nombre del archivo adjunto, remitente, asunto y cuerpo del mensaje.</p> <p>c. En el campo <b>Operador</b>, seleccione un operador: Contiene.</p> <p>d. En el campo <b>Valor</b>, especifique un valor de filtro.</p> <p>e. Para especificar criterios de filtro adicionales, pulse <b>Añadir fila</b>.</p> <p>f. Pulse <b>Aplicar filtro</b> para filtrar los mensajes y las carpetas.</p>

17. 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.

18. 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 63. 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	<p>a. En el panel <b>Acciones</b>, pulse <b>Abrir buzón de Exchange</b>.</p> <p>b. Escriba el alias del buzón para identificarlo como el destino de la restauración.</p> <p>c. Arrastre el elemento de buzón de origen (o buzón) al buzón de destino en el panel de resultados.</p> <p><b>Restricción:</b> No puede arrastrar elementos de correo o subcarpetas desde la carpeta Elementos recuperables hasta un buzón de destino.</p>
Restaurar un elemento de buzón (o buzón de correo) a un archivo de carpetas personales de Outlook (.pst)	<p>a. En el panel <b>Acciones</b>, pulse <b>Abrir archivo PST no Unicode</b>.</p> <p>b. Cuando se abra la ventana <b>Abrir archivo</b>, seleccione un archivo .pst existente o cree un archivo .pst.</p> <p>c. Arrastre el elemento de buzón de origen (o buzón de correo) al archivo .pst de destino en el panel de resultados.</p> <p><b>Restricción:</b> Puede utilizar la vista <b>Navegador de restauración de buzón</b> solo con archivos .pst que no sean Unicode.</p>

Tabla 63. Restauración de un elemento de buzón de correo a otro buzón o archivo .pst (continuación)

Tarea	Acción
Restaurar una carpeta pública	<p>Seleccione esta acción para restaurar una carpeta pública a un buzón de carpeta pública en línea existente.</p> <p>Puede filtrar el buzón y restaurar una determinada carpeta pública a una carpeta pública en línea existente. En el campo <b>Carpeta a restaurar</b>, escriba el nombre de la carpeta pública que desea restaurar.</p> <ul style="list-style-type: none"> <li>• Para restaurar una subcarpeta de una carpeta padre, especifique la vía de acceso a la carpeta completa en este formato:  <i>nombre_carpeta_padre/  nombre_subcarpeta.</i></li> <li>• Para restaurar todas las subcarpetas en una carpeta padre utilice  <i>nombre_carpeta_padre/*.</i></li> <li>• 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 (\).</li> </ul> <p>También puede restaurar toda o parte de una carpeta pública a un buzón de carpeta pública diferente del buzón original. En el campo <b>Buzón de carpeta pública de destino</b> especifique el buzón de carpeta pública de destino en el que desea efectuar la restauración.</p>

19. 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)(<http://www.ibm.com/support/docview.wss?uid=ibm10882270>).

20. Cuando haya finalizado la operación de restauración de los elementos individuales, vuelva a IBM Spectrum Protect Plus. En el panel **Trabajos y operaciones > 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 buzones de 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 403) o bien puede ejecutar el asistente de configuración de IBM Spectrum Protect Plus para configurar automáticamente los permisos (véase el paso “15” en la página 435).

### 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, haga clic en **Gestionar protección > Bases de datos > Exchange > Crear trabajo** y, a continuación, seleccione **Restaurar** para abrir el asistente **Restaurar**.

#### Sugerencias:

- También puede abrir el asistente pulsando **Trabajos y operaciones > Crear trabajo > Restaurar > Exchange**.
  - Para obtener un resumen en ejecución de las selecciones en el asistente, pulse **Vista previa de restauración** en el panel de navegación del asistente.
  - El asistente se abre en la modalidad de configuración predeterminada. Para ejecutar el asistente en modalidad de configuración avanzada, seleccione **Configuración avanzada**. Con la modalidad de configuración avanzada, puede establecer más opciones para el trabajo de restauración.
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**, seleccione el tipo de trabajo de restauración que desea crear:

#### Bajo demanda: instantánea

Ejecuta una operación de restauración puntual. 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.

4. Complete los campos de la página **Instantánea de origen** y pulse **Siguiente** para continuar.

Los campos que se muestran dependen del número de elementos seleccionados en la página **Seleccionar origen** y en el tipo de restauración. Algunos campos tampoco se muestran hasta que se selecciona un campo relacionado.

**Campos que se muestran para una instantánea bajo demanda, una única restauración de recursos**

Opción	Descripción
<b>Rango de fechas</b>	Especifique un rango de fechas para mostrar las instantáneas disponibles dentro de ese intervalo.
<b>Tipo de almacenamiento de copias de seguridad</b>	<p>Todas las copias de seguridad del rango de fechas seleccionado se listan en filas que muestran la hora a la que se ha realizado la operación de copia de seguridad y la política de acuerdo de nivel de servicio (SLA) para la copia de seguridad. Seleccione la fila que contiene la hora de la copia de seguridad y la política de SLA que desea y, a continuación, realice una de las siguientes acciones:</p> <ul style="list-style-type: none"> <li>Haga clic en el tipo de almacenamiento de copia de seguridad desde el que desea restaurar. Los tipos de almacenamiento que se muestran dependen de los tipos disponibles en el entorno y se muestran en el orden siguiente: <ul style="list-style-type: none"> <li><b>Copia de seguridad</b> Restaura los datos de los que se ha hecho copia de seguridad en un servidor vSnap.</li> <li><b>Réplica</b> Restaura datos que se replican en un servidor vSnap.</li> <li><b>Almacenamiento de objetos</b> Restaura los datos que se copian en un servicio en la nube o en un servidor de repositorio.</li> <li><b>Archivado</b> Restaura los datos que se copian en un archivo de servicio en la nube o en un archivo de servidor de repositorio (cinta).</li> </ul> </li> <li>Haga clic en cualquier sitio en la fila. El primer tipo de copia de seguridad que se muestra secuencialmente desde la izquierda de la fila se selecciona de forma predeterminada. Por ejemplo, si se muestran los tipos de almacenamiento <b>Copia de seguridad</b>, <b>Réplica</b> y <b>Archivado</b>, <b>Copia de seguridad</b> se selecciona de forma predeterminada.</li> </ul>
<b>Utilizar el servidor vSnap alternativo para el trabajo de restauración</b>	<p>Si restaura datos desde un servicio en la nube o un servidor de repositorio, seleccione este recuadro para especificar un servidor vSnap alternativo y, a continuación, seleccione un servidor desde el menú <b>Seleccionar vSnap alternativo</b>.</p> <p>Cuando restaura datos desde un punto de restauración que se ha copiado en 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</p>


Opción	Descripción
	seguridad y de copia. Para reducir la carga en el servidor vSnap, puede seleccionar un servidor vSnap alternativo para que sirva como pasarela.

**Campos que se muestran para una instantánea bajo demanda, restauración de varios recursos; restauración de punto en el tiempo o restauración recurrente**

Opción	Descripción
<b>Tipo de ubicación de restauración</b>	<p>Seleccione un tipo de ubicación desde donde se restauran los datos:</p> <p><b>Sitio</b> El sitio en que se ha realizado la copia de seguridad de instantáneas. El sitio se define en el panel <b>Configuración del sistema &gt; Sitio</b>.</p> <p><b>Servicio en la nube</b> El servicio en la nube en el que se han copiado las instantáneas. El servicio en la nube se define en el panel <b>Configuración del sistema &gt; Almacenamiento de copias de seguridad &gt; Almacenamiento de objetos</b>.</p> <p><b>Servidor de repositorio</b> El servidor de repositorio en el que se han copiado las instantáneas. El servidor de repositorio se define en el panel <b>Configuración del sistema &gt; Almacenamiento de copias de seguridad &gt; Servidor de repositorio</b>.</p> <p><b>Archivado de servicio en la nube</b> El servicio de archivado en la nube en el que se copiaron las instantáneas. El servicio en la nube se define en el panel <b>Configuración del sistema &gt; Almacenamiento de copias de seguridad &gt; Almacenamiento de objetos</b>.</p> <p><b>Archivado de servidor de repositorio</b> El servidor de repositorio en el que se han copiado las instantáneas en cintas. El servidor de repositorio se define en el panel <b>Configuración del sistema &gt; Almacenamiento de copias de seguridad &gt; Servidor de repositorio</b>.</p>
<b>Seleccionar una ubicación</b>	<p>Si está restaurando datos desde un sitio, seleccione una de las siguientes ubicaciones de restauración:</p> <p><b>Demo</b> El sitio de demostración desde el que se restauran las instantáneas.</p> <p><b>Primario</b> El sitio primario desde el que se restauran las instantáneas.</p> <p><b>Secundario</b> El sitio secundario desde el que se restauran las instantáneas.</p> <p>Si está restaurando datos desde un servidor de nube o de repositorio, seleccione un servidor en el menú <b>Seleccionar una ubicación</b>.</p>
<b>Selector de fecha</b>	Para las operaciones de restauración bajo demanda, especifique un rango de fechas para mostrar las instantáneas disponibles dentro de ese rango.
<b>Punto de restauración</b>	Para las operaciones de restauración bajo demanda, seleccione una instantánea en la lista de instantáneas disponibles en el rango de fechas seleccionado.
<b>Utilizar el servidor vSnap alternativo para el trabajo de restauración</b>	Si restaura datos desde un servicio en la nube o un servidor de repositorio, seleccione este recuadro para especificar un servidor vSnap alternativo y, a continuación, seleccione un servidor desde el menú <b>Seleccionar vSnap alternativo</b> .



Opción	Descripción
	Cuando restaura datos desde un punto de restauración que se ha copiado en un servicio en la nube o un servidor de repositorio, se utiliza un servidor vSnap como pasarela para completar esta 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 copia. Para reducir la carga en el servidor vSnap, puede seleccionar un servidor vSnap alternativo para que sirva como pasarela.

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. En la página **Establecer destino**, seleccione **Restaurar a la instancia original** y pulse **Siguiente**.
7. 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.
8. 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.
9. 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**.
10. 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**.
11. 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.
12. 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**.
13. En la GUI MMC de IBM Spectrum Protect Plus, pulse el nodo **Proteger y recuperar datos** y seleccione **Exchange Server**.
14. 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.
15. 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**.
16. 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.
17. Para completar la operación de restauración, en el panel **Acciones**, pulse una de las opciones de restauración siguientes.

Tabla 64. Opciones de restauración	
Opción	Acción
<b>Restaurar correo a la ubicación original</b>	Restaurar los elementos de correo a su ubicación en el momento de la operación de copia de seguridad.
<b>Restaurar correo a una ubicación alternativa</b>	<p>Restaurar los elementos de correo a un buzón distinto.</p> <ul style="list-style-type: none"> <li>En la ventana <b>Opciones de buzón alternativo</b>, especifique el nombre de <b>Alias de buzón</b>.</li> </ul> <p><b>Consejo:</b> Si los elementos de buzón o las tareas están marcados con un distintivo en la carpeta <b>Elementos recuperables</b> de un buzón, los elementos se restauran con el atributo del distintivo en la vista <b>Elementos y tareas con distintivo</b> del buzón de destino.</p>
<b>Restaurar correo a un archivo PST no Unicode</b>  <b>Restricción:</b> <ul style="list-style-type: none"> <li>Esta opción solo está disponible para Exchange Server 2013.</li> <li>Cada carpeta puede contener un máximo de 16.383 elementos de correo.</li> </ul>	<p>Restaurar los elementos de correo a un archivo de carpetas personales que no sea Unicode (.pst).</p> <p>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.</p> <p>Si el archivo .pst existe, se utiliza. De lo contrario, el archivo se creará.</p>

Tabla 64. Opciones de restauración (continuación)

Opción	Acción
<b>Restaurar correo a archivo PST Unicode</b>	<p>Restaurar los elementos de correo a un archivo .pst de Unicode.</p> <p>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.</p> <p><b>Consejo:</b></p> <p>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.</p> <p>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.</p>
<b>Restaurar buzón de carpeta pública</b>	<p>Restaurar un buzón de carpeta pública a un buzón de carpeta pública en línea.</p> <p>En el campo <b>Carpeta a restaurar</b>, especifique el nombre de la carpeta pública que desea restaurar:</p> <ul style="list-style-type: none"> <li>• Para restaurar una subcarpeta de una carpeta padre, especifique la vía de acceso a la carpeta completa en este formato: <i>nombre_carpeta_padre/nombre_subcarpeta.</i></li> <li>• Para restaurar todas las subcarpetas en una carpeta padre utilice <i>nombre_carpeta_padre/*.</i></li> <li>• 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 (\).</li> </ul> <p>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 <b>Buzón de carpeta pública de destino</b>, especifique el buzón de la carpeta pública de destino.</p>

Tabla 64. Opciones de restauración (continuación)

Opción	Acción
<b>Restaurar correo a buzón de archivado</b>	<p>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.</p> <p>Puede filtrar el buzón de archivado y restaurar una carpeta de buzón específica. En el campo <b>Carpeta a restaurar</b> especifique el nombre de la carpeta del buzón de archivado que desea restaurar.</p> <ul style="list-style-type: none"> <li>• Para restaurar una subcarpeta de una carpeta padre, especifique la vía de acceso a la carpeta completa en este formato: <i>nombre_carpeta_padre/nombre_subcarpeta.</i></li> <li>• Para restaurar todas las subcarpetas en una carpeta padre utilice <i>nombre_carpeta_padre/*.</i></li> <li>• 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 (\).</li> </ul> <p>En el campo <b>Buzón de archivado de destino</b>, especifique el destino del buzón de archivado.</p>
<b>Excluir elementos de correo recuperables al restaurar el buzón</b>	<p>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.</p> <p>Especifique <b>Sí</b> para excluir los elementos de correo de la carpeta Elementos recuperables de las operaciones de restauración de buzón. <b>No</b> es el valor predeterminado.</p>

**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)(<http://www.ibm.com/support/docview.wss?uid=ibm10882270>).

18. 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, haga clic en **Gestionar protección > Bases de datos > Exchange > Crear trabajo** y, a continuación, seleccione **Restaurar** para abrir el asistente **Restaurar**.

### Sugerencias:

- También puede abrir el asistente pulsando **Trabajos y operaciones > Crear trabajo > Restaurar > Exchange**.
  - Para obtener un resumen en ejecución de las selecciones en el asistente, pulse **Vista previa de restauración** en el panel de navegación del asistente.
  - El asistente se abre en la modalidad de configuración predeterminada. Para ejecutar el asistente en modalidad de configuración avanzada, seleccione **Configuración avanzada**. Con la modalidad de configuración avanzada, puede establecer más opciones para el trabajo de restauración.
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**, seleccione el tipo de trabajo de restauración que desea crear:

#### Bajo demanda: instantánea

Ejecuta una operación de restauración puntual. 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.

4. Complete los campos de la página **Instantánea de origen** y pulse **Siguiente** para continuar.

Los campos que se muestran dependen del número de elementos seleccionados en la página **Seleccionar origen** y en el tipo de restauración. Algunos campos tampoco se muestran hasta que se selecciona un campo relacionado.

#### Campos que se muestran para una instantánea bajo demanda, una única restauración de recursos

Opción	Descripción
<b>Rango de fechas</b>	Especifique un rango de fechas para mostrar las instantáneas disponibles dentro de ese intervalo.

Opción	Descripción
<b>Tipo de almacenamiento de copias de seguridad</b>	<p>Todas las copias de seguridad del rango de fechas seleccionado se listan en filas que muestran la hora a la que se ha realizado la operación de copia de seguridad y la política de acuerdo de nivel de servicio (SLA) para la copia de seguridad. Seleccione la fila que contiene la hora de la copia de seguridad y la política de SLA que desea y, a continuación, realice una de las siguientes acciones:</p> <ul style="list-style-type: none"> <li>Haga clic en el tipo de almacenamiento de copia de seguridad desde el que desea restaurar. Los tipos de almacenamiento que se muestran dependen de los tipos disponibles en el entorno y se muestran en el orden siguiente: <ul style="list-style-type: none"> <li><b>Copia de seguridad</b> Restaura los datos de los que se ha hecho copia de seguridad en un servidor vSnap.</li> <li><b>Réplica</b> Restaura datos que se replican en un servidor vSnap.</li> <li><b>Almacenamiento de objetos</b> Restaura los datos que se copian en un servicio en la nube o en un servidor de repositorio.</li> <li><b>Archivado</b> Restaura los datos que se copian en un archivo de servicio en la nube o en un archivo de servidor de repositorio (cinta).</li> </ul> </li> <li>Haga clic en cualquier sitio en la fila. El primer tipo de copia de seguridad que se muestra secuencialmente desde la izquierda de la fila se selecciona de forma predeterminada. Por ejemplo, si se muestran los tipos de almacenamiento <b>Copia de seguridad</b>, <b>Réplica</b> y <b>Archivado</b>, <b>Copia de seguridad</b> se selecciona de forma predeterminada.</li> </ul>
<b>Utilizar el servidor vSnap alternativo para el trabajo de restauración</b>	<p>Si restaura datos desde un servicio en la nube o un servidor de repositorio, seleccione este recuadro para especificar un servidor vSnap alternativo y, a continuación, seleccione un servidor desde el menú <b>Seleccionar vSnap alternativo</b>.</p> <p>Cuando restaura datos desde un punto de restauración que se ha copiado en 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 copia. Para reducir la carga en el servidor vSnap, puede seleccionar un servidor vSnap alternativo para que sirva como pasarela.</p>

**Campos que se muestran para una instantánea bajo demanda, restauración de varios recursos; restauración de punto en el tiempo o restauración recurrente**

Opción	Descripción
<b>Tipo de ubicación de restauración</b>	<p>Seleccione un tipo de ubicación desde donde se restauran los datos:</p> <p><b>Sitio</b> El sitio en que se ha realizado la copia de seguridad de instantáneas. El sitio se define en el panel <b>Configuración del sistema &gt; Sitio</b>.</p> <p><b>Servicio en la nube</b> El servicio en la nube en el que se han copiado las instantáneas. El servicio en la nube se define en el panel <b>Configuración del sistema &gt; Almacenamiento de copias de seguridad &gt; Almacenamiento de objetos</b>.</p>

Opción	Descripción
	<p><b>Servidor de repositorio</b> El servidor de repositorio en el que se han copiado las instantáneas. El servidor de repositorio se define en el panel <b>Configuración del sistema &gt; Almacenamiento de copias de seguridad &gt; Servidor de repositorio</b>.</p> <p><b>Archivado de servicio en la nube</b> El servicio de archivado en la nube en el que se copiaron las instantáneas. El servicio en la nube se define en el panel <b>Configuración del sistema &gt; Almacenamiento de copias de seguridad &gt; Almacenamiento de objetos</b>.</p> <p><b>Archivado de servidor de repositorio</b> El servidor de repositorio en el que se han copiado las instantáneas en cintas. El servidor de repositorio se define en el panel <b>Configuración del sistema &gt; Almacenamiento de copias de seguridad &gt; Servidor de repositorio</b>.</p>
<b>Seleccionar una ubicación</b>	<p>Si está restaurando datos desde un sitio, seleccione una de las siguientes ubicaciones de restauración:</p> <p><b>Demo</b> El sitio de demostración desde el que se restauran las instantáneas.</p> <p><b>Primario</b> El sitio primario desde el que se restauran las instantáneas.</p> <p><b>Secundario</b> El sitio secundario desde el que se restauran las instantáneas.</p> <p>Si está restaurando datos desde un servidor de nube o de repositorio, seleccione un servidor en el menú <b>Seleccionar una ubicación</b>.</p>
<b>Selector de fecha</b>	Para las operaciones de restauración bajo demanda, especifique un rango de fechas para mostrar las instantáneas disponibles dentro de ese rango.
<b>Punto de restauración</b>	Para las operaciones de restauración bajo demanda, seleccione una instantánea en la lista de instantáneas disponibles en el rango de fechas seleccionado.
<b>Utilizar el servidor vSnap alternativo para el trabajo de restauración</b>	<p>Si restaura datos desde un servicio en la nube o un servidor de repositorio, seleccione este recuadro para especificar un servidor vSnap alternativo y, a continuación, seleccione un servidor desde el menú <b>Seleccionar vSnap alternativo</b>.</p> <p>Cuando restaura datos desde un punto de restauración que se ha copiado en un servicio en la nube o un servidor de repositorio, se utiliza un servidor vSnap como pasarela para completar esta 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 copia. Para reducir la carga en el servidor vSnap, puede seleccionar un servidor vSnap alternativo para que sirva como pasarela.</p>

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. 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.

7. 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

Restaura 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 del registro están habilitadas, esta opción restaura la base de datos y aplica registros del volumen de copia de seguridad del 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.

8. 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.
9. 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**.
10. 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 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, haga clic en **Gestionar protección > Bases de datos > Exchange > Crear trabajo** y, a continuación, seleccione **Restaurar** para abrir el asistente **Restaurar**.

#### Sugerencias:

- También puede abrir el asistente pulsando **Trabajos y operaciones > Crear trabajo > Restaurar > Exchange**.
  - Para obtener un resumen en ejecución de las selecciones en el asistente, pulse **Vista previa de restauración** en el panel de navegación del asistente.
  - El asistente se abre en la modalidad de configuración predeterminada. Para ejecutar el asistente en modalidad de configuración avanzada, seleccione **Configuración avanzada**. Con la modalidad de configuración avanzada, puede establecer más opciones para el trabajo de restauración.
2. En la página **Seleccionar origen**, realice las acciones 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**, seleccione el tipo de trabajo de restauración que desea crear:

#### Bajo demanda: instantánea

Ejecuta una operación de restauración puntual. 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.

4. Complete los campos de la página **Instantánea de origen** y pulse **Siguiente** para continuar.
- Los campos que se muestran dependen del número de elementos seleccionados en la página **Seleccionar origen** y en el tipo de restauración. Algunos campos tampoco se muestran hasta que se selecciona un campo relacionado.

**Campos que se muestran para una instantánea bajo demanda, una única restauración de recursos**

Opción	Descripción
<b>Rango de fechas</b>	Especifique un rango de fechas para mostrar las instantáneas disponibles dentro de ese intervalo.
<b>Tipo de almacenamiento de copias de seguridad</b>	<p>Todas las copias de seguridad del rango de fechas seleccionado se listan en filas que muestran la hora a la que se ha realizado la operación de copia de seguridad y la política de acuerdo de nivel de servicio (SLA) para la copia de seguridad. Seleccione la fila que contiene la hora de la copia de seguridad y la política de SLA que desea y, a continuación, realice una de las siguientes acciones:</p> <ul style="list-style-type: none"> <li>Haga clic en el tipo de almacenamiento de copia de seguridad desde el que desea restaurar. Los tipos de almacenamiento que se muestran dependen de los tipos disponibles en el entorno y se muestran en el orden siguiente: <ul style="list-style-type: none"> <li><b>Copia de seguridad</b> Restaura los datos de los que se ha hecho copia de seguridad en un servidor vSnap.</li> <li><b>Réplica</b> Restaura datos que se replican en un servidor vSnap.</li> <li><b>Almacenamiento de objetos</b> Restaura los datos que se copian en un servicio en la nube o en un servidor de repositorio.</li> <li><b>Archivado</b> Restaura los datos que se copian en un archivo de servicio en la nube o en un archivo de servidor de repositorio (cinta).</li> </ul> </li> <li>Haga clic en cualquier sitio en la fila. El primer tipo de copia de seguridad que se muestra secuencialmente desde la izquierda de la fila se selecciona de forma predeterminada. Por ejemplo, si se muestran los tipos de almacenamiento <b>Copia de seguridad</b>, <b>Réplica</b> y <b>Archivado</b>, <b>Copia de seguridad</b> se selecciona de forma predeterminada.</li> </ul>
<b>Utilizar el servidor vSnap alternativo para el trabajo de restauración</b>	<p>Si restaura datos desde un servicio en la nube o un servidor de repositorio, seleccione este recuadro para especificar un servidor vSnap alternativo y, a continuación, seleccione un servidor desde el menú <b>Seleccionar vSnap alternativo</b>.</p> <p>Cuando restaura datos desde un punto de restauración que se ha copiado en 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 copia. Para reducir la carga en el servidor vSnap, puede seleccionar un servidor vSnap alternativo para que sirva como pasarela.</p>

**Campos que se muestran para una instantánea bajo demanda, restauración de varios recursos; restauración de punto en el tiempo o restauración recurrente**

Opción	Descripción
<b>Tipo de ubicación de restauración</b>	<p>Seleccione un tipo de ubicación desde donde se restauran los datos:</p> <p><b>Sitio</b> El sitio en que se ha realizado la copia de seguridad de instantáneas. El sitio se define en el panel <b>Configuración del sistema &gt; Sitio</b>.</p> <p><b>Servicio en la nube</b> El servicio en la nube en el que se han copiado las instantáneas. El servicio en la nube se define en el panel <b>Configuración del sistema &gt; Almacenamiento de copias de seguridad &gt; Almacenamiento de objetos</b>.</p> <p><b>Servidor de repositorio</b> El servidor de repositorio en el que se han copiado las instantáneas. El servidor de repositorio se define en el panel <b>Configuración del sistema &gt; Almacenamiento de copias de seguridad &gt; Servidor de repositorio</b>.</p> <p><b>Archivado de servicio en la nube</b> El servicio de archivado en la nube en el que se copiaron las instantáneas. El servicio en la nube se define en el panel <b>Configuración del sistema &gt; Almacenamiento de copias de seguridad &gt; Almacenamiento de objetos</b>.</p> <p><b>Archivado de servidor de repositorio</b> El servidor de repositorio en el que se han copiado las instantáneas en cintas. El servidor de repositorio se define en el panel <b>Configuración del sistema &gt; Almacenamiento de copias de seguridad &gt; Servidor de repositorio</b>.</p>
<b>Seleccionar una ubicación</b>	<p>Si está restaurando datos desde un sitio, seleccione una de las siguientes ubicaciones de restauración:</p> <p><b>Demo</b> El sitio de demostración desde el que se restauran las instantáneas.</p> <p><b>Primario</b> El sitio primario desde el que se restauran las instantáneas.</p> <p><b>Secundario</b> El sitio secundario desde el que se restauran las instantáneas.</p> <p>Si está restaurando datos desde un servidor de nube o de repositorio, seleccione un servidor en el menú <b>Seleccionar una ubicación</b>.</p>
<b>Selector de fecha</b>	Para las operaciones de restauración bajo demanda, especifique un rango de fechas para mostrar las instantáneas disponibles dentro de ese rango.
<b>Punto de restauración</b>	Para las operaciones de restauración bajo demanda, seleccione una instantánea en la lista de instantáneas disponibles en el rango de fechas seleccionado.
<b>Utilizar el servidor vSnap alternativo para el trabajo de restauración</b>	<p>Si restaura datos desde un servicio en la nube o un servidor de repositorio, seleccione este recuadro para especificar un servidor vSnap alternativo y, a continuación, seleccione un servidor desde el menú <b>Seleccionar vSnap alternativo</b>.</p> <p>Cuando restaura datos desde un punto de restauración que se ha copiado en un servicio en la nube o un servidor de repositorio, se utiliza un servidor vSnap como pasarela para completar esta 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 copia. Para reducir la carga en el servidor vSnap, puede seleccionar un servidor vSnap alternativo para que sirva como pasarela.</p>

5. En la página **Establecer destino**, especifique dónde desea montar los archivos de base de datos y haga clic en **Siguiente**.

Opción	Descripción
<b>Restaurar a ubicación original</b>	Seleccione esta opción para montar los archivos de base de datos en el servidor original.
<b>Restaurar a ubicación alternativa</b>	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.

6. En la página **Método de restauración**, seleccione **Acceso instantáneo** y, a continuación, pulse **Siguiente**.
7. Opcional: En la página **Opciones de trabajo**, configure las opciones adicionales, si es necesario, y pulse **Siguiente** para continuar.
8. 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.
9. 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**.
10. 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**.
11. 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.
12. 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 74](#).

### Requisitos previos para MongoDB

Se deben cumplir todos los requisitos del sistema y los requisitos previos para IBM Spectrum Protect Plus servidor 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 74](#). Para obtener información sobre el establecimiento de privilegios de sudo, consulte [“Establecimiento de privilegios sudo” en la página 449](#).
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 447](#).
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 MongoDB a 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 desde 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.

A blue rectangular button with a white plus icon on the left and the text "Add application server" in white.

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.

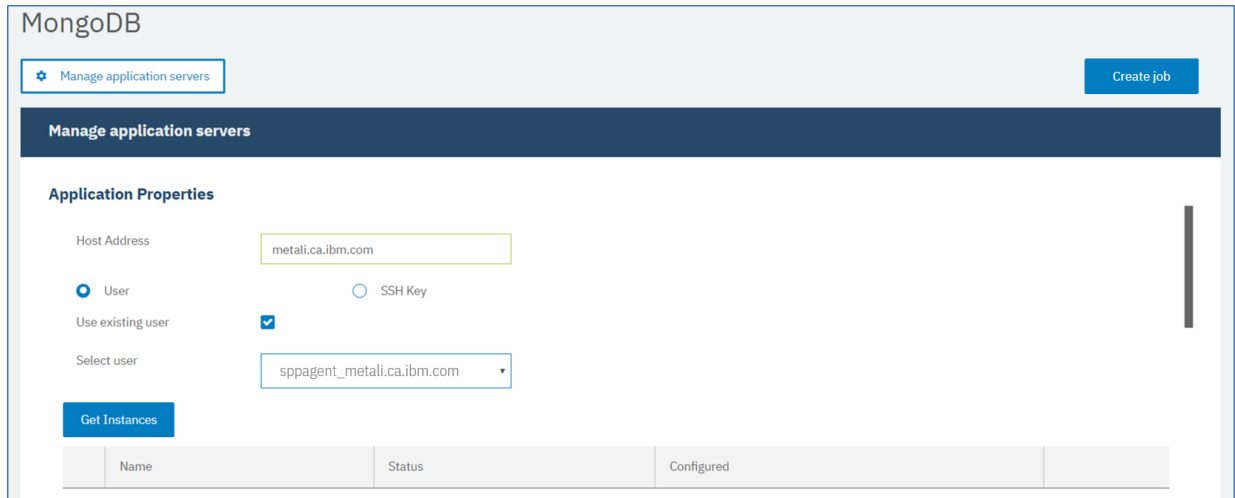


Figura 47. Adición de un agente MongoDB

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 18, “Gestión del acceso de usuarios”](#), en la página 533.

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](#).

### Registro de la base de datos de aplicaciones de MongoDB Ops Manager para protección

Para proteger la base de datos de aplicaciones de MongoDB Ops Manager, primero debe registrar la dirección de host de Ops Manager con IBM Spectrum Protect Plus.

### Procedimiento

1. En el panel de navegación, expanda **Gestionar protección > Aplicaciones > MongoDB**.
2. En la ventana **MongoDB**, haga clic en **Gestionar servidores de aplicaciones** y, a continuación, en **Añadir servidor de aplicaciones**.



3. En el formulario Propiedades de aplicación, escriba la dirección de host para la base de datos de aplicaciones de Ops Manager. Obtenga las instancias y establezca las credenciales siguiendo los pasos indicados en [“Adición de un servidor de aplicaciones de MongoDB”](#) en la página 449.

La base de datos de aplicaciones de Ops Manager se lista en la tabla Instancias como muestra el ejemplo siguiente:

```
metali8.limerick.ie.ibm.com Connection: '333.0.5.1:88888' Ops Manager Application Database
```

### Qué hacer a continuación

La base de datos de aplicaciones de MongoDB Ops Manager está disponible para una copia de seguridad. Puede definir trabajos de copia de seguridad y restauración 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). Para obtener más información, consulte [“Copia de seguridad de datos de MongoDB”](#) en la página 454 y [“Definición de un trabajo de acuerdo de nivel de servicio regular”](#) en la página 455.

### 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

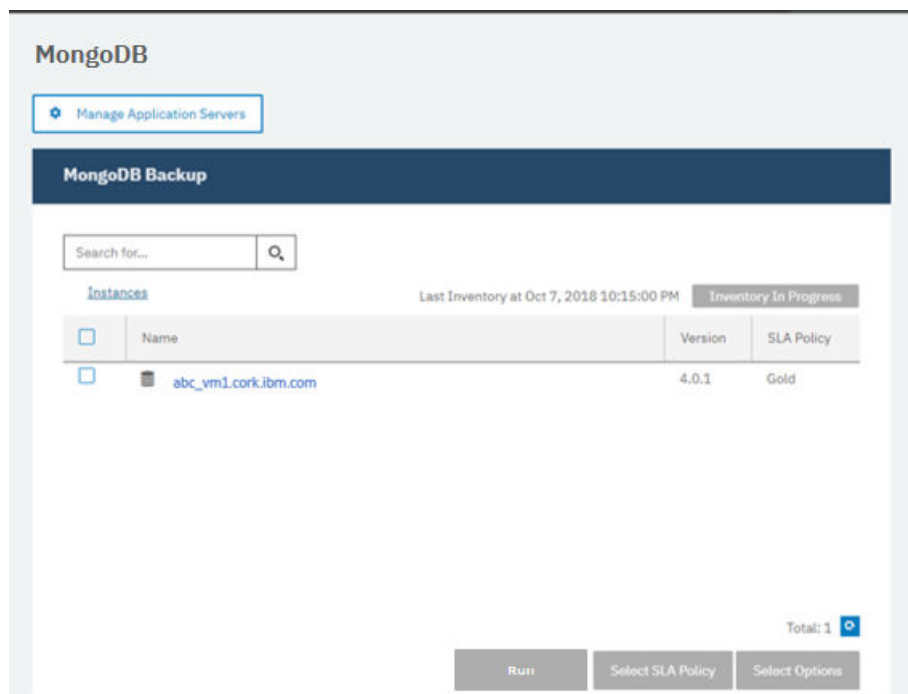
Asegúrese de que ha añadido los servidores de aplicaciones de MongoDB a IBM Spectrum Protect Plus. Para obtener instrucciones, consulte [Adición de un servidor de aplicaciones de MongoDB](#).

## 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.

**1. Physical** - Basic Test for physical host network configuration

Name	Description	Status	Message
Host FQDN Resolvable Test	Host FQDN must be resolvable to an IPv4 address	✓	
Socket Connection Test	Must allow socket connection on port 22 for Linux	✓	

**2. Remote** - Remote executor test for session creation and remote agent deployment

Name	Description	Status	Message
Remote Session Test	Latest remote agent must be installed on host, SSH and SFTP service must be installed on Linux host, and port must be open to create session to SSH service.	✓	
Remote Agent Execute Test	Remote agent must be configured correctly using user credentials with sufficient privileges.	✓	

**3. LINUX** - Basic Linux prerequisites for file and volume operations

Name	Description	Status	Message
Sudo Privileges	User must have password-less sudo privileges	✓	

OK

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, solúcelos y vuelva a ejecutar la prueba para verificar los arreglos.

## Copia de seguridad de datos de MongoDB

Puede definir trabajos de copia de seguridad para proteger los datos de MongoDB. 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 volumen 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 18, “Gestión del acceso de usuarios”, en la página 533](#) y [“Roles para MongoDB” en la página 447](#).

**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.  
  
Para ejecutar un trabajo de copia de seguridad bajo demanda para varias bases de datos asociadas con una política de SLA, haga clic en **Crear trabajo**, seleccione **Copia de seguridad ad hoc** y siga las instrucciones en [“Ejecución de un trabajo de copia de seguridad ad hoc” en la página 517](#).
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** para ese nombre de 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.

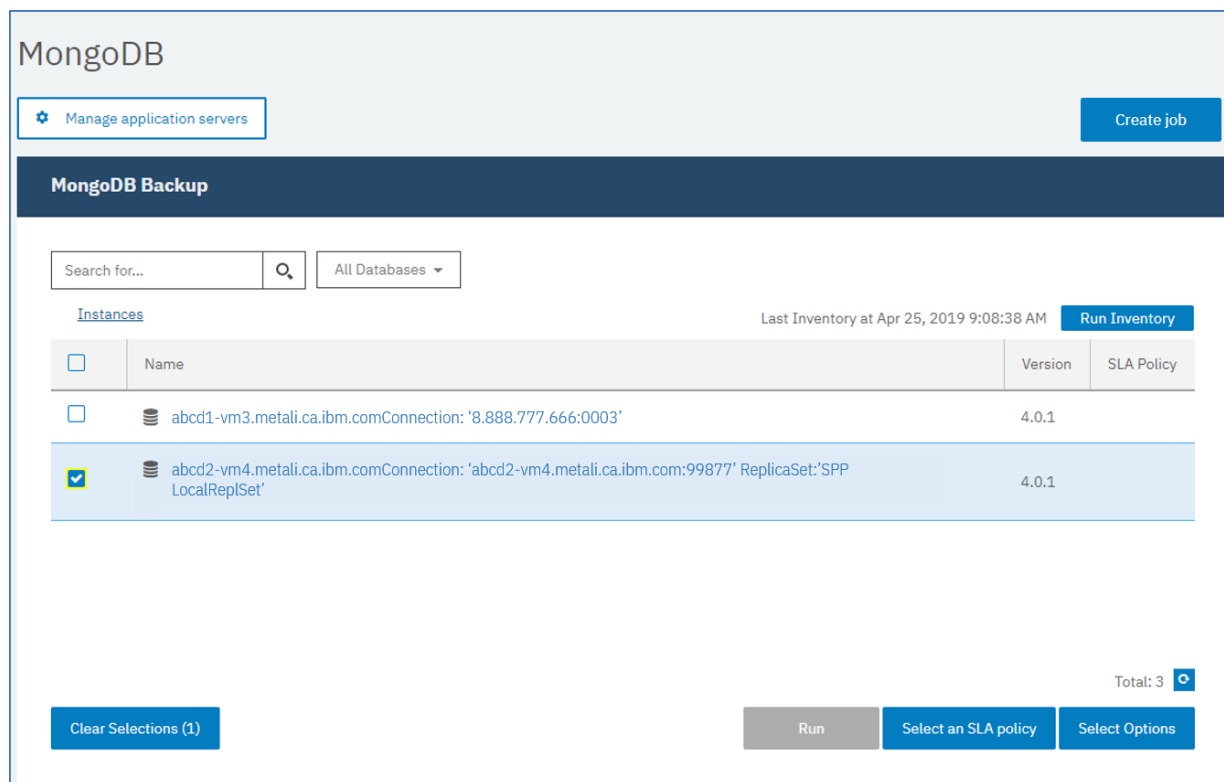


Figura 48. Panel Copia de seguridad de MongoDB que muestra las instancias

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.

Clear Selections (1) Run Select an SLA policy Select Options

**Options**

Maximum Parallel Streams per Database

Save

**SLA Policy Status**

Filter Job Log: Info Warning Error Summary

Policy	Frequency	Total	Succeeded	Failed	Next Run	Status	Policy Options	Actions
Gold	Every 4 Hours	1	1	0	Apr 25, 2019 10:05:00 AM	Idle		

Figura 49. Opciones de copia de seguridad y estado de la política de SLA

- 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 456.

- 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** para ese nombre de 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 de base de datos completa.

### Procedimiento

- 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.

**Configure Options** ×

☐ Pre-Script

☐ Post-Script

☐ Continue job/task on script error

Exclude Resources

Force full backup of resources.

Forcing a full backup of a resource, runs a new full base backup of that resource.

**Save**

Figura 50. 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. Sátese 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 454.
- 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 18, “Gestión del acceso de usuarios”](#), en la página 533 y [“Roles para MongoDB”](#) en la página 447.
- 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** y, a continuación, seleccione **Restaurar** para abrir el asistente de restauración.

#### Sugerencias:

- También puede abrir el asistente pulsando **Trabajos y operaciones > Crear trabajo > Restaurar > MongoDB**.
  - Para obtener un resumen en ejecución de las selecciones en el asistente, pulse **Vista previa de restauración** en el panel de navegación del asistente.
  - El asistente se abre en la modalidad de configuración predeterminada. Para ejecutar el asistente en modalidad de configuración avanzada, seleccione **Configuración avanzada**. Con la modalidad de configuración avanzada, puede establecer más opciones para el trabajo de restauración.
2. En la página **Seleccionar origen**, realice las acciones 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**, seleccione el tipo de trabajo de restauración que desea crear:

**Bajo demanda: instantánea**

Ejecuta una operación de restauración puntual. 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.

4. Complete los campos de la página **Instantánea de origen** y pulse **Siguiente** para continuar.

Los campos que se muestran dependen del número de elementos seleccionados en la página **Seleccionar origen** y en el tipo de restauración. Algunos campos tampoco se muestran hasta que se selecciona un campo relacionado.

**Campos que se muestran para una instantánea bajo demanda, una única restauración de recursos**

Opción	Descripción
<b>Rango de fechas</b>	Especifique un rango de fechas para mostrar las instantáneas disponibles dentro de ese intervalo.
<b>Tipo de almacenamiento de copias de seguridad</b>	<p>Todas las copias de seguridad del rango de fechas seleccionado se listan en filas que muestran la hora a la que se ha realizado la operación de copia de seguridad y la política de acuerdo de nivel de servicio (SLA) para la copia de seguridad. Seleccione la fila que contiene la hora de la copia de seguridad y la política de SLA que desea y, a continuación, realice una de las siguientes acciones:</p> <ul style="list-style-type: none"> <li>Haga clic en el tipo de almacenamiento de copia de seguridad desde el que desea restaurar. Los tipos de almacenamiento que se muestran dependen de los tipos disponibles en el entorno y se muestran en el orden siguiente: <ul style="list-style-type: none"> <li><b>Copia de seguridad</b> Restaura los datos de los que se ha hecho copia de seguridad en un servidor vSnap.</li> <li><b>Réplica</b> Restaura datos que se replican en un servidor vSnap.</li> <li><b>Almacenamiento de objetos</b> Restaura los datos que se copian en un servicio en la nube o en un servidor de repositorio.</li> <li><b>Archivado</b> Restaura los datos que se copian en un archivo de servicio en la nube o en un archivo de servidor de repositorio (cinta).</li> </ul> </li> <li>Haga clic en cualquier sitio en la fila. El primer tipo de copia de seguridad que se muestra secuencialmente desde la izquierda de la fila se selecciona de</li> </ul>

Opción	Descripción
	forma predeterminada. Por ejemplo, si se muestran los tipos de almacenamiento <b>Copia de seguridad, Réplica y Archivado, Copia de seguridad</b> se selecciona de forma predeterminada.
<b>Utilizar el servidor vSnap alternativo para el trabajo de restauración</b>	<p>Si restaura datos desde un servicio en la nube o un servidor de repositorio, seleccione este recuadro para especificar un servidor vSnap alternativo y, a continuación, seleccione un servidor desde el menú <b>Seleccionar vSnap alternativo</b>.</p> <p>Cuando restaura datos desde un punto de restauración que se ha copiado en 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 copia. Para reducir la carga en el servidor vSnap, puede seleccionar un servidor vSnap alternativo para que sirva como pasarela.</p>

**Campos que se muestran para una instantánea bajo demanda, restauración de varios recursos; restauración de punto en el tiempo o restauración recurrente**

Opción	Descripción
<b>Tipo de ubicación de restauración</b>	<p>Seleccione un tipo de ubicación desde donde se restauran los datos:</p> <p><b>Sitio</b> El sitio en que se ha realizado la copia de seguridad de instantáneas. El sitio se define en el panel <b>Configuración del sistema &gt; Sitio</b>.</p> <p><b>Servicio en la nube</b> El servicio en la nube en el que se han copiado las instantáneas. El servicio en la nube se define en el panel <b>Configuración del sistema &gt; Almacenamiento de copias de seguridad &gt; Almacenamiento de objetos</b>.</p> <p><b>Servidor de repositorio</b> El servidor de repositorio en el que se han copiado las instantáneas. El servidor de repositorio se define en el panel <b>Configuración del sistema &gt; Almacenamiento de copias de seguridad &gt; Servidor de repositorio</b>.</p> <p><b>Archivado de servicio en la nube</b> El servicio de archivado en la nube en el que se copiaron las instantáneas. El servicio en la nube se define en el panel <b>Configuración del sistema &gt; Almacenamiento de copias de seguridad &gt; Almacenamiento de objetos</b>.</p> <p><b>Archivado de servidor de repositorio</b> El servidor de repositorio en el que se han copiado las instantáneas en cintas. El servidor de repositorio se define en el panel <b>Configuración del sistema &gt; Almacenamiento de copias de seguridad &gt; Servidor de repositorio</b>.</p>
<b>Seleccionar una ubicación</b>	<p>Si está restaurando datos desde un sitio, seleccione una de las siguientes ubicaciones de restauración:</p> <p><b>Demo</b> El sitio de demostración desde el que se restauran las instantáneas.</p> <p><b>Primario</b> El sitio primario desde el que se restauran las instantáneas.</p> <p><b>Secundario</b> El sitio secundario desde el que se restauran las instantáneas.</p>

Opción	Descripción
	Si está restaurando datos desde un servidor de nube o de repositorio, seleccione un servidor en el menú <b>Seleccionar una ubicación</b> .
<b>Selector de fecha</b>	Para las operaciones de restauración bajo demanda, especifique un rango de fechas para mostrar las instantáneas disponibles dentro de ese rango.
<b>Punto de restauración</b>	Para las operaciones de restauración bajo demanda, seleccione una instantánea en la lista de instantáneas disponibles en el rango de fechas seleccionado.
<b>Utilizar el servidor vSnap alternativo para el trabajo de restauración</b>	<p>Si restaura datos desde un servicio en la nube o un servidor de repositorio, seleccione este recuadro para especificar un servidor vSnap alternativo y, a continuación, seleccione un servidor desde el menú <b>Seleccionar vSnap alternativo</b>.</p> <p>Cuando restaura datos desde un punto de restauración que se ha copiado en un servicio en la nube o un servidor de repositorio, se utiliza un servidor vSnap como pasarela para completar esta 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 copia. Para reducir la carga en el servidor vSnap, puede seleccionar un servidor vSnap alternativo para que sirva como pasarela.</p>

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. 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](#).

7. 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.

8. 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.

9. En la página **Planificación**, pulse **Siguiente** para iniciar los trabajos bajo demanda después de completar el asistente de restauración. 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.
10. 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.

11. 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 454](#).



- 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 18, “Gestión del acceso de usuarios”](#), en la página 533 y [“Roles para MongoDB”](#) en la página 447.
- 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** y, a continuación, seleccione **Restaurar** para abrir el asistente de restauración.

### Sugerencias:

- También puede abrir el asistente pulsando **Trabajos y operaciones > Crear trabajo > Restaurar > MongoDB**.
  - Para obtener un resumen en ejecución de las selecciones en el asistente, pulse **Vista previa de restauración** en el panel de navegación del asistente.
  - El asistente se abre en la modalidad de configuración predeterminada. Para ejecutar el asistente en modalidad de configuración avanzada, seleccione **Configuración avanzada**. Con la modalidad de configuración avanzada, puede establecer más opciones para el trabajo de restauración.
2. En la página **Seleccionar origen**, realice las acciones 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**, seleccione el tipo de trabajo de restauración que desea crear:

#### Bajo demanda: instantánea

Ejecuta una operación de restauración puntual. 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.

4. Complete los campos de la página **Instantánea de origen** y pulse **Siguiente** para continuar.

Los campos que se muestran dependen del número de elementos seleccionados en la página **Seleccionar origen** y en el tipo de restauración. Algunos campos tampoco se muestran hasta que se selecciona un campo relacionado.

**Campos que se muestran para una instantánea bajo demanda, una única restauración de recursos**

Opción	Descripción
<b>Rango de fechas</b>	Especifique un rango de fechas para mostrar las instantáneas disponibles dentro de ese intervalo.
<b>Tipo de almacenamiento de copias de seguridad</b>	<p>Todas las copias de seguridad del rango de fechas seleccionado se listan en filas que muestran la hora a la que se ha realizado la operación de copia de seguridad y la política de acuerdo de nivel de servicio (SLA) para la copia de seguridad. Seleccione la fila que contiene la hora de la copia de seguridad y la política de SLA que desea y, a continuación, realice una de las siguientes acciones:</p> <ul style="list-style-type: none"> <li>Haga clic en el tipo de almacenamiento de copia de seguridad desde el que desea restaurar. Los tipos de almacenamiento que se muestran dependen de los tipos disponibles en el entorno y se muestran en el orden siguiente: <ul style="list-style-type: none"> <li><b>Copia de seguridad</b> Restaura los datos de los que se ha hecho copia de seguridad en un servidor vSnap.</li> <li><b>Réplica</b> Restaura datos que se replican en un servidor vSnap.</li> <li><b>Almacenamiento de objetos</b> Restaura los datos que se copian en un servicio en la nube o en un servidor de repositorio.</li> <li><b>Archivado</b> Restaura los datos que se copian en un archivo de servicio en la nube o en un archivo de servidor de repositorio (cinta).</li> </ul> </li> <li>Haga clic en cualquier sitio en la fila. El primer tipo de copia de seguridad que se muestra secuencialmente desde la izquierda de la fila se selecciona de forma predeterminada. Por ejemplo, si se muestran los tipos de almacenamiento <b>Copia de seguridad</b>, <b>Réplica</b> y <b>Archivado</b>, <b>Copia de seguridad</b> se selecciona de forma predeterminada.</li> </ul>
<b>Utilizar el servidor vSnap alternativo para el trabajo de restauración</b>	<p>Si restaura datos desde un servicio en la nube o un servidor de repositorio, seleccione este recuadro para especificar un servidor vSnap alternativo y, a continuación, seleccione un servidor desde el menú <b>Seleccionar vSnap alternativo</b>.</p> <p>Cuando restaura datos desde un punto de restauración que se ha copiado en 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 copia. Para reducir la carga en el servidor vSnap, puede seleccionar un servidor vSnap alternativo para que sirva como pasarela.</p>

**Campos que se muestran para una instantánea bajo demanda, restauración de varios recursos; restauración de punto en el tiempo o restauración recurrente**

Opción	Descripción
<b>Tipo de ubicación de restauración</b>	<p>Seleccione un tipo de ubicación desde donde se restauran los datos:</p> <p><b>Sitio</b> El sitio en que se ha realizado la copia de seguridad de instantáneas. El sitio se define en el panel <b>Configuración del sistema &gt; Sitio</b>.</p> <p><b>Servicio en la nube</b> El servicio en la nube en el que se han copiado las instantáneas. El servicio en la nube se define en el panel <b>Configuración del sistema &gt; Almacenamiento de copias de seguridad &gt; Almacenamiento de objetos</b>.</p> <p><b>Servidor de repositorio</b> El servidor de repositorio en el que se han copiado las instantáneas. El servidor de repositorio se define en el panel <b>Configuración del sistema &gt; Almacenamiento de copias de seguridad &gt; Servidor de repositorio</b>.</p> <p><b>Archivado de servicio en la nube</b> El servicio de archivado en la nube en el que se copiaron las instantáneas. El servicio en la nube se define en el panel <b>Configuración del sistema &gt; Almacenamiento de copias de seguridad &gt; Almacenamiento de objetos</b>.</p> <p><b>Archivado de servidor de repositorio</b> El servidor de repositorio en el que se han copiado las instantáneas en cintas. El servidor de repositorio se define en el panel <b>Configuración del sistema &gt; Almacenamiento de copias de seguridad &gt; Servidor de repositorio</b>.</p>
<b>Seleccionar una ubicación</b>	<p>Si está restaurando datos desde un sitio, seleccione una de las siguientes ubicaciones de restauración:</p> <p><b>Demo</b> El sitio de demostración desde el que se restauran las instantáneas.</p> <p><b>Primario</b> El sitio primario desde el que se restauran las instantáneas.</p> <p><b>Secundario</b> El sitio secundario desde el que se restauran las instantáneas.</p> <p>Si está restaurando datos desde un servidor de nube o de repositorio, seleccione un servidor en el menú <b>Seleccionar una ubicación</b>.</p>
<b>Selector de fecha</b>	Para las operaciones de restauración bajo demanda, especifique un rango de fechas para mostrar las instantáneas disponibles dentro de ese rango.
<b>Punto de restauración</b>	Para las operaciones de restauración bajo demanda, seleccione una instantánea en la lista de instantáneas disponibles en el rango de fechas seleccionado.
<b>Utilizar el servidor vSnap alternativo para el trabajo de restauración</b>	<p>Si restaura datos desde un servicio en la nube o un servidor de repositorio, seleccione este recuadro para especificar un servidor vSnap alternativo y, a continuación, seleccione un servidor desde el menú <b>Seleccionar vSnap alternativo</b>.</p> <p>Cuando restaura datos desde un punto de restauración que se ha copiado en un servicio en la nube o un servidor de repositorio, se utiliza un servidor vSnap como pasarela para completar esta 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 copia. Para reducir la carga en el servidor vSnap, puede seleccionar un servidor vSnap alternativo para que sirva como pasarela.</p>



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. En la página **Establecer destino**, seleccione **Restaurar a la instancia original** y pulse **Siguiente**.

7. 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.

8. 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.

9. En la página **Planificación**, pulse **Siguiente** para iniciar los trabajos bajo demanda después de completar el asistente de restauración. 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.
10. 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.

11. 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 454.
- 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 18, “Gestión del acceso de usuarios”](#), en la página 533 y [“Roles para MongoDB”](#) en la página 447.
- 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** y, a continuación, seleccione **Restaurar** para abrir el asistente de restauración.

#### Sugerencias:

- También puede abrir el asistente pulsando **Trabajos y operaciones > Crear trabajo > Restaurar > MongoDB**.
  - Para obtener un resumen en ejecución de las selecciones en el asistente, pulse **Vista previa de restauración** en el panel de navegación del asistente.
  - El asistente se abre en la modalidad de configuración predeterminada. Para ejecutar el asistente en modalidad de configuración avanzada, seleccione **Configuración avanzada**. Con la modalidad de configuración avanzada, puede establecer más opciones para el trabajo de restauración.
2. En la página **Seleccionar origen**, realice las acciones 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**, seleccione el tipo de trabajo de restauración que desea crear:
- Bajo demanda: instantánea**  
Ejecuta una operación de restauración puntual. 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.
4. Complete los campos de la página **Instantánea de origen** y pulse **Siguiente** para continuar.
- Los campos que se muestran dependen del número de elementos seleccionados en la página **Seleccionar origen** y en el tipo de restauración. Algunos campos tampoco se muestran hasta que se selecciona un campo relacionado.

**Campos que se muestran para una instantánea bajo demanda, una única restauración de recursos**

Opción	Descripción
<b>Rango de fechas</b>	Especifique un rango de fechas para mostrar las instantáneas disponibles dentro de ese intervalo.
<b>Tipo de almacenamiento de copias de seguridad</b>	<p>Todas las copias de seguridad del rango de fechas seleccionado se listan en filas que muestran la hora a la que se ha realizado la operación de copia de seguridad y la política de acuerdo de nivel de servicio (SLA) para la copia de seguridad. Seleccione la fila que contiene la hora de la copia de seguridad y la política de SLA que desea y, a continuación, realice una de las siguientes acciones:</p> <ul style="list-style-type: none"> <li>Haga clic en el tipo de almacenamiento de copia de seguridad desde el que desea restaurar. Los tipos de almacenamiento que se muestran dependen de los tipos disponibles en el entorno y se muestran en el orden siguiente: <ul style="list-style-type: none"> <li><b>Copia de seguridad</b> Restaura los datos de los que se ha hecho copia de seguridad en un servidor vSnap.</li> <li><b>Réplica</b> Restaura datos que se replican en un servidor vSnap.</li> <li><b>Almacenamiento de objetos</b> Restaura los datos que se copian en un servicio en la nube o en un servidor de repositorio.</li> <li><b>Archivado</b> Restaura los datos que se copian en un archivo de servicio en la nube o en un archivo de servidor de repositorio (cinta).</li> </ul> </li> <li>Haga clic en cualquier sitio en la fila. El primer tipo de copia de seguridad que se muestra secuencialmente desde la izquierda de la fila se selecciona de forma predeterminada. Por ejemplo, si se muestran los tipos de almacenamiento <b>Copia de seguridad</b>, <b>Réplica</b> y <b>Archivado</b>, <b>Copia de seguridad</b> se selecciona de forma predeterminada.</li> </ul>
<b>Utilizar el servidor vSnap alternativo para</b>	Si restaura datos desde un servicio en la nube o un servidor de repositorio, seleccione este recuadro para especificar un servidor vSnap alternativo y, a continuación, seleccione un servidor desde el menú <b>Seleccionar vSnap alternativo</b> .

Opción	Descripción
<b>el trabajo de restauración</b>	Cuando restaura datos desde un punto de restauración que se ha copiado en 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 copia. Para reducir la carga en el servidor vSnap, puede seleccionar un servidor vSnap alternativo para que sirva como pasarela.

**Campos que se muestran para una instantánea bajo demanda, restauración de varios recursos; restauración de punto en el tiempo o restauración recurrente**

Opción	Descripción
<b>Tipo de ubicación de restauración</b>	<p>Seleccione un tipo de ubicación desde donde se restauran los datos:</p> <p><b>Sitio</b> El sitio en que se ha realizado la copia de seguridad de instantáneas. El sitio se define en el panel <b>Configuración del sistema &gt; Sitio</b>.</p> <p><b>Servicio en la nube</b> El servicio en la nube en el que se han copiado las instantáneas. El servicio en la nube se define en el panel <b>Configuración del sistema &gt; Almacenamiento de copias de seguridad &gt; Almacenamiento de objetos</b>.</p> <p><b>Servidor de repositorio</b> El servidor de repositorio en el que se han copiado las instantáneas. El servidor de repositorio se define en el panel <b>Configuración del sistema &gt; Almacenamiento de copias de seguridad &gt; Servidor de repositorio</b>.</p> <p><b>Archivado de servicio en la nube</b> El servicio de archivado en la nube en el que se copiaron las instantáneas. El servicio en la nube se define en el panel <b>Configuración del sistema &gt; Almacenamiento de copias de seguridad &gt; Almacenamiento de objetos</b>.</p> <p><b>Archivado de servidor de repositorio</b> El servidor de repositorio en el que se han copiado las instantáneas en cintas. El servidor de repositorio se define en el panel <b>Configuración del sistema &gt; Almacenamiento de copias de seguridad &gt; Servidor de repositorio</b>.</p>
<b>Seleccionar una ubicación</b>	<p>Si está restaurando datos desde un sitio, seleccione una de las siguientes ubicaciones de restauración:</p> <p><b>Demo</b> El sitio de demostración desde el que se restauran las instantáneas.</p> <p><b>Primario</b> El sitio primario desde el que se restauran las instantáneas.</p> <p><b>Secundario</b> El sitio secundario desde el que se restauran las instantáneas.</p> <p>Si está restaurando datos desde un servidor de nube o de repositorio, seleccione un servidor en el menú <b>Seleccionar una ubicación</b>.</p>
<b>Selector de fecha</b>	Para las operaciones de restauración bajo demanda, especifique un rango de fechas para mostrar las instantáneas disponibles dentro de ese rango.
<b>Punto de restauración</b>	Para las operaciones de restauración bajo demanda, seleccione una instantánea en la lista de instantáneas disponibles en el rango de fechas seleccionado.

Opción	Descripción
<b>Utilizar el servidor vSnap alternativo para el trabajo de restauración</b>	<p>Si restaura datos desde un servicio en la nube o un servidor de repositorio, seleccione este recuadro para especificar un servidor vSnap alternativo y, a continuación, seleccione un servidor desde el menú <b>Seleccionar vSnap alternativo</b>.</p> <p>Cuando restaura datos desde un punto de restauración que se ha copiado en un servicio en la nube o un servidor de repositorio, se utiliza un servidor vSnap como pasarela para completar esta 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 copia. Para reducir la carga en el servidor vSnap, puede seleccionar un servidor vSnap alternativo para que sirva como pasarela.</p>

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. 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.

7. 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.

8. 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.

9. En la página **Planificación**, pulse **Siguiente** para iniciar los trabajos bajo demanda después de completar el asistente de restauración. 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.
10. 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.

11. 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 **mongoexport** 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 **mongoexport** para las bases de datos que necesite.
- Restaure cualquier número de colecciones utilizando los mandatos **mongodump** y **mongoexport** para las colecciones que necesite.

#### Procedimiento

1. En el panel de navegación, pulse **Gestionar protección > Aplicaciones > MongoDB > Crear trabajo** y, a continuación, seleccione **Restaurar** para abrir el asistente **Restaurar**.
2. En la página **Seleccionar origen**, realice las acciones 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 **Método de restauración**, seleccione **Probar** y pulse **Siguiente** para continuar con el proceso de restauración de prueba.
  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. Continúe a través de las páginas del asistente de restauración y seleccione las opciones necesarias.
6. 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.

7. Inicie la sesión en el servidor de MongoDB al que se dirige el trabajo de restauración de prueba.
8. Ejecute el mandato del sistema MongoDB `ps -ef | grep mongod` para encontrar la ubicación de instancia de MongoDB de recuperación temporal.
9. 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 <nombredb> <carpeta_volcado>
```

O,

```
mongodump --host <nombre_host> --port <puerto> --collection <nombre_colección>
<carpeta_volcado>
```

10. 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 <nombredb> <carpeta_volcado>
\<nombredb>
```

O,

```
mongorestore --host <nombre_host> --port <puerto> --collection <nombre_colección>
<carpeta_volcado>\<nombredb>
```

11. Cuando finalice la operación de restauración de la base de datos o de la colección, vaya a **Trabajos y operaciones > Recursos activos**.
12. Pulse **Acciones > Cancelar restauración** para finalizar el procedimiento de restauración granular.

# 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 copia de seguridad y restauración de bases de datos del servidor Oracle”](#) en la página 85.

## 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 > Bases de datos > Oracle**.
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
<b>Usuario</b>	<p>Pulse en esta opción para especificar un usuario existente o especifique un ID de usuario y contraseña. El usuario debe tener configurados privilegios <b>sudo</b>. Rellene los campos según se indica a continuación:</p> <p><b>Utilizar usuario existente</b> 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 <b>Seleccionar usuario</b>.</p> <p><b>ID de usuario</b> 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 <i>dominio\nombre</i>. Si el usuario es un administrador local, utilice el formato <i>local_administrator</i>.</p> <p>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.</p> <p><b>Contraseña</b> Escriba la contraseña del servidor de aplicaciones.</p>
<b>Clave SSH</b>	<p>Pulse en esta opción para utilizar una clave SSH. Seleccione una clave de la lista <b>Seleccionar una clave SSH</b>.</p>

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 <a href="#">“Creación de un rol” en la página 539</a> .

### Conceptos relacionados

“Gestión del acceso de usuarios” en la página 533

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 478

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 481

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 > Bases de datos > Oracle**.
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 Plus y el host.

### Procedimiento

Para probar la conexión, complete los pasos siguientes:

1. En el panel de navegación, pulse **Gestionar protección > Bases de datos > Oracle**.
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 del 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 del registro habilitada, una copia de seguridad del 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 18, “Gestión del acceso de usuarios”](#), en la página 533.
- 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 476.
- Configure las políticas de SLA. Para obtener más información, consulte el apartado [“Crear políticas de copia de seguridad”](#) en la página 169.

### Acerca de esta tarea

Durante la copia de seguridad de base de datos 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 el trabajo de 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 476.

## Procedimiento

Para definir un trabajo de copia de seguridad de Oracle, complete los pasos siguientes:

1. En el panel de navegación, pulse **Gestionar protección > Bases de datos > 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**.

**Consejo:** Cuando se ejecuta un trabajo para la política de SLA seleccionada, todos los recursos asociados con esa política de SLA se incluyen en la operación de copia de seguridad. Para hacer copia de seguridad únicamente de los recursos seleccionados, puede ejecutar un trabajo bajo demanda. Un trabajo bajo demanda ejecuta inmediatamente la operación de copia de seguridad.

- Para ejecutar un trabajo de copia de seguridad bajo demanda par un único recurso, seleccione el recurso y haga clic en **Ejecutar**. Si el recurso no está asociado con una política de SLA, el botón **Ejecutar** no está disponible.
  - Para ejecutar un trabajo de copia de seguridad bajo demanda para uno o más recursos, haga clic en **Crear trabajo**, seleccione **Copia de seguridad ad hoc** y siga las instrucciones en [“Ejecución de un trabajo de copia de seguridad ad hoc”](#) en la página 517.
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 del 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 del registro de transacción desde la ubicación primaria hasta el volumen de copia de seguridad del registro a la frecuencia específica por el valor de **Frecuencia**.

Si un trabajo bajo demanda se ejecuta con la opción **Habilitar copia de seguridad del registro** habilitada, se realiza la copia de seguridad del registro. Sin embargo, cuando el trabajo se ejecuta de nuevo en una planificación, la opción se inhabilita para que la ejecución del trabajo impida la posible pérdida de segmentos en una cadena de copias de seguridad.

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 del 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 del 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 del 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 icono de portapapeles **Opciones de política**  que está asociado al trabajo en la sección **Estado de política de SLA**. Establezca las opciones de política adicionales siguientes:

### 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 de base de datos 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 <a href="#">página 481</a> .

## Conceptos relacionados

“Configuración de scripts para las operaciones de copia de seguridad y restauración” en la [página 518](#)

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 **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 478](#).
- 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 18, “Gestión del acceso de usuarios”](#), en la [página 533](#).

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 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, haga clic en **Gestionar protección > Bases de datos > Oracle > Crear trabajo** y, a continuación, seleccione **Restaurar** para abrir el asistente **Restaurar**.

#### Sugerencias:

- También puede abrir el asistente pulsando **Trabajos y operaciones > Crear trabajo > Restaurar > Oracle**.
  - Para obtener un resumen en ejecución de las selecciones en el asistente, pulse **Vista previa de restauración** en el panel de navegación del asistente.
  - El asistente se abre en la modalidad de configuración predeterminada. Para ejecutar el asistente en modalidad de configuración avanzada, seleccione **Configuración avanzada**. Con la modalidad de configuración avanzada, puede establecer más opciones para el trabajo de restauración.
2. En la página **Seleccionar origen**, realice las acciones 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**, seleccione el tipo de trabajo de restauración que desea crear:

#### Bajo demanda: instantánea

Ejecuta una operación de restauración puntual. 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.

4. Complete los campos de la página **Instantánea de origen** y pulse **Siguiente** para continuar.

Los campos que se muestran dependen del número de elementos seleccionados en la página **Seleccionar origen** y en el tipo de restauración. Algunos campos tampoco se muestran hasta que se selecciona un campo relacionado.

**Campos que se muestran para una instantánea bajo demanda, una única restauración de recursos**

Opción	Descripción
<b>Rango de fechas</b>	Especifique un rango de fechas para mostrar las instantáneas disponibles dentro de ese intervalo.
<b>Tipo de almacenamiento de copias de seguridad</b>	<p>Todas las copias de seguridad del rango de fechas seleccionado se listan en filas que muestran la hora a la que se ha realizado la operación de copia de seguridad y la política de acuerdo de nivel de servicio (SLA) para la copia de seguridad. Seleccione la fila que contiene la hora de la copia de seguridad y la política de SLA que desea y, a continuación, realice una de las siguientes acciones:</p> <ul style="list-style-type: none"> <li>Haga clic en el tipo de almacenamiento de copia de seguridad desde el que desea restaurar. Los tipos de almacenamiento que se muestran dependen de los tipos disponibles en el entorno y se muestran en el orden siguiente: <ul style="list-style-type: none"> <li><b>Copia de seguridad</b> Restaura los datos de los que se ha hecho copia de seguridad en un servidor vSnap.</li> <li><b>Réplica</b> Restaura datos que se replican en un servidor vSnap.</li> <li><b>Almacenamiento de objetos</b> Restaura los datos que se copian en un servicio en la nube o en un servidor de repositorio.</li> <li><b>Archivado</b> Restaura los datos que se copian en un archivo de servicio en la nube o en un archivo de servidor de repositorio (cinta).</li> </ul> </li> <li>Haga clic en cualquier sitio en la fila. El primer tipo de copia de seguridad que se muestra secuencialmente desde la izquierda de la fila se selecciona de forma predeterminada. Por ejemplo, si se muestran los tipos de almacenamiento <b>Copia de seguridad</b>, <b>Réplica</b> y <b>Archivado</b>, <b>Copia de seguridad</b> se selecciona de forma predeterminada.</li> </ul>
<b>Utilizar el servidor vSnap alternativo para el trabajo de restauración</b>	<p>Si restaura datos desde un servicio en la nube o un servidor de repositorio, seleccione este recuadro para especificar un servidor vSnap alternativo y, a continuación, seleccione un servidor desde el menú <b>Seleccionar vSnap alternativo</b>.</p> <p>Cuando restaura datos desde un punto de restauración que se ha copiado en 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</p>

Opción	Descripción
	seguridad y de copia. Para reducir la carga en el servidor vSnap, puede seleccionar un servidor vSnap alternativo para que sirva como pasarela.

**Campos que se muestran para una instantánea bajo demanda, restauración de varios recursos; restauración de punto en el tiempo o restauración recurrente**

Opción	Descripción
<b>Tipo de ubicación de restauración</b>	<p>Seleccione un tipo de ubicación desde donde se restauran los datos:</p> <p><b>Sitio</b> El sitio en que se ha realizado la copia de seguridad de instantáneas. El sitio se define en el panel <b>Configuración del sistema &gt; Sitio</b>.</p> <p><b>Servicio en la nube</b> El servicio en la nube en el que se han copiado las instantáneas. El servicio en la nube se define en el panel <b>Configuración del sistema &gt; Almacenamiento de copias de seguridad &gt; Almacenamiento de objetos</b>.</p> <p><b>Servidor de repositorio</b> El servidor de repositorio en el que se han copiado las instantáneas. El servidor de repositorio se define en el panel <b>Configuración del sistema &gt; Almacenamiento de copias de seguridad &gt; Servidor de repositorio</b>.</p> <p><b>Archivado de servicio en la nube</b> El servicio de archivado en la nube en el que se copiaron las instantáneas. El servicio en la nube se define en el panel <b>Configuración del sistema &gt; Almacenamiento de copias de seguridad &gt; Almacenamiento de objetos</b>.</p> <p><b>Archivado de servidor de repositorio</b> El servidor de repositorio en el que se han copiado las instantáneas en cintas. El servidor de repositorio se define en el panel <b>Configuración del sistema &gt; Almacenamiento de copias de seguridad &gt; Servidor de repositorio</b>.</p>
<b>Seleccionar una ubicación</b>	<p>Si está restaurando datos desde un sitio, seleccione una de las siguientes ubicaciones de restauración:</p> <p><b>Demo</b> El sitio de demostración desde el que se restauran las instantáneas.</p> <p><b>Primario</b> El sitio primario desde el que se restauran las instantáneas.</p> <p><b>Secundario</b> El sitio secundario desde el que se restauran las instantáneas.</p> <p>Si está restaurando datos desde un servidor de nube o de repositorio, seleccione un servidor en el menú <b>Seleccionar una ubicación</b>.</p>
<b>Selector de fecha</b>	Para las operaciones de restauración bajo demanda, especifique un rango de fechas para mostrar las instantáneas disponibles dentro de ese rango.
<b>Punto de restauración</b>	Para las operaciones de restauración bajo demanda, seleccione una instantánea en la lista de instantáneas disponibles en el rango de fechas seleccionado.
<b>Utilizar el servidor vSnap alternativo para el trabajo de restauración</b>	Si restaura datos desde un servicio en la nube o un servidor de repositorio, seleccione este recuadro para especificar un servidor vSnap alternativo y, a continuación, seleccione un servidor desde el menú <b>Seleccionar vSnap alternativo</b> .

Opción	Descripción
	Cuando restaura datos desde un punto de restauración que se ha copiado en un servicio en la nube o un servidor de repositorio, se utiliza un servidor vSnap como pasarela para completar esta 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 copia. Para reducir la carga en el servidor vSnap, puede seleccionar un servidor vSnap alternativo para que sirva como pasarela.

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 **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.

7. 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

Restaura 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 del 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 del 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.

8. 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.

9. 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**.

10. 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 518](#)

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 476](#)

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.

# 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 copia de seguridad y restauración de bases de datos de Microsoft SQL Server” en la página 93](#).

## 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 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 IBM Spectrum Protect Plus. Esto alterará temporalmente el protocolo NTLM de Windows predeterminado.

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.

La autenticación Kerberos también requiere que el desfase horario entre el controlador de dominio y el dispositivo 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 en el 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 host de Microsoft SQL Server puede utilizar una cuenta de usuario específica para acceder a los recursos de esa instancia de SQL Server determinada.

Para completar operaciones de copia de seguridad del 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 del 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: [Error del planificador de tareas "No existe ninguna sesión de inicio de sesión especificada"](#)

## Adición de un servidor de aplicaciones SQL Server

Cuando se añade un servidor de aplicaciones SQL Server, 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 añadir un host de SQL Server, complete los pasos siguientes.

1. En el panel de navegación, pulse **Gestionar protección > Bases de datos > SQL**.
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 <a href="#">“Creación de un rol”</a> en la página 539.

## Conceptos relacionados

[“Gestión del acceso de usuarios”](#) en la página 533

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 491



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 496](#)

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 > Bases de datos > SQL**.
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 Plus y el host.

### Procedimiento

Para probar la conexión, complete los pasos siguientes:

1. En el panel de navegación, pulse **Gestionar protección > Bases de datos > SQL**.
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 de base de datos inicial, IBM Spectrum Protect Plus crea un volumen de LUN de vSnap y crea un recurso compartido NTFS en ese LUN de iSCSI. Durante las copias de seguridad incrementales, se reutiliza el volumen creado previamente. El agente de IBM Spectrum Protect Plus correlaciona el LUN con el servidor SQL Server y monta el volumen NTFS donde se ha completado la copia de seguridad. Si las copias de seguridad del registro están habilitadas, IBM Spectrum Protect Plus crea un volumen de vSnap distinto y crea un CIFS en ese volumen. Los archivos de transacciones de copia de seguridad del registro se copian en este recurso compartido según la planificación creada para la copia de seguridad del registro.

Cuando se completa el trabajo de copia de seguridad, el agente de IBM Spectrum Protect Plus desmonta el recurso compartido del servidor SQL Server y crea una instantánea de 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 18, “Gestión del acceso de usuarios”](#), en la página 533.

- El iniciador iSCSI de Microsoft debe estar habilitado y en ejecución en el servidor de Windows. Se debe habilitar 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](#).
- IBM Spectrum Protect Plus no admite la copia de seguridad del registro de los modelos de recuperación simples.
- 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](#).
- IBM Spectrum Protect Plus soporta copias de seguridad de base de datos y copias de seguridad del registro de transacciones. El nombre de producto se llena en msdb.dbo.backupset para los registros que crearon las copias de seguridad iniciadas desde IBM Spectrum Protect Plus.
- Para obtener más información sobre las copias de seguridad del registro para SQL, consulte [“Copias de seguridad de registros”](#) en la página 495.

**Nota:** Debido a las limitaciones con la infraestructura Volume Shadow Copy Services (VSS), los espacios iniciales, los espacios finales y los caracteres no imprimibles no se deben usar en los nombres de base de datos. Para obtener más información, consulte <https://support.microsoft.com/en-sg/help/2014054/backing-up-a-sql-server-database-using-a-vss-backup-application-may-fa>.

Realice las acciones siguientes:

- Registre los SQL Server a los que desea hacer copia de seguridad. Para obtener más información, consulte [“Adición de un servidor de aplicaciones SQL Server”](#) en la página 489.
- Configure las políticas de SLA. Para obtener más información, consulte [“Crear políticas de copia de seguridad”](#) en la página 169.
- 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 **Duplicaciones**. 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 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 > Bases de datos > 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**.

**Consejo:** Cuando se ejecuta un trabajo para la política de SLA seleccionada, todos los recursos asociados con esa política de SLA se incluyen en la operación de copia de seguridad. Para hacer copia de seguridad únicamente de los recursos seleccionados, puede ejecutar un trabajo bajo demanda. Un trabajo bajo demanda ejecuta inmediatamente la operación de copia de seguridad.

- Para ejecutar un trabajo de copia de seguridad bajo demanda por un único recurso, seleccione el recurso y haga clic en **Ejecutar**. Si el recurso no está asociado con una política de SLA, el botón **Ejecutar** no está disponible.
  - Para ejecutar un trabajo de copia de seguridad bajo demanda para uno o más recursos, haga clic en **Crear trabajo**, seleccione **Copia de seguridad ad hoc** y siga las instrucciones en [“Ejecución de un trabajo de copia de seguridad ad hoc”](#) en la página 517.
5. Haga clic en **Seleccionar opciones** para especificar más opciones antes de guardar el trabajo de copia de seguridad.

#### **Habilitar copia de seguridad de registro**

Seleccione esta opción para habilitar la copia de seguridad del registro de transacciones. Estos registros se utilizan para opciones de recuperación tales como operaciones de restauración de punto en el tiempo. Si las copias de seguridad del registro están habilitadas para los trabajos de copia de seguridad, las transacciones se registran de forma continua durante la copia de seguridad. Se envía una notificación si se detecta discontinuidad en las copias de seguridad de archivos de registro.

Para habilitar la creación de planificación de copia de seguridad del 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. No es necesario un área de transferencia para el proceso de copia de seguridad del registro.

Si un trabajo bajo demanda se ejecuta con la opción **Habilitar copia de seguridad del registro** habilitada, se realiza la copia de seguridad del registro. Sin embargo, cuando el trabajo se ejecuta de nuevo en una planificación, la opción se inhabilita para que la ejecución del trabajo impida la posible pérdida de segmentos en una cadena de copias de seguridad.

Seleccione una de las siguientes opciones:

#### **Copia de seguridad de los archivos de base de datos de uno en uno utilizando secuencias**


**paralelas** Seleccione esta opción para utilizar secuencias paralelas para hacer copia de seguridad de las bases de datos de forma secuencial.

#### **Copia de seguridad de los archivos de base de datos en paralelo utilizando secuencias paralelas**

Seleccione esta opción para usar secuencias paralelas para hacer copia de seguridad de las bases de datos en paralelo.

Por último, establezca **Máximo de secuencias paralelas por base de datos** seleccionando el número máximo de secuencias de datos que se va a utilizar por base de datos durante el proceso de copia de seguridad. Este valor se aplica a cada base de datos de la definición de trabajo. Se puede hacer copia de seguridad de bases de datos en paralelo si el valor de la opción se establece en **1**. Especificando varias secuencias paralelas se puede mejorar la velocidad de las copias de seguridad en algunos casos.

6. Pulse **Guardar** para guardar las opciones para los trabajos de copia de seguridad.  
El trabajo se ejecuta de acuerdo con lo definido en la política de SLA o bien se puede ejecutar manualmente desde la ventana **Trabajos y operaciones**.

7. Para configurar opciones adicionales, pulse el icono de portapapeles **Opciones de política**  que está asociado al trabajo en la sección **Estado de política de SLA**. Establezca las opciones de política adicionales siguientes:

#### **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 ejecuta 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 COMPLETED. Si un script posterior se completa con un código de retorno distinto de cero, el estado de la tarea de script posterior se notifica como COMPLETED.

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 FAILED.

#### **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 de base de datos 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:

<b>Acción</b>	<b>Cómo</b>
Cree una definición de trabajo de Restauración de SQL.	Consulte <a href="#">“Restauración de datos de SQL Server” en la página 496</a> .

#### **Conceptos relacionados**

[“Configuración de scripts para las operaciones de copia de seguridad y restauración” en la página 518](#)

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 bajo demanda” en la página 512](#)

Puede ejecutar cualquier trabajo bajo demanda, incluso si el trabajo se ha establecido para que se ejecute en una planificación.

### **Copias de seguridad de registros**

Los archivos de registro archivados para bases de datos contienen datos de transacciones comprometidas. Estos datos de transacción se pueden utilizar para ejecutar un proceso de recuperación en avance como parte de una operación de restauración. El uso de copias de seguridad del registro de archivado mejora el objetivo de punto de recuperación para los datos. Asegúrese de que las copias de seguridad del registro están habilitadas en los trabajos de copia de seguridad para permitir la recuperación en avance cuando restaura datos de Microsoft SQL Server.

Cuando habilita las copias de seguridad del registro por primera vez, debe ejecutar un trabajo de copia de seguridad para la política de SLA para activar el archivado de registros en IBM Spectrum Protect Plus en la base de datos. Esta copia de seguridad crea un volumen independiente en el repositorio de vSnap y el volumen se monta de forma persistente en el servidor de aplicaciones SQL. El volumen permanece montado en el servidor de aplicaciones SQL a menos que se haya borrado la opción **Habilitar copia de seguridad de registro** y se ejecute un nuevo trabajo de copia de seguridad. Para habilitar las copias de seguridad del registro, siga las instrucciones de [“Copia de seguridad de datos de SQL Server”](#) en la [página 491](#).

Revise los criterios siguientes antes de configurar las operaciones de copia de seguridad del registro:

- Para ejecutar copias de seguridad del registro, el usuario agente de SQL Server debe ser un administrador local de Windows. Este usuario debe tener el permiso sysadmin para gestionar trabajos de agente de SQL Server. El agente utilizará dicha cuenta de administrador para habilitar y acceder a los trabajos de copia de seguridad del registro. Para cada instancia de SQL Server, el usuario agente de SQL Server también debe ser el usuario del servicio de SQL Server y de la cuenta de servicio de agente de SQL Server. Esta regla es verdadera para que cada instancia de SQL Server esté protegida.
- IBM Spectrum Protect Plus no da soporte a operaciones de copia de seguridad del registro para modelos de recuperación simples.
- Evite configurar copias de seguridad del registro para una única base de datos SQL utilizando varios trabajos de copia de seguridad. Los registros se truncan durante las operaciones de copia de seguridad del registro. Si se añade una única base de datos SQL a varias definiciones de trabajo con la copia de seguridad del registro habilitada, una copia de seguridad del registro de un trabajo truncará un registro antes de que el siguiente trabajo realice una copia de seguridad. Este solapamiento puede provocar que fallen los trabajos de restauración de punto en el tiempo.
- Antes de que los registros se copien en el repositorio de vSnap, IBM Spectrum Protect Plus utiliza la carpeta de copia de seguridad que se ha configurado para la instancia de SQL Server como el área de transferencia para recopilar registros. El volumen donde se encuentra esta carpeta debe tener espacio suficiente para contener 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 en SQL Server Management Studio (SSMS).
- IBM Spectrum Protect Plus soporta copias de seguridad de base de datos y copias de seguridad del registro de transacciones. El nombre de producto se llena en msdb . dbo . backupset para los registros que crearon las copias de seguridad iniciadas desde IBM Spectrum Protect Plus.
- IBM Spectrum Protect Plus trunca automáticamente las copias de seguridad del registro 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, los registros no se truncan y deben gestionarse por separado.
- Cuando se completa un trabajo de copia de seguridad de SQL con copias de seguridad del registro habilitadas, se depuran todos los registros de transacciones hasta la finalización de ese trabajo desde SQL Server. La depuración del registro solo se produce si el trabajo de copia de seguridad de SQL se completa correctamente. Si no se realiza una copia de seguridad de las copias de seguridad del registro durante una reejecución del trabajo, no se produce la depuración de registro.
- Una operación de copia de seguridad del registro para una base de datos de SQL Server Always On secundaria puede fallar con el siguiente error:

La copia de seguridad del 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 se produce este error, cambie la preferencia de copia de seguridad del grupo de disponibilidad a **Primaria**. Después se realiza una copia de seguridad de los registros de la réplica primaria. Después de que se haya completado correctamente una copia de seguridad del registro de la réplica primaria, se puede cambiar la preferencia de copia de seguridad.

- Si se sobrescribe una base de datos de origen, todos los registros de transacciones anteriores hasta ese punto se colocan en un directorio de *condensación* después de 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.

## 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 491.
- 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 18, “Gestión del acceso de usuarios”](#), en la página 533.
- 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 del registro del último momento específico que crea IBM Spectrum Protect Plus deben restaurarse si la copia de seguridad del 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 el apartado <https://docs.microsoft.com/en-us/sql/t-sql/language-reference?view=sql-server-2017>.

- 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 > Bases de datos > SQL**. Haga clic en **Crear trabajo** y, a continuación, seleccione **Restaurar** para abrir el asistente **Restaurar**.

#### Sugerencias:

- También puede abrir el asistente pulsando **Trabajos y operaciones > Crear trabajo > Restaurar > SQL**.
  - Para obtener un resumen en ejecución de las selecciones en el asistente, pulse **Vista previa de restauración** en el panel de navegación del asistente.
  - El asistente se abre en la modalidad de configuración predeterminada. Para ejecutar el asistente en modalidad de configuración avanzada, seleccione **Configuración avanzada**. Con la modalidad de configuración avanzada, puede establecer más opciones para el trabajo de restauración.
2. En la página **Seleccionar origen**, realice 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**, seleccione el tipo de trabajo de restauración que desea crear:
- Bajo demanda: instantánea**  
Ejecuta una operación de restauración puntual. 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.
4. Complete los campos de la página **Instantánea de origen** y pulse **Siguiente** para continuar.
- Los campos que se muestran dependen del número de elementos seleccionados en la página **Seleccionar origen** y en el tipo de restauración. Algunos campos tampoco se muestran hasta que se selecciona un campo relacionado.

**Campos que se muestran para una instantánea bajo demanda, una única restauración de recursos**

Opción	Descripción
<b>Rango de fechas</b>	Especifique un rango de fechas para mostrar las instantáneas disponibles dentro de ese intervalo.
<b>Tipo de almacenamiento de copias de seguridad</b>	<p>Todas las copias de seguridad del rango de fechas seleccionado se listan en filas que muestran la hora a la que se ha realizado la operación de copia de seguridad y la política de acuerdo de nivel de servicio (SLA) para la copia de seguridad. Seleccione la fila que contiene la hora de la copia de seguridad y la política de SLA que desea y, a continuación, realice una de las siguientes acciones:</p> <ul style="list-style-type: none"> <li>Haga clic en el tipo de almacenamiento de copia de seguridad desde el que desea restaurar. Los tipos de almacenamiento que se muestran dependen de los tipos disponibles en el entorno y se muestran en el orden siguiente: <ul style="list-style-type: none"> <li><b>Copia de seguridad</b> Restaura los datos de los que se ha hecho copia de seguridad en un servidor vSnap.</li> <li><b>Réplica</b> Restaura datos que se replican en un servidor vSnap.</li> <li><b>Almacenamiento de objetos</b> Restaura los datos que se copian en un servicio en la nube o en un servidor de repositorio.</li> <li><b>Archivado</b> Restaura los datos que se copian en un archivo de servicio en la nube o en un archivo de servidor de repositorio (cinta).</li> </ul> </li> <li>Haga clic en cualquier sitio en la fila. El primer tipo de copia de seguridad que se muestra secuencialmente desde la izquierda de la fila se selecciona de forma predeterminada. Por ejemplo, si se muestran los tipos de almacenamiento <b>Copia de seguridad</b>, <b>Réplica</b> y <b>Archivado</b>, <b>Copia de seguridad</b> se selecciona de forma predeterminada.</li> </ul>
<b>Utilizar el servidor vSnap alternativo para</b>	Si restaura datos desde un servicio en la nube o un servidor de repositorio, seleccione este recuadro para especificar un servidor vSnap alternativo y, a continuación, seleccione un servidor desde el menú <b>Seleccionar vSnap alternativo</b> .



Opción	Descripción
<b>el trabajo de restauración</b>	Cuando restaura datos desde un punto de restauración que se ha copiado en 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 copia. Para reducir la carga en el servidor vSnap, puede seleccionar un servidor vSnap alternativo para que sirva como pasarela.

**Campos que se muestran para una instantánea bajo demanda, restauración de varios recursos; restauración de punto en el tiempo o restauración recurrente**

Opción	Descripción
<b>Tipo de ubicación de restauración</b>	<p>Seleccione un tipo de ubicación desde donde se restauran los datos:</p> <p><b>Sitio</b> El sitio en que se ha realizado la copia de seguridad de instantáneas. El sitio se define en el panel <b>Configuración del sistema &gt; Sitio</b>.</p> <p><b>Servicio en la nube</b> El servicio en la nube en el que se han copiado las instantáneas. El servicio en la nube se define en el panel <b>Configuración del sistema &gt; Almacenamiento de copias de seguridad &gt; Almacenamiento de objetos</b>.</p> <p><b>Servidor de repositorio</b> El servidor de repositorio en el que se han copiado las instantáneas. El servidor de repositorio se define en el panel <b>Configuración del sistema &gt; Almacenamiento de copias de seguridad &gt; Servidor de repositorio</b>.</p> <p><b>Archivado de servicio en la nube</b> El servicio de archivado en la nube en el que se copiaron las instantáneas. El servicio en la nube se define en el panel <b>Configuración del sistema &gt; Almacenamiento de copias de seguridad &gt; Almacenamiento de objetos</b>.</p> <p><b>Archivado de servidor de repositorio</b> El servidor de repositorio en el que se han copiado las instantáneas en cintas. El servidor de repositorio se define en el panel <b>Configuración del sistema &gt; Almacenamiento de copias de seguridad &gt; Servidor de repositorio</b>.</p>
<b>Seleccionar una ubicación</b>	<p>Si está restaurando datos desde un sitio, seleccione una de las siguientes ubicaciones de restauración:</p> <p><b>Demo</b> El sitio de demostración desde el que se restauran las instantáneas.</p> <p><b>Primario</b> El sitio primario desde el que se restauran las instantáneas.</p> <p><b>Secundario</b> El sitio secundario desde el que se restauran las instantáneas.</p> <p>Si está restaurando datos desde un servidor de nube o de repositorio, seleccione un servidor en el menú <b>Seleccionar una ubicación</b>.</p>
<b>Selector de fecha</b>	Para las operaciones de restauración bajo demanda, especifique un rango de fechas para mostrar las instantáneas disponibles dentro de ese rango.
<b>Punto de restauración</b>	Para las operaciones de restauración bajo demanda, seleccione una instantánea en la lista de instantáneas disponibles en el rango de fechas seleccionado.

Opción	Descripción
<b>Utilizar el servidor vSnap alternativo para el trabajo de restauración</b>	<p>Si restaura datos desde un servicio en la nube o un servidor de repositorio, seleccione este recuadro para especificar un servidor vSnap alternativo y, a continuación, seleccione un servidor desde el menú <b>Seleccionar vSnap alternativo</b>.</p> <p>Cuando restaura datos desde un punto de restauración que se ha copiado en un servicio en la nube o un servidor de repositorio, se utiliza un servidor vSnap como pasarela para completar esta 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 copia. Para reducir la carga en el servidor vSnap, puede seleccionar un servidor vSnap alternativo para que sirva como pasarela.</p>

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.

Opcionalmente, 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. Al cambiar el nombre de una base de datos SQL, se aplica la regla de denominación para identificadores. Para obtener más información, consulte <https://docs.microsoft.com/en-us/sql/relational-databases/databases/database-identifiers>.

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 **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.

7. 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 del registro 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

Restaura 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 del 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.

#### Modalidad de espera

Cuando se selecciona la opción de Modalidad en espera, esto deja la base de datos SQL en un estado de solo lectura. Las transacciones no confirmadas se deshacen y se guardan en un archivo de deshacer que se puede utilizar posteriormente para poner la base de datos en línea. Las transacciones almacenadas en el archivo en espera se pueden aplicar cuando la base de datos está lista para ser recuperada.

**Nota:** Es posible que la ubicación de una base de datos restaurada utilizando la modalidad en espera esté en la ubicación de la base de datos original al visualizar la base de datos en SQL Management Studio. La ubicación será realmente el directorio especificado por el usuario para una restauración en modalidad de producción y `C:\ProgramData\mnt\uuid_subdirectory` para una restauración en modalidad de prueba.

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 del 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.

8. 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.

9. 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**.

10. 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 518](#)

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 SQL Server” en la página 489](#)

Cuando se añade un servidor de aplicaciones SQL Server, 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.

[“Copia de seguridad de datos de SQL Server” en la página 491](#)

Utilice un trabajo de copia de seguridad para realizar copias de seguridad de entornos SQL Server con instantáneas.



---

## Capítulo 15. 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 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 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 hay disponible una política de SLA adecuada. 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 actualizar el sistema operativo, siga las instrucciones que se indican en [“Creación de una política de SLA para hipervisores, bases de datos y sistemas de archivos”](#) en la [página 244](#).

**Restricción:** No puede seleccionar el servidor de vSnap incorporado como destino de la política de SLA para hacer una copia de seguridad de IBM Spectrum Protect Plus. El servidor de vSnap incorporado se denomina localhost y se instala automáticamente cuando inicialmente el dispositivo IBM Spectrum Protect Plus se despliega. Seleccione un servidor vSnap externo secundario como destino cuando crea la política de SLA para hacer copia de seguridad de IBM Spectrum Protect Plus.

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.
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 178](#).

---

### Restauración de la aplicación de IBM Spectrum Protect Plus

Restaurar los valores de configuración, los puntos de restauración 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, el recurso de nube o el servidor de repositorio debe estar registrado en la ubicación de IBM Spectrum Protect Plus alternativa.

Cuando se inicia un trabajo de restauración de catálogo, se asigna un identificador de sesión de trabajo (ID). Durante la fase inicial, el trabajo se podrá supervisar en la IU de IBM Spectrum Protect Plus en la pantalla de gestión de trabajos hasta que el paso de recuperación inicie la restauración de base de datos interna. Una vez que el trabajo entra en este estado, IBM Spectrum Protect Plus ya no está disponible. Durante esta fase, la información de registro se graba en la ubicación: `/data/log/adminconsole/managedb-catalogrestore-time.log`, donde *time* es el tiempo Epoch. Los datos contenidos en este registro se relacionan con la restauración del catálogo de configuración y recuperación de mongo. Una vez completado el proceso, se iniciará el servicio `virgo` y los datos se grabarán en el registro `virgo`. Cuando se completa el trabajo, la interfaz de usuario de IBM Spectrum Protect Plus es de nuevo accesible.

## 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 las 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.

### Conceptos relacionados

[“Tipos de trabajo” en la página 509](#)

Los trabajos se utilizan para ejecutar operaciones de copia de seguridad, restauración, mantenimiento e inventario en IBM Spectrum Protect Plus.



## Caducidad de las sesiones de trabajo


Puede hacer caducar una sesión de trabajo alterando temporalmente los valores de retención de la instantánea que se asignaron durante la creación de la copia de seguridad.

### Acerca de esta tarea

La caducidad de una sesión de trabajo no eliminará una instantánea y el punto de recuperación relacionado si la instantánea está bloqueada por una relación de réplica o copia. Ejecute el trabajo habilitado para la réplica o la copia para cambiar el bloqueo a 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. Como alternativa, en la pestaña Máquinas virtuales / Bases de datos, seleccione Aplicaciones o Hipervisores para buscar la entrada de catálogo deseada especificando el nombre. Los nombres se pueden buscar escribiendo un texto parcial, usando un asterisco (\*) como único carácter comodín o usando un signo de interrogación (?) para la coincidencia de patrón.  
  
Para obtener más información sobre el uso de la función de búsqueda, consulte [Apéndice A, “Directrices de búsqueda”](#), en la página 567.
3. Si está buscando en la pestaña Sesiones de copia de seguridad, utilice filtros para ajustar la búsqueda entre los tipos de trabajo y el rango 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**.

## Supresión de metadatos de recursos del catálogo de IBM Spectrum Protect Plus

Cuando ejecuta un trabajo de inventario, se añaden recursos al catálogo de IBM Spectrum Protect Plus. Para liberar espacio en el catálogo, puede hacer caducar los datos de los puntos de restauración asociados con los recursos.

### 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 tipo de recursos y, a continuación, especifique una serie de búsqueda para buscar un recurso por nombre.

Para obtener más información sobre el uso de la función de búsqueda, consulte [Apéndice A, “Directrices de búsqueda”](#), en la página 567.

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 de catálogo asociados con el recurso se eliminan del catálogo.

#### **Conceptos relacionados**

[“Tipos de trabajo” en la página 509](#)

Los trabajos se utilizan para ejecutar operaciones de copia de seguridad, restauración, mantenimiento e inventario en IBM Spectrum Protect Plus.

---

## Capítulo 16. Gestión de trabajos y operaciones

Puede gestionar y supervisar trabajos en la ventana **Trabajos y operaciones**. También puede configurar scripts para que se ejecuten antes o después de los trabajos.

### 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, inventario y de informes están predefinidos y no se pueden modificar. Sin embargo, puede modificar las planificaciones de los trabajos de mantenimiento, inventario y de informes.

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.

También puede ejecutar trabajos de copia de seguridad para un único recurso o varios recursos seleccionados que están asociados con una política de SLA en lugar de hacer una copia de seguridad de todos los recursos asociados con la política.

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.

Los trabajos de restauración se han ejecutado en una planificación o bajo demanda.

En los trabajos planificados, el nombre del trabajo lo define el usuario que crea el trabajo.

En los trabajos bajo demanda, el nombre del trabajo `onDemandRestore` se genera automáticamente cuando se ejecuta el 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`.

### Informe

Un trabajo de informes ejecuta un informe planificado. El nombre del trabajo es el nombre del informe precedido por `Report_`.

Los nombres de informes son similares al ejemplo siguiente:

```
Report_VM Backup History
```

### Conceptos relacionados

[“Protección de sistemas virtualizados” en la página 257](#)

Debe registrar los sistemas virtualizados que desee proteger en IBM Spectrum Protect Plus y, a continuación, crear trabajos para realizar copias de seguridad y restauración de los recursos asociados con los sistemas.

[“Protección de bases de datos” en la página 375](#)

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.

### Tareas relacionadas

[“Creación de una política de SLA para hipervisores, bases de datos y sistemas de archivos” en la página 244](#)

Puede crear políticas de acuerdo de nivel de servicio (SLA) personalizadas para definir políticas de frecuencia de copia de seguridad, de retención, de réplica y de copia que sean específicas del entorno.

[“Ejecución de un trabajo de copia de seguridad ad hoc” en la página 517](#)

Con un trabajo de copia de seguridad ad hoc, puede seleccionar uno o más recursos asociados con una política de SLA y ejecutar una operación de copia de seguridad bajo demanda para esos recursos.

## Creación de trabajos y planificaciones de trabajos

---

El método para crear trabajos y planificaciones de trabajos depende del tipo de trabajo.

Puede crear trabajos y planificaciones para trabajos de copia de seguridad y restauración. La tabla siguiente describe los trabajos de copia de seguridad y restauración disponibles y proporciona enlaces a los pasos necesarios para crear los trabajos y las planificaciones de trabajos o ejecutar los trabajos bajo demanda.

Los trabajos de mantenimiento se crean de forma predeterminada. Los trabajos de inventario y de informe se crean automáticamente cuando se ejecuta una operación de inventario o cuando se planifica un informe.

Tipo de trabajo	Descripción	Cómo crear el trabajo
Copia de seguridad	Puede crear una definición de trabajo y asignar una o más políticas de acuerdo de nivel de servicio (SLA) a esa definición. La definición de trabajo define los recursos de copia de seguridad y la política de SLA define la planificación, los destinos y otras opciones para la operación de copia de seguridad.	<p>Consulte los temas que contienen instrucciones para realizar una copia de seguridad de datos por tipo de recurso en las secciones siguientes:</p> <ul style="list-style-type: none"> <li>• <a href="#">Capítulo 10, “Protección de sistemas virtualizados”, en la página 257</a></li> <li>• <a href="#">Capítulo 11, “Protección de sistemas de archivos”, en la página 309</a></li> <li>• <a href="#">Capítulo 12, “Protección de contenedores”, en la página 329</a></li> <li>• <a href="#">Capítulo 13, “Protección de datos en sistemas en nube”, en la página 369</a></li> <li>• <a href="#">Capítulo 14, “Protección de bases de datos”, en la página 375</a></li> </ul> <p>Por ejemplo, el tema de copia de seguridad para VMware es <a href="#">“Copia de seguridad de datos de VMware” en la página 262</a>.</p>
Copia de seguridad ad hoc	Cuando se ejecuta un trabajo para la política de SLA seleccionada, todos los recursos asociados con esa política de SLA se incluyen en la operación de copia de seguridad. Si desea hacer copia de seguridad únicamente de los recursos seleccionados utilizando una política de SLA seleccionada, puede ejecutar un trabajo ad hoc, que ejecuta la operación de copia de seguridad inmediatamente.	Consulte <a href="#">“Ejecución de un trabajo de copia de seguridad ad hoc” en la página 517</a> .
Restaurar	<p>Después de haber ejecutado un trabajo de copia de seguridad al menos una vez, puede ejecutar un trabajo de restauración para restaurar los datos.</p> <p>Puede crear un trabajo de restauración que se ejecuta en una planificación o que se ejecuta bajo demanda.</p>	<p>Consulte los temas que contienen instrucciones para restaurar datos por tipo de recurso en las secciones siguientes:</p> <ul style="list-style-type: none"> <li>• <a href="#">Capítulo 10, “Protección de sistemas virtualizados”, en la página 257</a></li> <li>• <a href="#">Capítulo 11, “Protección de sistemas de archivos”, en la página 309</a></li> <li>• <a href="#">Capítulo 12, “Protección de contenedores”, en la página 329</a></li> <li>• <a href="#">Capítulo 13, “Protección de datos en sistemas en nube”, en la página 369</a></li> <li>• <a href="#">Capítulo 14, “Protección de bases de datos”, en la página 375</a></li> </ul> <p>Por ejemplo, el tema de restauración para VMware es <a href="#">“Restauración de datos de VMware” en la página 273</a>.</p>

#### Conceptos relacionados

[“Tipos de trabajo” en la página 509](#)

Los trabajos se utilizan para ejecutar operaciones de copia de seguridad, restauración, mantenimiento e inventario en IBM Spectrum Protect Plus.

#### Tareas relacionadas

“Creación de una política de SLA para hipervisores, bases de datos y sistemas de archivos” en la página 244

Puede crear políticas de acuerdo de nivel de servicio (SLA) personalizadas para definir políticas de frecuencia de copia de seguridad, de retención, de réplica y de copia que sean específicas del entorno.


## Inicio de trabajos bajo demanda

---

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, haga clic en el icono de menú de acciones  y, a continuación, pulse **Iniciar**.

El trabajo se inicia y se añade a la pestaña **Trabajos en ejecución**.

#### Qué hacer a continuación

Para ver el registro de trabajo para el trabajo, seleccione el trabajo en la pestaña **Trabajos en ejecución** y haga clic en **Registro de trabajo**. Para descargar el registro para el trabajo, pulse **Download.zip**.

Para ver todos los trabajos que se están ejecutando o que se han ejecutado simultáneamente con el trabajo, haga clic en **Trabajos simultáneos**.

## Visualización de trabajos

---

Vea información sobre el estado de los trabajos en ejecución y el estado general de los trabajos que se completaron correctamente o con fallos o advertencias.

#### Procedimiento

Para ver trabajos, complete los pasos siguientes:

1. En el panel de navegación, haga clic en **Trabajos y operaciones**.
2. En la página **Trabajos en ejecución**, vea el estado de los trabajos que se están ejecutando actualmente, como se muestra en el ejemplo siguiente.

**Jobs and Operations**

Running Jobs | Job History | Active Resources | Schedule

7 Total Jobs | 0 Backup | 0 Inventory | 0 Maintenance | 7 Restore

CPU Usage: 4% (IBM Spectrum Protect Plus Host Machine)

Sort By: Start | Search by name...

**onDemandRestore\_1590032799201**  
SQL  
Type: Restore | Activity: Resource active  
Start Time: May 20, 2020 8:46:40 PM  
Duration: 0h 7m 24s  
Databases Completed: 1/1

**onDemandRestore\_1589411636416**  
SQL  
Type: Restore | Activity: Resource active  
Start Time: May 13, 2020 4:13:56 PM  
Duration: 3h 24m 16s  
Databases Completed: 1/1

**onDemandRestore\_1589257013247**

**onDemandRestore**  
Type: Restore | Start Time: May 20, 2020 8:46:40 PM  
Job Log | Concurrent Jobs | Download .zip  
Failed: 0 | Success: 1 | Total: 1

Status	Time	ID	Description
Summary	May 20, 2020 8:46:40 PM	CTGGA2398	Starting job for policy onDemandRestore_1590032799201 (ID:1654). id -> 1590032800093. IBM Spectrum Protect Plus version 10.1.6-1948.
Detail	May 20, 2020 8:46:41 PM	CTGGA2109	Policy has (1) destination database mappings.
Detail	May 20, 2020 8:46:41 PM	CTGGA1527	Resolved policy to (restore).

3. Para ver los trabajos completado, haga clic en **Historial de trabajo**.

La cinta a lo largo de esta pantalla muestra el estado de los trabajos históricos. Utilice el filtro para definir la duración del historial de trabajo que se va a visualizar.

**Jobs and Operations**

Running Jobs | Job History | Active Resources | Schedule

51.14% Success Rate | 2710 Total Jobs | 741 Failed | 583 Warning | 1386 Successful

Job history period: Last 30 days

Sort By: Start | Search by name...

**vmware\_SLA1\_1object\_policy**  
Type: Backup | Status: Partial  
Start Time: Jun 6, 2020 3:00:01 PM  
Duration: 0h 2m 23s  
Total VMs: 2

**vmware\_SLA3\_1object\_policy**  
Type: Backup - Copy | Status: Failed  
Start Time: Jun 6, 2020 3:00:01 PM  
Duration: 0h 0m 8s

**sql\_bigdb-cd2-dedup**  
Type: Backup | Status: Failed

**vmware\_SLA1\_1object\_policy**  
Type: Backup | Start Time: Jun 6, 2020 3:00:01 PM  
Progress | Job Log | Concurrent Jobs | Download .zip  
Failed: 1 | Success: 1 | Total: 2

Status	Time	ID	Description
Summary	Jun 6, 2020 3:00:00 PM	CTGGA2399	Starting job for policy BACKUP with job name vmware_SLA1_1object_policy (ID:1361). id -> 1591480800138. IBM Spectrum Protect Plus version 10.1.6-1972.
Detail	Jun 6, 2020 3:00:02 PM	CTGGA0171	Job options : retention (type:days count:1)
Detail	Jun 6, 2020 3:00:02 PM	CTGGA0062	Discovering virtual machines that need to be protected

4. Para ver los recursos activos en su entorno, haga clic en **Recursos activos**.

Muestra los recursos activos de la aplicación y el hipervisor. En el caso de los hipervisores, los campos visualizados son recurso, tipo, destino y última actualización. También se visualiza la información de etiqueta de disco virtual si el origen de destino es un disco virtual.

5. Para ver la planificación general para todos los trabajos, pulse **Planificar**.

Mediante el menú **Acciones**, puede elegir iniciar un trabajo o pausar una planificación. También puede editar algunas planificaciones de trabajos recurrentes y de mantenimiento haciendo clic en el icono de planificación y guardando los cambios. Para editar un trabajo de restauración, haga clic en el icono de edición para ese trabajo.

6. Opcional: Para descargar un registro de trabajo y otros archivos que reflejan la información mostrada en la ventana **Trabajos y operaciones**, haga clic en **Descargar.zip**.

## Visualización del progreso del trabajo de copia de seguridad en el nivel de recurso

Vea el estado de los recursos individuales en un trabajo de copia de seguridad. La visualización del trabajo en el nivel de recurso le permite determinar el rendimiento de copia de seguridad de cada

recurso. Esta característica proporciona información para ayudarle a optimizar el rendimiento de copia de seguridad y a resolver posibles problemas.

### Acerca de esta tarea

Esta característica está disponible solo para trabajos de copia de seguridad. El progreso de los recursos individuales no se muestra para otros tipos de trabajo.


### Procedimiento

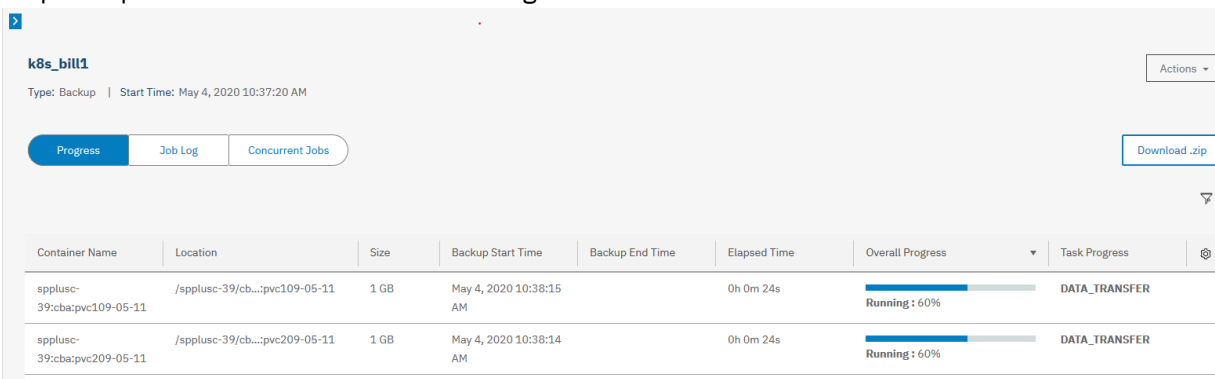
Para ver el progreso de recursos individuales en un trabajo de copia de seguridad, complete los pasos siguientes:

1. En el panel de navegación, haga clic en **Trabajos y operaciones**.
2. Haga clic en **Trabajos en ejecución** para trabajos que están en curso o **Historial de trabajos** para trabajos que se han completado.
3. Seleccione el trabajo que contiene los recursos que desea ver y, a continuación, haga clic en **Progreso**.

La información sobre cada recurso se muestra en una tabla. Esta información incluye el progreso de la operación de copia de seguridad para cada recurso en la columna **Progreso general**.

Si es aplicable para el tipo de recurso, la tarea que se ejecuta para la operación de copia de seguridad también se muestra en la columna **Progreso de la tarea**. Esta columna no se incluye para algunos tipos de recurso, como hipervisores, cuyas operaciones de copia de seguridad no incluyen tareas individuales.


El ejemplo siguiente muestra la información de progreso para un trabajo de copia de seguridad de Kubernetes. En este ejemplo, el progreso de copia de seguridad general para el recurso es del 60% como muestra la columna **Progreso general**. La tarea de copia de seguridad actual que se está ejecutando, la transferencia de datos, se muestra en la columna **Progreso de tarea**. La tabla se ha ampliado pulsando el  con forma de triángulo.




Container Name	Location	Size	Backup Start Time	Backup End Time	Elapsed Time	Overall Progress	Task Progress
spplusc-39:cbapvc109-05-11	/spplusc-39/cb...:pvc109-05-11	1 GB	May 4, 2020 10:38:15 AM		0h 0m 24s	Running : 60%	DATA_TRANSFER
spplusc-39:cbapvc209-05-11	/spplusc-39/cb...:pvc209-05-11	1 GB	May 4, 2020 10:38:14 AM		0h 0m 24s	Running : 60%	DATA_TRANSFER

Figura 51. Visualización de la información de trabajo en el nivel de recurso

4. Opcional: Puede personalizar las columnas que se muestran en la tabla y filtrar los recursos que se muestran por estado de progreso.

Para personalizar las columnas, haga clic en el icono de valores  para seleccionar las columnas. De forma predeterminada, se muestran todas las columnas.

Para filtrar los recursos por estado de progreso, haga clic en el icono de filtro  y seleccione los valores de estado que desee. Por ejemplo, si desea ver solo los recursos que están en proceso de ejecución, seleccione la casilla de verificación **En ejecución** y borre las otras.

## Visualización de los registros de trabajo

Para cada ejecución del trabajo, se proporciona un registro que muestra información como el estado del trabajo, la hora de inicio y de finalización del trabajo y un mensaje que se asocia al trabajo.



## Procedimiento

Para ver los registros de trabajo, complete los pasos siguientes:

1. En el panel de navegación, haga clic en **Trabajos y operaciones**
2. Haga clic en **Trabajos en ejecución** para trabajos que están en curso o **Historial de trabajos** para trabajos que se han completado.
3. Seleccione un trabajo y haga clic en **Registro de trabajo**.

Se muestra el registro de trabajo para el trabajo seleccionado.

## Visualización de trabajos simultáneos

A los trabajos que solapan otros trabajos se los conoce como trabajos simultáneos. Puede ver trabajos que se están ejecutando o que se han ejecutado simultáneamente con otro trabajo.

### Procedimiento

Para ver los trabajos que se están ejecutando o que se han ejecutado con otro trabajo, complete los pasos siguientes:

1. En el panel de navegación, haga clic en **Trabajos y operaciones**
2. Haga clic en **Trabajos en ejecución** para trabajos que están en curso o **Historial de trabajos** para trabajos que se han completado.
3. Seleccione un trabajo y pulse **Trabajos simultáneos**.

Para los trabajos que se muestran en la pestaña **Trabajos en ejecución**, se muestra una lista de todos los trabajos que se están ejecutando simultáneamente con el trabajo seleccionado. Para los trabajos que se muestran en la pestaña **Historial de trabajos**, se muestra una lista de todos los trabajos que se han ejecutado simultáneamente con el trabajo seleccionado.



**Restricción:** Varios trabajos de copia de seguridad no pueden realizar una copia de seguridad del mismo recurso al mismo tiempo. Si varios trabajos comparten un recurso o recursos, el trabajo que procesa el recurso se ejecutará primero y los demás trabajos que se inician durante el mismo periodo de tiempo fallarán.

## Cómo poner en pausa y reanudar trabajos

Puede poner en pausa y reanudar un trabajo planificado. 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 desea poner en pausa y haga clic en el icono de menú de acciones  y, a continuación, haga clic en **Pausar planificación**.
3. Para reanudar la planificación de trabajos, haga clic en el  y, a continuación, haga clic en **Liberar planificación**.

## Edición de trabajos y planificaciones de trabajos

Puede editar las opciones de trabajo y planificar algunos tipos de trabajo.

### Acerca de esta tarea

Para los trabajos de restauración, puede editar las opciones de trabajo utilizando el asistente **Restaurar**.

Para los siguientes tipos de trabajo, puede editar la planificación de trabajos:



- Restaurar (trabajos recurrentes)

- Inventario
- Informe
- Mantenimiento

### Procedimiento

Para editar un trabajo o una planificación de trabajos, complete los pasos siguientes:

1. En el panel de navegación, pulse **Trabajos y operaciones**, a continuación, pulse la pestaña **Planificación**.
2. Pulse el icono de edición o de planificación.

Opción	Descripción
	Haga clic en este icono de edición para abrir el asistente <b>Restaurar</b> y cambie las opciones para el trabajo. Siga las instrucciones para utilizar el asistente en el tema de restauración de recursos aplicable en Capítulo 10, “Protección de sistemas virtualizados”, en la página 257 y Capítulo 14, “Protección de bases de datos”, en la página 375.
	Haga clic en este icono de edición para cambiar la planificación de trabajos.

## 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 **Trabajos en ejecución**.
2. Haga clic en el menú **Acciones** asociado con el trabajo y, a continuación, seleccione **Cancelar**.

## Supresión de trabajos


Puede suprimir un trabajo de restauración o informe que tiene un estado de DESOCUPADO.

### Acerca de esta tarea

Este procedimiento solo se aplica a los trabajos de restauración y de informe. Para suprimir un trabajo de copia de seguridad, debe suprimir la política de acuerdo de nivel de servicio (SLA) asociada con dicho trabajo.

### Procedimiento

Para suprimir un trabajo de restauración o informe, complete los pasos siguientes:

1. En el panel de navegación, pulse **Trabajos y operaciones**, a continuación, pulse la pestaña **Planificación**.
2. Pulse el icono Suprimir  asociado con el trabajo.

## 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.

**Consejo:** 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 del registro, las copias de seguridad del registro no se inhabilitan cuando se utiliza la función de volver a ejecutar. Las copias de seguridad del 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, haga clic en **Volver a ejecutar**.  
Si no se puede volver a ejecutar el trabajo de copia de seguridad, la opción **Volver a ejecutar** no estará disponible.

### Resultados

Todas las opciones de SLA y las exclusiones asociadas al trabajo original se incluyen en la operación de volver a ejecutar. Cualquier opción o cambio de exclusión que aplique después de la última operación de copia de seguridad parcial se ignora. Si el trabajo que se vuelve a ejecutar se completa correctamente, el resumen del trabajo se actualiza para mostrar el éxito de la operación.

## Ejecución de un trabajo de copia de seguridad ad hoc

---

Con un trabajo de copia de seguridad ad hoc, puede seleccionar uno o más recursos asociados con una política de SLA y ejecutar una operación de copia de seguridad bajo demanda para esos recursos.

### Acerca de esta tarea

Esta característica asocia la política de SLA seleccionada y los recursos en un trabajo ad hoc para la ejecución de una operación de copia de seguridad bajo demanda inmediata. Esto no cambia las asignaciones de política de SLA para recursos asociados con trabajos planificados.


## Procedimiento


Para ejecutar un trabajo de copia de seguridad ad hoc, complete los pasos siguientes:

1. En el panel de navegación, haga clic en **Trabajos y operaciones** > **Crear trabajo**.
2. Seleccione **Copia de seguridad ad hoc** para abrir el asistente de copia de seguridad.

### Sugerencias:

- También puede abrir el asistente desde las páginas de gestión de aplicación o hipervisor individuales haciendo clic en **Gestionar protección** > **Hipervisores** o **Gestionar protección** > **Aplicaciones**.
  - Para obtener un resumen de ejecución de las selecciones en el asistente, haga clic en **Vista previa de copia de seguridad** en el panel de navegación en el asistente.
3. En la página **Tipo de origen**, haga clic en el hipervisor o la aplicación para los recursos que desea incluir en el trabajo.
  4. En la página **Seleccionar política de SLA**, seleccione la política de SLA y, a continuación, haga clic en **Siguiente**.
  5. En la página **Seleccionar origen**, realice las acciones siguientes:
    - a) Revise los recursos disponibles.

Puede especificar todo o parte de un nombre en el cuadro de filtro para ubicar los recursos 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) Haga clic en el icono de signo más  al lado del recurso que desea añadir al trabajo.

Para eliminar un recurso de la lista, haga clic en el icono de signo menos  al lado del recurso.
    - c) Pulse **Siguiente**.
  6. En la página **Revisar**, revise los valores de trabajo y, a continuación, haga clic en **Enviar** para crear y ejecutar el trabajo.

## Qué hacer a continuación

Para ver el estado y otra información sobre el trabajo, haga clic en **Trabajos y operaciones** en el panel de navegación y, después, haga clic en el trabajo en la pestaña **Trabajos en ejecución**.

## 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 visualiza 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 <a href="#">página 519</a> .

# Adición de un script a un servidor

Puede añadir un script al servidor desde el que se ejecutará el script.

## Procedimiento

Complete los pasos siguientes para añadir un script a 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 17. 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. Pulse la pestaña **Informes**.
3. Seleccione **Utilización del almacenamiento de copias de seguridad** en el menú desplegable **Filtrar por categoría**.
4. Ejecute el informe haciendo clic en el icono **Ejecutar informe** (▶) junto al informe deseado.

Están disponibles los siguientes informes:

### Informe Utilización de copia de seguridad de máquina virtual

Las máquinas virtuales se pueden reducir mediante el uso de los cuadros de selección **Tipo de hipervisor**, **Hipervisor** y **Etiquetas de máquina virtual**. El valor predeterminado es **Todos**, que muestra datos para todas las copias de seguridad de máquina virtual.

El informe Utilización de copia de seguridad de máquina virtual incluye el nombre de la máquina virtual, su ubicación, el tipo de hipervisor, la política de SLA que se utiliza para proteger la máquina virtual y la ubicación del almacenamiento de copias de seguridad utilizado. 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. Se visualiza el tamaño de la copia de seguridad de cada máquina virtual y el número de puntos de recuperación disponibles para cada máquina virtual. Por último, el número total de máquinas virtuales protegidas aparece en la parte inferior del informe. El cuadro **Buscar** se puede utilizar para filtrar más los resultados de informe.

### Informe Utilización del almacenamiento de vSnap

Utilice las opciones de informe para filtrar servidores vSnap específicos para que se muestren a través del cuadro de selección **Almacenamiento de vSnap**. Para filtrar volúmenes de destino de réplica,

seleccione **Excluir volúmenes de destino de réplica**. Para ver una vista detallada de las máquinas virtuales y de las bases de datos individuales que están protegidas en cada servidor vSnap, seleccione **Mostrar recursos protegidos por el almacenamiento de vSnap**. Este área del informe muestra los nombres de las máquinas virtuales, el hipervisor asociado, la ubicación y la proporción de compresión y deduplicación del servidor vSnap.

El informe Utilización del almacenamiento de vSnap muestra los servidores vSnap, el sitio, estado, espacio total, espacio libre y espacio utilizado. Cuando se expande, se muestran las proporciones de deduplicación y compresión, si procede, para cada servidor vSnap. 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. El cuadro **Buscar** se puede utilizar para filtrar más los resultados de informe.

**Nota:** 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 528](#)

Puede ejecutar, guardar o planificar informes en IBM Spectrum Protect Plus.

[“Tipos de informes” en la página 521](#)

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. Pulse la pestaña **Informes**.
3. Seleccione **Protección** en el menú desplegable **Filtrar por categoría**.
4. Ejecute el informe haciendo clic en el icono **Ejecutar informe** (▶) junto al informe deseado.

Están disponibles los siguientes informes:

### Informe Historial de copia de seguridad de volumen persistente de contenedor

El informe Historial de copia de seguridad de volumen persistente de contenedor muestra el historial de trabajos de copia de seguridad del volumen de contenedor persistente. Utilice las opciones de informe para filtrar por tipo de Reclamación de volumen persistente (PVC) y para seleccionar **PVC** específicas para mostrar. El informe se puede filtrar más por trabajos que han fallado o trabajos que se han realizado correctamente en el campo **Estado** y por políticas de acuerdo de nivel de servicio (SLA) específicas utilizando el campo **Política de SLA**. Establezca un valor entero en el campo **Historial de copia de seguridad de los últimos días** para mostrar el historial de copia de seguridad para un número de días especificado.

### 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 **Estado** por trabajos fallidos o trabajos que se han realizado correctamente. El informe se puede filtrar más por políticas de acuerdo de nivel de servicio (SLA) específicas utilizando el campo



**Política de SLA.** Se puede especificar un valor de entero para el campo **Historial de copia de seguridad de los últimos días** para limitar los resultados.

En la vista de detalles del informe, expanda un trabajo asociado para ver más detalles de trabajo, como por ejemplo, el motivo por el que un trabajo ha fallado o el tamaño de una copia de seguridad correcta. El cuadro **Buscar** se puede utilizar para filtrar más los resultados de informe.

### **Informe de conformidad con RPO de las bases de datos en políticas de SLA**

Utilice las opciones de informe para filtrar por **Tipo de aplicación** y para seleccionar un **Servidor de aplicaciones** específico para mostrar. El informe se puede filtrar más por bases de datos que están en conformidad o no con el RPO definido a través del campo **Mostrar bases de datos que son**, o por **Tipo de protección**, incluidos los datos de los que se ha realizado una copia de seguridad en vSnap, utilizando la réplica, utilizando la copia de almacenamiento de objetos o utilizando el archivado.

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. La vista rápida muestra un gráfico circular de un recuento de copias de seguridad en vSnap que se están en conformidad y aquellas que no están en conformidad. La vista de resumen muestra la política de SLA, la planificación de SLA, el número de copias de seguridad en vSnap que están en conformidad y el número de las que no están en conformidad, y las réplicas que están en conformidad y las que no. También se muestran bases de datos que no están en conformidad con los tipos de protección que incluyen nombres de base de datos, servidores de aplicaciones, tipos de aplicación, la última hora de protección satisfactoria y el motivo de falta de conformidad.

### **Informe Historial de copia de seguridad del sistema de archivos**

Ejecute el informe Historial de copia de seguridad del sistema de archivos para revisar el historial de protección de los sistemas de archivos específicos. Para ejecutar el informe, se debe especificar al menos un servidor en la opción **Servidor** y se debe seleccionar un sistema de archivos para la opción **Sistema de archivos**. Utilice las opciones de informe para filtrar **Estado** por trabajos fallidos o trabajos que se han realizado correctamente. El informe se puede filtrar más por políticas de acuerdo de nivel de servicio (SLA) específicas utilizando el campo **Política de SLA**. El valor predeterminado para las cuatro opciones es **Todos**. Se puede especificar un valor de entero para el campo **Historial de copia de seguridad de los últimos días** para limitar los resultados.

Las propiedades de informe muestran la fecha de creación y la cuenta que se ha utilizado para generar el informe. También se incluyen los filtros de informe utilizados cuando se generó el informe. En la vista de detalles del informe, el sistema de archivos se lista con el servidor y el número total de ejecuciones. Se visualizan la política de SLA, la hora del trabajo y el estado del trabajo. Se puede ampliar la información de un trabajo asociado para ver más detalles de trabajo, como por ejemplo la razón por la que un trabajo ha fallado y el tamaño de una copia de seguridad realizada correctamente. El cuadro **Buscar** se puede utilizar para filtrar más los resultados de informe.

### **Informe Conformidad con RPO de las políticas de SLA del sistema de archivos**

Utilice las opciones de informe para seleccionar un **Servidor** específico para mostrar. El informe se puede filtrar más por **Tipo de protección**, incluidos los datos de los que se ha realizado una copia de seguridad en vSnap, utilizando la réplica, utilizando la copia de almacenamiento de objetos o utilizando el archivado. El valor predeterminado para estos dos filtros es **Todos**. Los sistemas de archivos que se encuentran en conformidad o no en conformidad con el RPO definido se pueden filtrar mediante el campo **Visualizar sistemas de archivos que son**.

El informe Conformidad con RPO de las políticas de SLA del sistema de archivos muestra los sistemas de archivos en relación con los objetivos de punto de recuperación tal como se definen en las políticas de SLA. Las propiedades de informe muestran la fecha de creación y la cuenta que se ha utilizado para generar el informe. También se incluyen los filtros de informe utilizados cuando se generó el informe. La vista rápida muestra un gráfico circular de un recuento de copias de seguridad en vSnap conformes y aquellas no conformes. La vista de resumen muestra la política de SLA, la planificación de SLA, el número de copias de seguridad en vSnap y los trabajos que utilizan la réplica. Se incluyen los trabajos de política de SLA del sistema de archivos que no están en conformidad si se ha seleccionado el filtro de no conformidad. La información que se visualiza son los trabajos de SLA de no conformidad: copia de seguridad en vSnap, réplica, copia de almacenamiento de objetos y archivado. Para los trabajos de política de SLA del sistema de archivos no conformes, se listan la

política de SLA y la planificación de SLA con cada sistema de archivos, servidor, la última hora de protección correcta y el motivo de falta de conformidad.

### 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 **Tipo de aplicación**, **Servidor de aplicaciones** y **Tipo de servidor de aplicaciones** para mostrar. 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 protegidas y no 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 detalles se muestra para cada tipo de base de datos y proporciona información adicional, incluidos los nombres de base de datos, el servidor de aplicaciones y la MV de alojamiento. La vista de detalles también proporciona esta información sobre bases de datos no protegidas en la sección Vista de detalles - Bases de datos no protegidas. El cuadro **Buscar** se puede utilizar para filtrar más los resultados de informe.

### Informe Sistemas de archivos protegidos y no protegidos

Ejecute el informe Sistemas de archivos protegidos y no protegidos para ver el estado de protección de los sistemas de archivos. El informe muestra los sistemas de archivos protegidos y no protegidos 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 **Servidor**, **Tipo de sistema operativo** y **Tipo de sistema de archivos** para mostrar. Para excluir sistemas de archivos que están protegidos mediante trabajos de copia de seguridad basados en el hipervisor, seleccione **Ocultar sistemas de archivos protegidos como parte de la copia de seguridad de hipervisor**. Para excluir sistemas de archivos no protegidos en el informe, seleccione **Ocultar sistemas de archivos no protegidos**.

Las propiedades de informe muestran la fecha de creación y la cuenta que se ha utilizado para generar el informe. También se incluyen los filtros de informe utilizados cuando se generó el informe. La vista de resumen muestra el estado de protección de los sistemas de archivos registrados. Se visualizan dos vistas detalladas, una para los sistemas de archivos protegidos y la otra para los sistemas de archivos no protegidos. La información se organiza por Sistema de archivos, Vía de acceso, Tipo de sistema de archivos, Tipo de SO y Servidor con el número total de sistemas de archivos protegidos y no protegidos visualizados. El cuadro **Buscar** se puede utilizar para filtrar más los resultados de informe.

### 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 **Hipervisor/Cuentas** específicas para mostrar. 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 ha hecho copia de seguridad en el almacenamiento de copias de seguridad secundario, seleccione **Mostrar solo las máquinas virtuales con copias de seguridad de copia de almacenamiento de objetos**. Las **Etiquetas** también se pueden utilizar para filtrar informes.

Las máquinas virtuales protegidas muestran una visión general de las máquinas virtuales protegidas, incluido el número total de máquinas virtuales protegidas, el nombre de máquina virtual, hipervisor/cuenta, tipo de hipervisor, ubicación y la capacidad gestionada. La capacidad gestionada es la capacidad utilizada de una máquina virtual. Las máquinas virtuales no protegidas proporcionan la misma información para las máquinas virtuales que no están protegidas. El cuadro **Buscar** se puede utilizar para filtrar más los resultados de informe.

## 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 **Estado** por trabajos fallidos o trabajos que se han realizado correctamente. El informe se puede filtrar más por políticas de acuerdo de nivel de servicio (SLA) específicas utilizando el campo **Política de SLA**. Se puede especificar un entero para el campo **Historial de copia de seguridad de los últimos días** para limitar los resultados y se puede utilizar **Etiquetas** para filtrar el informe.

La vista de detalles muestra la política de SLA utilizada en la lista de máquinas virtuales, cuenta y número total de ejecuciones. La información de cada ejecución se puede ampliar para listar el tamaño de datos de copia de seguridad. También se visualiza el tiempo de protección, estado y el almacenamiento de copias de seguridad utilizado. El cuadro **Buscar** se puede utilizar para filtrar más los resultados de informe.

## Informe de conformidad con RPO de las VM en políticas de SLA

Utilice las opciones de informe para filtrar por **Tipo, Hipervisor/Cuenta, Tipo de protección** que incluye datos de los que se ha hecho copia de seguridad en vSnap, usando la réplica, la copia de almacenamiento de objetos, el archivado o la instantánea, y para visualizar las máquinas virtuales que están en conformidad o no con el RPO definido a través del campo **Visualizar máquinas virtuales que son**. También hay un filtro para **Etiquetas**.

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. La vista rápida muestra un gráfico circular de un recuento de copias de seguridad en vSnap que se están en conformidad y aquellas que no están en conformidad. También hay un gráfico circular de instantáneas que están en conformidad y las que no están en conformidad. Una vista de resumen muestra la política de SLA utilizada, la planificación de SLA, la proporción de copias de seguridad en vSnap para conformes y no conformes y la proporción de instantáneas de conformes y no conformes. También se muestran las MV que no están en la vista de conformidad para cada tipo de protección. El cuadro **Buscar** se puede utilizar para filtrar más los resultados de informe.

## Conceptos relacionados

[“Tipos de informes” en la página 521](#)

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. Pulse la pestaña **Informes**.
3. Seleccione **Sistema** en el menú desplegable **Filtrar por categoría**.
4. Ejecute el informe haciendo clic en el icono **Ejecutar informe** (▶) junto al informe deseado.

Están disponibles los siguientes informes:

### Informe de configuración

Utilice la opción **Tipo de configuración** para filtrar los tipos de configuración que se deben visualizar. El informe de configuración muestra la configuración de los servidores de aplicaciones, sistemas virtualizados, almacenamiento de copia de seguridad para disco, almacenamiento de objetos, servidores de repositorio, proxies VADP, servidores LDAP y servidores SMTP. En el informe se incluye el nombre del recurso, el tipo de recurso (SO o aplicación), proveedor, sitio asociado, estado y estado

de la conexión SSL. No se muestran todas las opciones para cada componente del informe de configuración. El cuadro **Buscar** se puede utilizar para filtrar más los resultados de informe.

### Informe de trabajos

Utilice las opciones de informe para filtrar los tipos de trabajo seleccionando el cuadro de selección **Tipo de trabajo** y para visualizar los trabajos que se han ejecutado correctamente durante un periodo de tiempo en el cuadro de selección **Días desde la ejecución correcta**. La vista rápida muestra un gráfico circular con el número de trabajos completados, trabajos fallidos y otros trabajos. La vista de resumen de los trabajos que se han ejecutado al menos una vez muestra el tipo de trabajo, el número de trabajos asociados con ese tipo, el número de ejecuciones, el número de trabajos completados, trabajos fallidos y otros trabajos. La vista de detalle de los trabajos que se ejecutan al menos una vez incluye el trabajo, tipo, número de ejecuciones y el número de trabajos completados, trabajos fallidos y otros trabajos, la última ejecución correcta y el porcentaje de éxito. En todos los casos, otros trabajos son los 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 detalles, haga clic en el icono de signo más (+) situado junto a un trabajo asociado para ver detalles adicionales del trabajo como, por ejemplo el ID de trabajo, el tiempo promedio de ejecución, el estado del último tiempo de ejecución, la hora de la última ejecución y el siguiente tiempo de ejecución planificado si el trabajo está planificado, y los recursos protegidos. Al final del informe se encuentra una vista de detalle para los trabajos que nunca se han ejecutado.

### 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.

#### Protección de Office 365

El campo **Protección de Office 365** muestra los usuarios protegidos a través del trabajo de copia de seguridad de la aplicación Office 365. El campo **Capacidad front-end** muestra el tamaño total utilizado de los usuarios protegidos.

#### Protección del volumen persistente del contenedor

El campo **Protección del volumen persistente de contenedor** muestra los volúmenes persistentes de contenedor protegidos. El campo **Capacidad front-end** muestra el tamaño utilizado de estos volúmenes persistentes de contenedor.

#### 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 521

Puede personalizar los informes predefinidos para supervisar la utilización del almacenamiento de copia de seguridad y otros aspectos del entorno del sistema.

## Ejecución de un informe de entorno de máquinas virtuales

Puede ejecutar informes para el entorno de máquina virtual (MV) en IBM Spectrum Protect Plus. Los informes pueden ayudarle a supervisar la cantidad de espacio libre en cada hipervisor, el uso de almacenamiento de números de unidad lógica (LUN) y el estado de todas las máquinas virtuales.

### Procedimiento

1. En el panel de navegación, pulse **Informes y registros > Informes**.
2. Pulse la pestaña **Informes**.
3. Seleccione **Entorno de máquina virtual** en el menú desplegable **Filtrar por categoría**.
4. Ejecute el informe haciendo clic en el icono **Ejecutar informe** (▶) junto al informe deseado.

Están disponibles los siguientes informes:

#### Informe Almacén de datos de máquina virtual

Elija esta opción para revisar la utilización de almacenamiento de los almacenes de datos en el entorno de la máquina virtual. La información que proporciona este informe se puede filtrar utilizando el **Tipo de hipervisor** e **Hipervisor**. El **Filtro de vista de detalle** controla los almacenes de datos que deben visualizarse en la vista de detalles 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 detalles.

La vista rápida muestra un gráfico circular con la utilización de almacenamiento de espacio libre y utilizado. La vista de resumen muestra el hipervisor, el recuento de almacén de datos y la capacidad y el espacio libre. La vista de detalles muestra los almacenes de datos y muestra los almacenes de datos huérfanos que no tienen máquinas virtuales registradas. También se muestra el hipervisor asociado, el tipo de hipervisor, el tipo de almacén de datos, la capacidad, el espacio libre y el porcentaje utilizado. Las tres vistas contienen los almacenes de datos totales, la capacidad total y el espacio libre total. El cuadro **Buscar** se puede utilizar para filtrar más los resultados de informe.

#### Informes de LUN de máquinas virtuales

Revise la utilización de almacenamiento de números de unidades lógicas (LUN) de las máquinas virtuales. Los filtros para este tipo de informe incluyen **Tipo de hipervisor** e **Hipervisores**. 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.

En el informe, la vista de resumen muestra el hipervisor, el número de LUN asociados con el hipervisor y la capacidad. En la vista de detalles, se muestra el nombre de LUN, el ID de LUN, el proveedor de almacenamiento, el hipervisor, el almacén de datos o el volumen, la capacidad, el tipo de transporte y la correlación de dispositivos en bruto para cada LUN. Ambas vistas muestran el recuento total de LUN y la capacidad total. El cuadro **Buscar** se puede utilizar para filtrar más los resultados de informe.

#### Informe de extensión de instantáneas de máquinas virtuales

Este informe de extensión de instantáneas muestra la antigüedad, el nombre y el número de instantáneas que se utilizan para proteger los recursos de hipervisor. Las opciones de informe disponibles para filtrar son por **Tipo de hipervisor**, **Hipervisor** y **Etiquetas**. Utilice el filtro **Hora de creación del filtro** para visualizar instantáneas de periodos específicos de tiempo.

El informe contiene una vista de detalles que muestra el nombre de instantánea y la hora de creación de la instantánea. Cada instantánea aparece debajo de la máquina virtual asociada, el hipervisor y el tipo de hipervisor. El número total de máquinas virtuales e instantáneas se muestra al final de la vista. El cuadro **Buscar** se puede utilizar para filtrar más los resultados de informe.

## 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. Las opciones de informe disponibles para filtrar son por **Tipo de hipervisor**, **Hipervisor**, **Días desde el último apagado**, **Días desde la última suspensión**, **Días desde el último encendido** y **Etiquetas**.

El informe contiene la vista rápida que es un gráfico circular que muestra la utilización de almacenamiento basada en el estado de alimentación de la máquina virtual: MV apagadas, máquinas virtuales encendidas, plantillas y máquinas virtuales suspendidas. También hay vistas de detalles para cada uno de los estados de alimentación. La vista de detalles, Máquinas virtuales encendidas, muestra el nombre de la máquina virtual, la fecha y el número de días desde que se apagaron, el hipervisor asociado, el tipo de hipervisor, el espacio suministrado y el almacén de datos o el volumen. El total de máquinas virtuales apagadas se muestra en la parte inferior de esta vista junto con el espacio total suministrado. el nombre de la máquina virtual, la fecha y el número de días desde que se apagaron, el hipervisor asociado, el tipo de hipervisor, el espacio suministrado y el almacén de datos del volumen. El número total de MV suspendidas y el espacio total suministrador se muestra en la parte inferior de la vista. La vista de detalles, Plantilla, contiene los nombres de plantilla, el hipervisor asociado, el tipo de hipervisor, el espacio suministrado y el almacén de datos o el volumen. El número total de plantillas y el espacio suministrado total aparece en la parte inferior de la vista. La vista de detalles, Máquinas virtuales encendidas, contiene el nombre de la máquina virtual, la fecha y el número de días que las máquinas virtuales han estado encendidas, el hipervisor asociado, el tipo de hipervisor, el espacio suministrado y el almacén de datos o el volumen. Al final de la vista se encuentra el número total de máquinas virtuales encendidas y el espacio total suministrado. El cuadro **Buscar** se puede utilizar para filtrar más los resultados de informe.

## 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 qué **Hipervisor** se debe visualizar.

El informe contiene una vista de detalles que muestra el nombre de la máquina virtual y el espacio suministrado. Cada máquina virtual aparece bajo el almacén de datos o volumen asociado, hipervisor o tipo de hipervisor. El número total de almacenes de datos/volúmenes y máquinas virtuales se muestra al final de la vista. El cuadro **Buscar** se puede utilizar para filtrar más los resultados de informe.

### Conceptos relacionados

“Tipos de informes” en la página 521

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.

### Antes de empezar

Los roles personalizados que se asignan a los usuarios que ejecutan informes requieren que se establezcan los permisos adecuados en ese rol de modo que se pueda visualizar el informe. Para obtener más información sobre los roles, tipos de permiso y permisos, consulte [“Gestión de roles” en la página 537](#).

## Procedimiento

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

1. En el panel de navegación, pulse **Informes y registros > Informes**.
2. Pulse la pestaña **Informes**.
3. Ejecute el informe haciendo clic en el icono **Ejecutar informe** (▶) junto al informe deseado.
  - Para ejecutar el informe con parámetros personalizados, establezca los parámetros en la ventana **Ejecutar informe** y haga clic en **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 521

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. Pulse la pestaña **Informes**.
3. Haga clic en el icono **Crear informe personalizado** (+) junto al informe que desea personalizar.
4. En la ventana **Crear informe personalizado**, seleccione la pestaña **Parámetros**. Especifique un nombre para el informe en el campo **Nombre** y especifique una descripción para el informe personalizado en el campo **Descripción**. Establezca los parámetros personalizados relacionados con el informe seleccionado.



**Nota:** Los nombres de informe pueden incluir caracteres alfanuméricos y los símbolos siguientes: \$-\_.+!\*'(). No se permiten espacios en el nombre de informe.

5. De manera opcional, en la pestaña **Planificar**, marque el recuadro **Definir planificación**. Si se va a definir una planificación, proporcione esta información:

**Restricción:** Los días de la semana para la opción **Semanas** está disponible solo si instala el arreglo temporal de IBM Spectrum Protect Plus 10.1.6 eFix2 o posterior.

- En **Frecuencia**, entre un valor entero y seleccione **Minutos**, **Horas**, **Días**, **Semanas**, **Meses** o **Años**. Cuando se selecciona **Semanas**, puede seleccionar uno o más días de la semana. La **Hora de inicio** se aplicará a los días seleccionados de la semana.
  - En **Hora de inicio**, especifique una fecha y hora y seleccione el huso horario adecuado. El huso horario predeterminado que se muestra se basa en los valores del navegador
  - Especifique la dirección de correo electrónico del destinatario que va a recibir una copia del informe en el campo de dirección de correo electrónico. Se debe añadir al menos un destinatario. Si se necesitan más direcciones, haga clic en el icono de signo más **Añadir un destinatario** (+).
6. Pulse el botón **Guardar informe**.
  7. Para localizar un informe personalizado, pulse en la pestaña **Informes personalizados**.
  8. Haga clic en el icono **Ejecutar informe personalizado** (▶) para ejecutar el informe.



9. De manera opcional, para actualizar un informe personalizado, haga clic en el icono **Actualizar informe personalizado** (). Para eliminar un informe personalizado, haga clic en el icono **Eliminar informe** (.

### Qué hacer a continuación

Ejecute el informe personalizado y revise los resultados del informe.

### Conceptos relacionados

[“Gestión de informes y registros” en la página 521](#)


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 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. Pulse la pestaña **Informes**.
3. Defina una planificación para un informe pulsando el icono **Planificar informe con parámetros predeterminados** () junto al informe deseado.

**Nota:** Para planificar un informe con parámetros no predeterminados, cree un informe personalizado. Para obtener más información, consulte el apartado [“Creación de un informe personalizado” en la página 529](#).

4. Aparecerá la ventana **Planificar informe con parámetros predeterminados**.

**Restricción:** Los días de la semana para la opción **Semanas** está disponible solo si instala el arreglo temporal de IBM Spectrum Protect Plus 10.1.6 eFix2 o posterior.

- En **Frecuencia**, entre un valor entero y seleccione **Minutos, Horas, Días, Semanas, Meses o Años**. Cuando se selecciona **Semanas**, puede seleccionar uno o más días de la semana. La **Hora de inicio** se aplicará a los días seleccionados de la semana.
- En **Hora de inicio**, especifique una fecha y hora y seleccione el huso horario adecuado. El huso horario predeterminado que se muestra se basa en los valores de su navegador web.
- Especifique la dirección de correo electrónico del destinatario que va a recibir una copia del informe en el campo de dirección de correo electrónico. Se debe añadir al menos un destinatario. Si se necesitan más direcciones, haga clic en el icono de signo más **Añadir un destinatario** (.

5. Pulse el botón **Planificar**.

### 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 521](#)

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 542](#)

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 18. 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 solo 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.

**Restricción:** No asigne un usuario de control de acceso basado en rol (RBAC) a más de un grupo de recursos de VMware. Los usuarios que se han asignado al grupo de recursos Etiqueta y categorías y, a continuación, se asignan a Hosts y clústeres o a Máquinas virtuales y plantillas darán como resultado que los datos no se visualicen para la vista Hosts y clústeres o Máquinas virtuales y plantillas. Solo se visualizará información para las etiquetas y categorías que estén seleccionadas como vista cuando se realizan operaciones.

### 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 IBM Spectrum Protect Plus, 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	<ol style="list-style-type: none"><li>a. Seleccione un tipo de recurso en el menú <b>Elegir un tipo de recurso</b>.</li><li>b. Seleccione los subtipos de recursos y, a continuación, pulse <b>Añadir recursos</b>. Los recursos se añaden a la vista <b>Recursos seleccionados</b>.</li></ol>
Desde plantilla	<ol style="list-style-type: none"><li>a. Seleccione un grupo de recursos en la lista <b>¿Qué grupo de recursos desea utilizar como plantilla?</b>. Los recursos de la plantilla seleccionada se añaden a la vista <b>Recursos seleccionados</b>.</li><li>b. Puede añadir recursos utilizando la lista <b>Elegir un tipo de recurso</b> y las listas asociadas.</li></ol> <p>Para ver los tipos de recursos disponibles y su uso, consulte <a href="#">"Tipos de recursos"</a> en la página 535.</p>

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 <a href="#">“Creación de un rol”</a> en la página 539.

### 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	<ul style="list-style-type: none"> <li>• Rol</li> <li>• Usuario</li> <li>• Identidad</li> </ul>	Se utiliza para otorgar acceso a roles y usuarios a través del panel <b>Cuentas</b> .
Aplicación	<ul style="list-style-type: none"> <li>• Db2</li> <li>• Oracle</li> <li>• SQL - Clúster autónomo/migración tras error</li> <li>• SQL siempre activado</li> </ul>	Sirve para otorgar acceso para ver bases de datos de aplicaciones individuales en un servidor de aplicaciones en IBM Spectrum Protect Plus.
Contenedor	Kubernetes	Se utiliza para otorgar acceso a recursos del contenedor.
Sistema de archivos	Windows	Se utiliza para otorgar acceso a recursos del sistema de archivos.
Servidor de aplicaciones	<ul style="list-style-type: none"> <li>• Db2</li> <li>• SQL</li> <li>• Oracle</li> </ul>	Se utiliza para otorgar acceso a servidores de aplicaciones en IBM Spectrum Protect Plus sin tener acceso a bases de datos individuales.
Hipervisor	<ul style="list-style-type: none"> <li>• VMware</li> <li>• Hyper-V</li> <li>• Amazon EC2</li> </ul>	Se utiliza para otorgar acceso a recursos del sistema virtualizado.
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.

Tipo de recurso	Subtipo	Descripción
Informe	<ul style="list-style-type: none"> <li>Utilización del almacenamiento de copias de seguridad</li> <li>Protección</li> <li>Sistema</li> <li>Entorno de VE</li> </ul>	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.
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 <b>Sistema &gt; Identidad</b> .
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.

Tipo de recurso	Subtipo	Descripción
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 IBM Spectrum Protect Plus, 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. Se pueden establecer permisos para permitir a un usuario crear, ver y ejecutar los trabajos de copia de seguridad y restauración definidos en un grupo de recursos, pero no suprimirlos.

De forma similar, se pueden establecer permisos para crear cuentas de administrador, habilitar un usuario para crear y editar todas las cuentas, establecer sitios y recursos e interactuar con todas las características 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**

Los usuarios con el rol Administrador de aplicaciones pueden completar las siguientes acciones:

- Registrar y modificar los recursos de base de datos de aplicaciones que ha delegado 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**

Los usuarios con el rol Solo copia de seguridad pueden completar las siguientes acciones:

- Crear, ver y ejecutar 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**.

### **OC\_MONITOR\_ROLE**

Se crea OC\_MONITOR\_ROLE cuando IBM Spectrum Protect Operations Center crea el usuario OC\_MONITOR. Centro de operaciones necesita este rol y este usuario para conectar con el entorno de IBM Spectrum Protect Plus. El usuario OC\_MONITOR utiliza OC\_MONITOR\_ROLE y proporciona los permisos necesarios para conectar Centro de operaciones a IBM Spectrum Protect Plus. No edite este rol.

### **Restaurar únicamente**

Los usuarios con el rol Solo restauración pueden 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**

Los usuarios con el rol Autoservicio pueden supervisar las operaciones de seguridad y de restauración existentes que ha delegado 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 que está asignado al rol SUPERUSER:

- Modificar y suprimir cuentas de usuario
- Cambiar contraseñas de usuario
- Asignar roles de usuario



## VM Admin

Los usuarios con el rol Administrador de máquina virtual pueden completar las siguientes acciones:

- 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	<p>a. Seleccione un rol en el menú <b>¿Qué rol deseo utilizar como plantilla?</b>. Los permisos que están asociados al rol de plantilla se seleccionan de forma predeterminada.</p> <p>b. Seleccione permisos adicionales para aplicar al rol y suprima los permisos que no sean necesarios.</p> <p>Para ver los permisos disponibles y su uso, consulte <a href="#">“Tipos de permisos”</a> en la página 539.</p>

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.

Nombre	Permisos	Descripción
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	Se utiliza para interactuar con certificados SSL para acceder a servidores de nube.
Almacenamiento de objetos	Registrar, ver, editar, anular registro	Se utiliza para interactuar con el almacenamiento de objetos que se define como almacenamiento de copias de seguridad para operaciones de copia.
Nube	Registrar, ver, editar, anular registro	Se utiliza para interactuar con servidores de nube que se definen como almacenamiento de copias de seguridad para operaciones de copia.
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.
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. <b>Nota:</b> Si el usuario tiene permiso para <b>Ejecutar</b> un trabajo, también puede <b>Retener, Liberar y Realizar acciones de restauración personalizadas</b> para el trabajo
Proxy VADP	Registrar, ver, editar, anular registro	Se utiliza para interactuar con VADP.
Informe	Crear, ver, editar, suprimir	Sirve para interactuar con informes.

Nombre	Permisos	Descripción
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.
Servidor de script	Registrar, ver, editar, anular registro	Se utiliza para interactuar con el servidor en el que se ejecutan los PreScript y los PostScript.
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.
Usuario	Crear, ver, editar, suprimir	Se utiliza para interactuar con usuarios, asociar un grupo de recursos con un rol y proporcionar 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 siguientes 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 534](#) y [“Creación de un rol” en la página 539](#).

### 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

Con IBM Spectrum Protect Plus, puede utilizar un servidor Lightweight Directory Access Protocol (LDAP) para gestionar usuarios. Cuando crea una cuenta de usuario de LDAP, puede añadir la cuenta de usuario a un grupo de usuarios.

### Antes de empezar

Complete las tareas siguientes:

- Asegúrese de que ha registrado un proveedor de LDAP con IBM Spectrum Protect Plus. Para registrar un proveedor de LDAP, siga las instrucciones de [“Adición de un servidor LDAP”](#) en la página 216.
- Si desea utilizar roles personalizados y grupos de recursos, asegúrese de que los roles o grupos están disponibles. Para obtener instrucciones sobre la creación de roles y grupos, consulte [“Creación de un rol”](#) en la página 539 y [“Creación de un grupo de recursos”](#) en la página 534.

### Procedimiento

Para crear una cuenta de usuario para un grupo LDAP, 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 > Grupo LDAP**.
4. En el campo **Nombre de grupo** de la sección **Seleccionar grupo LDAP**, especifique el grupo LDAP realizando una de las siguientes acciones:
  - Especifique el nombre de grupo LDAP.
  - Busque el nombre de grupo LDAP escribiendo un texto parcial, un asterisco (\*) como único carácter comodín o un signo de interrogación (?) para la coincidencia de patrón. Para ver todos los grupos LDAP, haga clic en el botón **Ver todos**.
  - Opcionalmente, se puede proporcionar un nombre distinguido relativo (RDN) llenando el campo **RDN de grupo**.
5. Los grupos LDAP se visualizan en la tabla **Grupos LDAP**. Seleccione un grupo LDAP.
6. En la sección **Asignar rol**, seleccione uno o varios roles para el usuario.
7. En la sección **Grupos de permisos**, revise los permisos y los recursos que están disponibles para el usuario y, a continuación, pulse **Continuar**.
8. 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**.
9. Pulse **Crear usuario**.

### Resultados

La cuenta de usuario se muestra en la tabla de usuarios. De forma opcional, para ver los roles, los permisos y los grupos de recursos disponibles, seleccione un usuario en la tabla de usuarios.

## 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 19. 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 está actualizando IBM Spectrum Protect Plus desde un release anterior, 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 grandes 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 509](#)

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 bajo demanda” en la página 512](#)

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 20. 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 567387](#).

---

### 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.

---

### ¿Cómo puedo disponer en niveles los datos en el almacenamiento en la nube o en cintas?

No puede disponer en niveles los datos de IBM Spectrum Protect Plus en el almacenamiento en cintas. Puede disponer en niveles los datos de IBM Spectrum Protect Plus en el almacenamiento en la nube, pero solo en las clases de almacenamiento en la nube que soportan la recuperación de datos rápida. Cuando se copian datos en cintas de IBM Spectrum Protect Plus a Servidor de IBM Spectrum Protect, no es buena idea utilizar la función de organización por niveles de IBM Spectrum Protect. Si está archivando datos en cintas, debe utilizar una agrupación de almacenamiento en memoria caché fría.

Revise las directrices sobre el almacenamiento en cintas y en la nube:

- Aunque no puede disponer en niveles los datos de IBM Spectrum Protect Plus en cintas, puede activar o copiar los datos de IBM Spectrum Protect Plus en cintas. Para ello, defina una agrupación de almacenamiento de memoria caché de datos fríos para copiar datos en cintas, como se describe en el Paso 1: Creación de una agrupación de almacenamiento en cintas y una agrupación de almacenamiento en memoria caché de datos fríos para copiar datos en cintas.
- Puede disponer en niveles los datos de IBM Spectrum Protect Plus en agrupaciones de almacenamiento en contenedores en la nube, pero solo en las clases de almacenamiento en la nube que soportan la recuperación de datos rápida. Si utiliza Amazon Web Services (AWS) con el protocolo Simple Storage Service (S3) para mover datos a agrupaciones de contenedores en la nube, no mueva los datos a Amazon S3 Glacier. Para escenarios e instrucciones sobre la copia o archivado de datos en el almacenamiento en la nube, consulte Configuración para copiar o archivar datos. Para obtener instrucciones sobre la disposición en niveles de los datos en la nube, consulte [Disposición en niveles de](#)

los datos en el almacenamiento en la nube o en cintas en la documentación del producto IBM Spectrum Protect.

No puede disponer en niveles los datos de IBM Spectrum Protect Plus en cintas. Para almacenar datos de IBM Spectrum Protect Plus en cintas, copie los datos en un servidor de IBM Spectrum Protect para su almacenamiento en soporte de cintas físicas o en una biblioteca de cintas virtual. Para obtener distintos escenarios y más información sobre cómo configurar el almacenamiento, consulte [“Configuración para copiar o archivar datos en IBM Spectrum Protect”](#) en la página 198 y [“Configuración para copiar o archivar datos en la nube”](#) en la página 191. Usted

Para configurar una agrupación de almacenamiento en memoria caché fría para archivar o copiar datos en cintas, consulte [“Paso 1: Creación de una agrupación de almacenamiento en cintas y una agrupación de almacenamiento de memoria caché de datos fríos para copiar datos en cintas”](#) en la página 200.

## Resolución de problemas de Soporte de copia de seguridad de Kubernetes

Para ayudar a resolver problemas con Soporte de copia de seguridad de Kubernetes, puede recopilar archivos de registro de depuración y ver los registros de rastreo. También puede seguir procedimientos para diagnosticar problemas.

### Recopilación de archivos de registro de Soporte de copia de seguridad de Kubernetes para la resolución de problemas

Puede generar archivos de registro de depuración en el entorno de Kubernetes para resolver problemas de despliegue de las operaciones de Soporte de copia de seguridad de Kubernetes y Soporte de copia de seguridad de Kubernetes en el servidor de IBM Spectrum Protect Plus.

#### Acerca de esta tarea

Todos los archivos se recopilan en el directorio /tmp en el sistema local y se empaquetan en un archivo de archivado tar.gz. El archivo de archivado se denomina generalmente `baas_debug_logs_timestamp.tar.gz`.

#### Procedimiento

Utilice uno de los métodos siguientes para recopilar registros para la resolución de problemas:

- Para recopilar solo los registros de Kubernetes con fines de depuración, emita el mandato siguiente:

```
./baas_install.sh -l
```

Este mandato recopila registros de depuración para el despliegue de Soporte de copia de seguridad de Kubernetes que especifican los parámetros en `baas_config.cfg`. Se recopilan la información de estado actual y los registros de los componentes de Soporte de copia de seguridad de Kubernetes del clúster Kubernetes. Los registros se estructuran en función de la arquitectura de registro básico de Kubernetes. Para obtener más información, consulte el apartado [Registro básico en Kubernetes](#).

- Para recopilar el paquete de registro que incluye los archivos de depuración para el despliegue de Soporte de copia de seguridad de Kubernetes y el servidor de IBM Spectrum Protect Plus, emita el mandato siguiente:

```
./baas_install.sh -l -x
```

#### 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 al soporte de IBM Software para solicitar ayuda.

## Tareas relacionadas

[“Establecimiento del nivel de rastreo de los archivos de registro” en la página 551](#)

Puede establecer el nivel de rastreo de los archivos de registro locales para ayudarle a resolver los problemas que puede encontrarse en Soporte de copia de seguridad de Kubernetes.

## Referencia relacionada

[“Consulta rápida de resolución de problemas” en la página 554](#)

Se proporcionan soluciones a problemas de Soporte de copia de seguridad de Kubernetes básicos.

[“Resolución de problemas en operaciones de Soporte de copia de seguridad de Kubernetes” en la página 558](#)

Los procedimientos de resolución de problemas están disponibles para ayudarle a diagnosticar y resolver problemas de Soporte de copia de seguridad de Kubernetes.

## Establecimiento del nivel de rastreo de los archivos de registro

Puede establecer el nivel de rastreo de los archivos de registro locales para ayudarle a resolver los problemas que puede encontrarse en Soporte de copia de seguridad de Kubernetes.

### Acerca de esta tarea

Puede establecer los niveles de rastreo para resolver problemas con los componentes de planificador, controlador y gestor de transacción de Soporte de copia de seguridad de Kubernetes. El nivel de rastreo que establece también se aplica a los niveles de registro para el agente de Soporte de copia de seguridad de Kubernetes, así como los niveles de registro en los registros de trabajo de IBM Spectrum Protect Plus y el archivo `command.log`.

Este valor no afecta al componente de transportador de datos.

Para establecer el nivel de rastreo, debe actualizar el archivo de configuración `baas_config.cfg` y, a continuación, actualizar el despliegue de Soporte de copia de seguridad de Kubernetes.

**Consejo:** El nivel de rastreo predeterminado es INFO. Si está experimentando problemas que requieren resolución de problemas, establezca el nivel de rastreo en DEBUG.

### Procedimiento

Para establecer el nivel de rastreo, complete los pasos siguientes en la línea de mandatos de Kubernetes:

1. Inicie sesión en el sistema operativo en el nodo maestro de clúster Kubernetes que se utiliza como nodo de instalación.
2. Vaya al directorio donde se ha desempquetado el paquete de instalación `SPP_V10.1.6_for_Containers.tar.gz`.
3. Vaya al directorio `installer` emitiendo el mandato siguiente:

```
cd installer
```

4. Edite el archivo `baas_config.cfg` con un editor de texto y modifique el valor para el parámetro **PRODUCT\_LOGLEVEL**.

Están disponibles las siguientes opciones de rastreo:

#### DEBUG

Visualiza los mensajes a nivel de depuración en los archivos de registro del gestor de transacción, controlador y planificador.

#### INFO

Visualiza todos los mensajes de usuario en los archivos de registro del gestor de transacción, controlador y planificador, incluidos los mensajes de información, advertencia y error. Este valor es el valor predeterminado.

#### WARNING

Visualiza los mensajes de advertencia y error en en los archivos de registro del gestor de transacción, controlador y planificador.

## ERROR

Visualiza solo los mensajes de error en los archivos de registro del gestor de transacción, controlador y planificador.

Por ejemplo, para establecer el nivel de rastreo en la modalidad de depuración, establezca el parámetro **PRODUCT\_LOGLEVEL** de la siguiente manera:

```
PRODUCT_LOGLEVEL="DEBUG"
```

5. Actualice el despliegue de Soporte de copia de seguridad de Kubernetes emitiendo el mandato siguiente:

```
./baas_install.sh -u
```

Cuando se le solicite, especifique **sí** para continuar.

6. Opcional: Para verificar el estado de la actualización, emita el mandato siguiente:

```
./baas_install.sh -s
```

**Consejo:** De forma alternativa, verifique el estado de la actualización utilizando el mandato **./helm status baas**.

## Qué hacer a continuación

Puede recopilar archivos de registro de Soporte de copia de seguridad de Kubernetes para resolver problemas o utilizar una herramienta de visualización como Kibana para ver y consultar datos en los archivos de registro del gestor de transacción, controlador y planificador. Para obtener instrucciones consulte:

- [“Recopilación de archivos de registro de Soporte de copia de seguridad de Kubernetes para la resolución de problemas” en la página 550](#)
- [“Visualización de registros de rastreo para Soporte de copia de seguridad de Kubernetes” en la página 552](#)

## Visualización de registros de rastreo para Soporte de copia de seguridad de Kubernetes

De forma opcional, puede utilizar la pila Elasticsearch, Fluentd y Kibana (EFK) para ver y analizar registros de rastreo generados por Soporte de copia de seguridad de Kubernetes.

Elasticsearch es un motor de búsqueda de texto completo distribuido. Fluentd es una herramienta que recopila registros de nodos de clúster y envía los registros al motor Elasticsearch. Kibana es una herramienta de visualización para Elasticsearch con una interfaz de usuario de web y una herramienta de desarrollo que se utiliza para consultar datos.

## Antes de empezar

Complete los pasos siguientes:

1. Despliegue la pila EFK en el clúster Kubernetes:
  - a. Despliegue el motor de búsqueda Elasticsearch. Para obtener instrucciones, consulte [Instalación de Elasticsearch](#).
  - b. Despliegue el recopilador de registros Fluentd en cada nodo de clúster. Para obtener instrucciones, consulte la publicación [Documentación de Fluentd](#).
  - c. Despliegue la herramienta de visualización Kibana. Para obtener instrucciones, consulte la publicación [Guía de Kibana](#).
2. Complete el despliegue de la pila EFK añadiendo un índice logstash a Kibana:
  - a. Acceda a la interfaz de usuario de Kibana abriendo un navegador web y especificando la URL del sistema donde se está ejecutando Kibana y especifique el número de puerto. Por ejemplo, especifique uno de los URL siguientes en el navegador web:

```
https://localhost:5601
```

o

```
http://su_dominio.com:5601
```

donde *su\_dominio* especifica el nombre de dominio del sistema.

- b. Si se le ofrecen las siguientes opciones para explorar datos, seleccione **Explorar por mi cuenta**.
- c. Haga clic en **Descubrir** > **Crear patrón de índice** y cree el patrón de índice `logstash-*`.

### Acerca de esta tarea

Cuando utiliza la pila EFK, los registros de todos los componentes de contenedor se fusionan y se muestran en la misma vista. Los registros de los pod detenidos se conservan en el almacenamiento de datos persistentes de Elasticsearch. Puede aplicar filtros para visualizar errores o mensajes específicos. También puede aplicar un filtro para mostrar eventos que tuvieron lugar en un periodo de tiempo específico.

Además de los mensajes de error y depuración, puede ver registros de rastreo para los siguientes componentes de Soporte de copia de seguridad de Kubernetes:

- Gestor de transacciones
- Controlador
- Planificador

### Procedimiento

Para ver registros de transacción para Soporte de copia de seguridad de Kubernetes, complete los pasos siguientes:

1. Abra la interfaz de usuario de Kibana y pulse el icono **Descubrir**.
2. Haga clic en el índice `logstash-*`.
3. Para ver registros para Soporte de copia de seguridad de Kubernetes, añada un filtro realizando las siguientes acciones:
  - a) Haga clic en **Añadir filtro** y especifique los siguientes valores de filtro:
    - Campo: `kubernetes.container_image`
    - Operador: `is`
    - Valor: `baas-`
  - b) Especifique un nombre para la búsqueda y pulse **Guardar**.  
Se visualizan los registros de rastreo para los contenedores `baas-transaction-manager`, `baas-controller` y `baas-scheduler`.
4. Puede crear filtros adicionales para mostrar más vistas granulares de los registros de rastreo de Soporte de copia de seguridad de Kubernetes.

Tabla 65. Filtros para visualizar registros de rastreo de Soporte de copia de seguridad de Kubernetes		
Tipo de datos que se deben mostrar	Filtro 1	Filtro 2
Registros del gestor de transacciones	<code>kubernetes.container_image is baas-transaction-manager</code>	Ninguno
Registros de controlador	<code>kubernetes.container_image is baas-controller</code>	Ninguno
Registros del planificador	<code>kubernetes.container_image is baas-scheduler</code>	Ninguno

Tabla 65. Filtros para visualizar registros de rastreo de Soporte de copia de seguridad de Kubernetes (continuación)

Tipo de datos que se deben mostrar	Filtro 1	Filtro 2
Mensajes de error	kubernetes.container_image is baas-	log is ERROR
Depuración de mensajes	kubernetes.container_image is baas-	log is DEBUG

## Consulta rápida de resolución de problemas

Se proporcionan soluciones a problemas de Soporte de copia de seguridad de Kubernetes básicos.

Utilice las soluciones de la tabla siguiente para resolver problemas básicos que pueden producirse con operaciones de Soporte de copia de seguridad de Kubernetes. Si todavía no puede resolver un problema, consulte “Resolución de problemas en operaciones de Soporte de copia de seguridad de Kubernetes” en la página 558 para obtener los procedimientos de resolución de problemas más detallados.

Tabla 66. Soluciones a problemas básicos

Problema	Solución
<p>La solicitud de Soporte de copia de seguridad de Kubernetes no es válida.</p> <p>Por ejemplo, el campo <b>Backupstatus</b> o <b>Restorestatus</b> se lista como No válido cuando ejecuta el mandato siguiente:</p> <pre>kubectrl describe baasreq request_name -n namespace</pre> <p>donde:</p> <p><b>nombre_solicitud</b> El nombre de la solicitud de copia de seguridad o restauración. Para las solicitudes de copia de seguridad, el valor es el nombre de la reclamación de volumen persistente (PVC). Para las solicitudes de restauración, el nombre debe ser exclusivo y no debe ser el mismo que el nombre de la PVC.</p> <p><b>espacio_nombres</b> El espacio de nombres en el que existe la PVC.</p>	<p>Asegúrese de que la solicitud se estructura correctamente verificando los elementos siguientes en el archivo YAML:</p> <ul style="list-style-type: none"> <li>Asegúrese de que no existen errores tipográficos.</li> <li>Asegúrese de que se utiliza el caso correcto en las sentencias. Kubernetes distingue entre mayúsculas y minúsculas.</li> </ul> <p>Por ejemplo, asegúrese de que la declaración de versión de API se lista como <code>apiVersion</code> y no <code>apiversion</code>.</p> <ul style="list-style-type: none"> <li>Para las solicitudes de restauración: <ul style="list-style-type: none"> <li>Asegúrese de que la indicación de fecha y hora para un punto de restauración se ha especificado correctamente en el campo <b>restorepoint</b>.</li> <li>Asegúrese de que el tipo de restauración se ha especificado correctamente en el campo <b>restoretype</b>.</li> </ul> </li> </ul> <p>Para obtener más información, consulte el apartado “Restauración de datos de contenedor utilizando la línea de mandatos” en la página 360.</p>



Tabla 66. Soluciones a problemas básicos (continuación)

Problema	Solución
Las instantáneas están fallando.	<p>Lleve a cabo una o varias de las acciones siguientes:</p> <ul style="list-style-type: none"> <li>• Verifique la configuración de Ceph-CSI para asegurarse de que los contenedores se están ejecutando correctamente. El software CSI es necesario para copias de seguridad de instantánea.</li> <li>• Asegúrese de que la clase de instantánea de volumen están definida para los PVC de los que se está haciendo copia de seguridad.</li> <li>• Asegúrese de que el secreto esté en el espacio de nombres correcto (el espacio de nombres para la PVC).</li> <li>• Asegúrese de que las configuraciones sean correctas en ConfigMap (baas-configmap).</li> </ul> <p>Para obtener más información, consulte <a href="#">“Resolución de problemas con trabajos de copia de seguridad de instantánea”</a> en la página 558.</p>
El transportador de datos no se puede iniciar.	<p>Lleve a cabo una o varias de las acciones siguientes:</p> <ul style="list-style-type: none"> <li>• Asegúrese de que el volumen de RBD de Ceph esté montado. Puede verificar si el volumen de RBD de Ceph no se ha podido montar emitiendo el mandato <b>kubect1 describe</b> en el módulo de transportador de datos.</li> <li>• En la salida del mandato <b>kubect1 describe</b>, compruebe los sucesos para asegurarse de que el volumen se ha inicializado ejecutando la PVC como parte de otro pod en modalidad de lectura/escritura.</li> <li>• En la salida del mandato <b>kubect1 describe</b>, compruebe los sucesos de error de autenticación. Para resolver errores de autenticación, asegúrese de que está ejecutando un registro de Docker seguro. Asegúrese de que el secreto de extracción esté en el espacio de nombres de la PVC. Para obtener instrucciones, consulte <a href="#">Sacar una imagen de un registro privado</a>.</li> </ul>
Se ha denegado el acceso o la conexión falla al montar los volúmenes NFS desde el servidor vSnap.	<p>Lleve a cabo una o varias de las acciones siguientes:</p> <ul style="list-style-type: none"> <li>• Compruebe la política de red del transportador de datos. Asegúrese de que las direcciones de servidor vSnap coincidan con las direcciones de servidor de IBM Spectrum Protect Plus.</li> <li>• Asegúrese de que existe una conexión directa desde el clúster Kubernetes al servidor vSnap de IBM Spectrum Protect Plus. La conexión por proxies no está soportada.</li> </ul>

Tabla 66. Soluciones a problemas básicos (continuación)

Problema	Solución
Los pods del planificador, el gestor de transacción y el controlador se han iniciado pero todos los pod continúan ejecutándose. En la salida del mandato <b>kubectl describe</b> para el pod de gestor de transacción, los sucesos indican que el sondeo de ejecución ha fallado.	<p>Verifique que los valores para los parámetros CLUSTER_API_SERVER_IP_ADDRESS y CLUSTER_API_SERVER_PORT se han especificado correctamente en el archivo de configuración baas_config.cfg.</p> <p>Si actualiza los valores en el archivo baas_config.cfg, emita el siguiente mandato para actualizar la configuración:</p> <pre>./baas_install.sh -u</pre> <p>Como alternativa, puede desinstalar y reinstalar Soporte de copia de seguridad de Kubernetes para borrar los archivos de registro anteriores. Para obtener instrucciones, consulte <a href="#">“Desinstalación de Soporte de copia de seguridad de Kubernetes”</a> en la página 162 and <a href="#">“Instalación y despliegue de imágenes de Soporte de copia de seguridad de Kubernetes en el entorno de Kubernetes”</a> en la página 156.</p>
Un objeto Kubernetes persiste en el estado de finalización.	<p>Emita el mandato siguiente:</p> <pre>kubectl delete object object_name --force --grace-period=0</pre> <p>Si el objeto continúa en estado de finalización, emita el mandato siguiente:</p> <pre>kubectl patch object -n namespace object_name -p '{"metadata":{"finalizers":null}}'</pre> <p>Donde:</p> <ul style="list-style-type: none"> <li><i>object</i> es un tipo de objeto en Kubernetes, como un despliegue, pod, volumen persistente (PV) o PVC</li> <li><i>object_name</i> es el nombre del objeto</li> <li><i>namespace</i> es el nombre del espacio de nombres en el que está el objeto</li> </ul>
Soporte de copia de seguridad de Kubernetes no se ha desinstalado de forma limpia.	<p>Limpie manualmente el entorno emitiendo los mandatos siguientes:</p> <pre>kubectl delete namespace baas kubectl delete clusterrole baas-controller kubectl delete clusterrole baas-scheduler kubectl delete clusterrole baas-spp-agent kubectl delete clusterrole baas-transaction-manager kubectl delete clusterrole aggregate-basreqs-admin-edit kubectl delete clusterrolebinding baas-controller kubectl delete clusterrolebinding baas-scheduler kubectl delete clusterrolebinding baas-spp-agent kubectl delete clusterrolebinding baas-transaction-manager kubectl delete customresourcedefinition baasreqs.baas.io</pre>

Tabla 66. Soluciones a problemas básicos (continuación)

Problema	Solución
La cancelación de un trabajo de copia de seguridad de copia da como resultado que los recursos queden excluidos.	<p>Limpié los recursos restantes completando los pasos siguientes:</p> <ol style="list-style-type: none"> <li>1. Suprima el despliegue de transportador de datos emitiendo los mandatos siguientes: <pre>kubectl get deploy -n namespace kubectl delete deploy --all -n namespace</pre> </li> <li>2. Suprima la cuenta de servicio emitiendo los mandatos siguientes: <pre>kubectl get serviceaccount -n namespace kubectl delete serviceaccount --all -n namespace</pre> </li> <li>3. Suprima la política de red emitiendo los mandatos siguientes: <pre>kubectl get networkpolicy -n namespace kubectl delete networkpolicy --all -n namespace</pre> </li> <li>4. Suprima la PVC y PV: <p>Una PVC que se crea durante una operación de copia de seguridad de copia tiene el siguiente convenio de denominación:</p> <pre>pvc-backup-pvcname-jobid-job_timestamp</pre> <p>Emita los mandatos siguientes:</p> <pre>kubectl get pvc -n namespace   grep pvc-backup kubectl get pvc -n namespace   grep pvc-backup   awk '{print \$1}'   xargs kubectl delete pvc -n namespace</pre> <p>Si todavía hay algún PV, emita los mandatos siguientes:</p> <pre>kubectl get pv   grep pvc-backup kubectl get pv   grep pvc-backup   awk '{print \$1}'   xargs kubectl delete pv</pre> </li> <li>5. Si es necesario, elimine los objetos volumesnapshot y volumesnapshotcontent emitiendo los mandatos siguientes: <pre>kubectl get volumesnapshot -n namespace kubectl get volumesnapshotcontent</pre> </li> </ol>

#### Tareas relacionadas

[“Recopilación de archivos de registro de Soporte de copia de seguridad de Kubernetes para la resolución de problemas” en la página 550](#)

Puede generar archivos de registro de depuración en el entorno de Kubernetes para resolver problemas de despliegue de las operaciones de Soporte de copia de seguridad de Kubernetes y Soporte de copia de seguridad de Kubernetes en el servidor de IBM Spectrum Protect Plus.

## Resolución de problemas en operaciones de Soporte de copia de seguridad de Kubernetes

Los procedimientos de resolución de problemas están disponibles para ayudarle a diagnosticar y resolver problemas de Soporte de copia de seguridad de Kubernetes.

Se proporcionan las instrucciones siguientes:

- [“Visualización de los archivos de registro” en la página 558](#)
- [“Resolución de problemas con trabajos de copia de seguridad de instantánea” en la página 558](#)
- [“Resolución de problemas con trabajos de copia de seguridad de copia” en la página 560](#)
- [“Resolución de problemas de los trabajos de restauración” en la página 562](#)

### Visualización de los archivos de registro

Para resolver problemas de Soporte de copia de seguridad de Kubernetes, empiece por visualizar la información en los archivos de registro. Los archivos de registros están disponibles para el gestor de transacción, el controlador y los componentes del planificador de Soporte de copia de seguridad de Kubernetes.

Puede ver los archivos de registro para varios componentes del gestor de transacción. Por ejemplo, para ver los archivos de registro para uno de los componentes del gestor de transacción, emita el siguiente mandato:

```
kubectl logs -f $(kubectl get pods -n baas | awk '/baas-transaction-manager/ {print $1;exit}') -n baas -c baas-transaction-manager -f
```

Para ver el archivo de registro para el trabajador gestor de transacción, emita el mandato siguiente:

```
kubectl logs -f $(kubectl get pods -n baas | awk '/baas-transaction-manager/ {print $1;exit}') -n baas -c baas-transaction-manager-worker -f
```

Para ver el archivo de registro para el componente de controlador, emita el siguiente mandato:

```
kubectl logs -f $(kubectl get pods -n baas | awk '/baas-controller/ {print $1;exit}') -n baas -f
```

Para ver el archivo de registro para el componente de planificador, emita el mandato siguiente:

```
kubectl logs -f $(kubectl get pods -n baas | awk '/baas-scheduler/ {print $1;exit}') -n baas -f
```

**Consejo:** Para ayudar a acelerar la visualización de los archivos de registro, puede añadir el distintivo **--since=duration** al mandato **kubectl logs** para devolver solo registros que son más recientes que una duración relativa. Puede especificar la duración en segundos (Ns), minutos (Nm) u horas (Nh).

Por ejemplo, para ver los archivos de registro para el componente planificador que tienen más de 3 horas, emita el mandato siguiente:

```
kubectl logs -f $(kubectl get pods -n baas | awk '/baas-scheduler/ {print $1;exit}') -n baas -f --since=3h
```

### Resolución de problemas con trabajos de copia de seguridad de instantánea

Si una operación de copia de seguridad de instantánea no se ha realizado correctamente, puede realizar una serie de acciones para diagnosticar el problema.

Antes de comenzar, asegúrese de que el nivel de rastreo se establece en DEBUG. Para obtener instrucciones sobre el establecimiento del nivel de rastreo de los archivos de registro, consulte [“Establecimiento del nivel de rastreo de los archivos de registro” en la página 551](#).

Complete los pasos siguientes para resolver problemas de copia de seguridad de instantánea:

1. Asegúrese de que los archivos de registro de Soporte de copia de seguridad de Kubernetes estén disponibles. Para obtener instrucciones sobre la visualización de los archivos de registro, consulte [“Visualización de los archivos de registro”](#) en la página 558.
2. Si IBM Spectrum Protect Plus envía la solicitud de instantánea, compruebe el registro de contenedor baas-transaction-manager en el pod baas-transaction-manager. En el archivo de registro, busque texto similar al ejemplo siguiente:

```
/createvolumesnapshot/demo/demo-vol01 Begin
Received parameters {'metadata.name': 'k8s18-1004-2222-1727b1c0828',
'spec.snapshotClassName':
'cirrus-csi-rbdplugin-snapclass', 'metadata.labels': {'storage.kubernetes.io/pvc': 'demo-
vol01'}}}
```

El nombre de instantánea esperado es el valor de la clave `metadata.name`.

A continuación, busque la llamada `createsnapshot` en el ejemplo siguiente:

```
2020-06-03 16:55:43,579[MainThread][kubernetes_api:createsnapshot Line 1056][INFO] -
{'apiVersion':
'snapshot.storage.k8s.io/v1alpha1', 'kind': 'VolumeSnapshot', 'metadata': {'annotations':
{}}, 'name':
'k8s18-1004-2222-1727b1c0828', 'namespace': 'demo', 'labels': {'app.kubernetes.io/
component': 'snapshot',
'app.kubernetes.io/managed-by': 'baas', 'app.kubernetes.io/name': 'baas', 'app.kubernetes.io/
version': '10.1.6',
'storage.kubernetes.io/pvc': 'demo-vol01'}}}, 'spec': {'snapshotClassName': 'cirrus-csi-
rbdplugin-snapclass',
'source': {'kind': 'PersistentVolumeClaim', 'name': 'demo-vol01'}}}
```

3. Si se encuentra una excepción en el Paso 2, es posible que encuentre la siguiente excepción en la llamada `createsnapshot`.

Tabla 67. Posible excepción de la copia de seguridad de instantánea	
Excepción	Acción
La instantánea no existe. Es posible que la instantánea no se haya creado correctamente.	Ejecute el mandato siguiente para determinar si la instantánea se ha creado correctamente:  <pre>kubectl describe volumesnapshots snapshotname -n namespace</pre>

4. Resuelva problemas de IBM Spectrum Protect Plus realizando las siguientes acciones:
  - a. En la interfaz de usuario de IBM Spectrum Protect Plus, verifique si los trabajos de inventario que se han colgado están impidiendo que los demás trabajos se registren en IBM Spectrum Protect Plus.
  - b. Busque el trabajo colgado en la lista de trabajos en ejecución o en el historial de trabajos. Busque los nombres de los trabajos con el siguiente convenio de denominación:

```
k8s_nombre_sla
```

donde *nombre\_sla* es el nombre de la política de SLA asignada a la PVC.

- c. Compruebe los registros de trabajo y resuelva los problemas notificados. Para obtener información sobre cómo ver y descargar los archivos de registro de IBM Spectrum Protect Plus, consulte [“Visualización de los registros de trabajo”](#) en la página 345.

Descargue el paquete de los archivos de registro y expanda el paquete. El paquete descargado tiene el siguiente convenio de denominación:

`JobLog_nombre_trabajo_indicación_fecha_hora_trabajo.zip`.

Para obtener información detallada sobre un trabajo, revise los archivos `command.log` y `JobLog_k8s_nombre_sla_indicación_fecha_hora_trabajo.csv`.

## Resolución de problemas con trabajos de copia de seguridad de copia

Si un trabajo de copia de seguridad de copia no se ha realizado correctamente, puede realizar una serie de acciones para diagnosticar el problema.

Antes de comenzar, asegúrese de que el nivel de rastreo de los archivos de registro esté establecido en DEBUG. Para obtener instrucciones sobre el establecimiento del nivel de rastreo de los archivos de registro, consulte [“Establecimiento del nivel de rastreo de los archivos de registro”](#) en la página 551.

Complete los pasos siguientes para resolver problemas de copia de seguridad de copia:

1. Asegúrese de que los archivos de registro de Soporte de copia de seguridad de Kubernetes estén disponibles. Para obtener instrucciones sobre la visualización de los archivos de registro, consulte [“Visualización de los archivos de registro”](#) en la página 558.
2. Verifique si el agente de IBM Spectrum Protect Plus está enviando una solicitud al planificador de IBM Spectrum Protect Plus. Abra el archivo de registro del planificador y busque texto que sea similar al ejemplo siguiente:

```
Planificar copia de datos para instantánea: demo:pvc-backup-demo-vol01-1004-1591203980176
```

El convenio de denominación para la copia de seguridad de copia de la PVC es:

```
namespace:pvc-backup-pvcname-jobid-job_timestamp
```

Busque la llamada al gestor de transacción para desplegar un transportador de datos, como el ejemplo siguiente:

```
url tmCopyBackupRequest: https://baas-transaction-manager:5000/datamover/demo/pvc-backup-demo-vol01-1004-1591203980176"
```

Si el planificador no envía solicitudes de copia de seguridad de copia, investigue y resuelva los problemas del planificador.

3. Si el planificador está enviando la solicitud de instantánea, compruebe el registro de contenedor baas-transaction-manager en el pod baas-transaction-manager. En el archivo de registro del gestor de transacción, busque la llamada de creación de transportador de datos en el texto que sea similar al ejemplo siguiente:

```
/datamover/demo/pvc-backup-demo-vol01-1004-1591203980176 method=POST
2020-06-03 17:11:26,455[MainThread][main:createdatamover Line 1187][DEBUG] - Creación de despliegue backup-demo-vol01-k8s-k8s18-copy2-1591203980176 for PVC demo:pvc-backup-demo-vol01-1004-1591203980176
```

En el registro baas-transaction-manager-worker del pod baas-transaction-manager, el inicio de la solicitud muestra el ID de tarea, la solicitud COPYBACKUP, el nombre de despliegue o el nombre del transportador de datos y el nombre del volumen:

```
2020-06-03 17:11:26,589: DEBUG/MainProcess] TaskPool: Apply <function _fast_trace_task at 0x7ff1707ac268> (args:('main.backgroundprocess', '29606e23-b6e3-4965-8156-930b42c12a25', {'lang': 'py', 'task': 'main.backgroundprocess', 'id': '29606e23-b6e3-4965-8156-930b42c12a25', 'shadow': None, 'eta': None, 'expires': None, 'group': None, 'retries': 0, 'timelimit': [None, None], 'root_id': '29606e23-b6e3-4965-8156-930b42c12a25', 'parent_id': None, 'argsrepr': '(\n  'COPYBACKUP',\n  {'command': 'backup', 'namespace': 'demo', 'deploymentName': 'backup-demo-vol01-k8s-k8s18-copy2-1591203980176', 'volumename': 'pvc-backup-demo-vol01-1004-1591203980176', 'vSnapIPAddresses': ['9.11.62.84'], 'vSnapMountPath': '/vsnap/vpool1/fs489', 'kafkaAddress': 'baas-kafka-svc.baas:9092', 'kafkaStatusLog': 'backup-demo-vol01-k8s-k8s18-copy2-1591203980176-status', 'kafkaCommandLog': 'backup-demo-vol01-k8s-k8s18-copy2-1591203980176-command', 'storageClass': None, 'sizeInBytes': None, 'pvclabels': {}}),\n  {'kwargsrepr': '{', 'origin': 'gen28@baas-transaction-manager-69cffc84fd-95kc4', 'reply_to': '38ff7ee8-718f-3b14-bd70-8a3f866823f6', 'correlation_id': ... kwargs:{}})\n[2020-06-03 17:11:26,593: DEBUG/MainProcess] Tarea aceptada: main.backgroundprocess[29606e23-b6e3-4965-8156-930b42c12a25] pid:24

Crear transportador de datos demo:backup-demo-vol01-k8s-k8s18-copy2-1591203980176 PVC=pvc-backup-demo-vol01-1004-1591203980176 isBackup=True
```

```
[2020-06-03 17:11:27,127: INFO/ForkPoolWorker-1] Task main.backgroundprocess[29606e23-b6e3-4965-8156-930b42c12a25] succeeded in 0.5342374939937145s: 0
```

En el registro del gestor de transacción, la siguiente sentencia de rastreo muestra si el despliegue ha tenido éxito o si ha fallado con la llamada `Get deployment`:

```
Obtener despliegue backup-demo-vol01-k8s-k8s18-copy2-1591203980176 for PVC demo:backup-demo-vol01-k8s-k8s18-copy2-1591203980176
```

4. En el registro de planificador, verifique si se ha completado la copia de seguridad de copia buscando rastreos similares a los ejemplos siguientes:

```
copyBackup volume:demo:pvc-backup-demo-vol01-1004-1591203980176 jobInfoId=1004  
ipAddr=[9.11.62.84] fileLocation= volumeSize=1073.741824 nextRunTime=1591290380176"
```

```
Configuración de la copia de seguridad para completar para copyBackup: demopvc-backup-demo-vol01-1004-1591203980176:1591203980176
```

5. Si se encuentra una excepción, es posible que encuentre las siguientes excepciones en la solicitud COPYBACKUP.

Tabla 68. Posibles excepciones de copia de seguridad	
Excepción	Acción
La instantánea no existe. Es posible que la instantánea no se haya creado correctamente.	Ejecute el mandato siguiente para determinar si la instantánea se ha creado correctamente:  <pre>kubectl describe volumesnapshots <i>snapshotname</i> -n <i>namespace</i></pre>
El despliegue no existe. Es posible que el transportador de datos no se haya creado correctamente.	Para obtener más información sobre el problema, obtenga el nombre del transportador de datos del mensaje de error y ejecute el mandato siguiente:  <pre>kubectl describe deploy backup-pvcname-jobname-job_timestamp -n <i>namespace</i></pre>

6. Resuelva problemas de IBM Spectrum Protect Plus realizando las siguientes acciones:
- En la interfaz de usuario de IBM Spectrum Protect Plus, verifique si los trabajos de inventario que se han colgado están impidiendo que los demás trabajos se registren en IBM Spectrum Protect Plus.
  - Busque el trabajo colgado en la lista de trabajos en ejecución o en el historial de trabajos. Busque los nombres de los trabajos con el siguiente convenio de denominación:

```
k8s_nombre_sla
```

donde *nombre\_sla* es el nombre de la política de SLA asignada a la PVC.

- Compruebe los registros de trabajo y resuelva los problemas notificados. Para obtener información sobre cómo ver y descargar los archivos de registro de IBM Spectrum Protect Plus, consulte [“Visualización de los registros de trabajo”](#) en la página 345.

Descargue el paquete de los archivos de registro y expanda el paquete. El paquete descargado tiene el siguiente convenio de denominación:

```
JobLog_nombre_trabajo_indicación_fecha_hora_trabajo.zip.
```

Para obtener información detallada sobre un trabajo, revise los archivos `command.log` y `JobLog_k8s_nombre_sla_indicación_fecha_hora_trabajo.csv`.

## Resolución de problemas de los trabajos de restauración

Si un trabajo de restauración se ha realizado correctamente, puede realizar las siguientes acciones para diagnosticar el problema.

Antes de comenzar, asegúrese de que el nivel de rastreo se establece en DEBUG. Para obtener instrucciones sobre el establecimiento del nivel de rastreo de los archivos de registro, consulte [“Establecimiento del nivel de rastreo de los archivos de registro”](#) en la página 551.

Complete los pasos siguientes para resolver problemas del trabajo de restauración:

1. Asegúrese de que los archivos de registro de Soporte de copia de seguridad de Kubernetes estén disponibles. Para obtener instrucciones sobre la visualización de los archivos de registro, consulte [“Visualización de los archivos de registro”](#) en la página 558.
2. Compruebe si hay errores en el registro de trabajo de restauración del servidor de IBM Spectrum Protect Plus denominado `onDemandRestore_timestamp`.

Si se ha iniciado el trabajo de restauración desde la línea de mandatos **kubect1**, puede buscar el nombre del trabajo de restauración en los objetos BaasReq mientras el trabajo de restauración está en curso emitiendo el siguiente mandato:

```
kubect1 describe baasreq restore_request_name -n namespace | grep Inprogress
```

Busque la salida que sea similar al ejemplo siguiente:

```
Inprogress: onDemandRestore_1591384200276
```

3. Si ha restaurado datos desde la línea de mandatos **kubect1**, compruebe si la solicitud de restauración se ha invalidado debido a parámetros no válidos en el archivo de configuración YAML. Utilice el mandato **kubect1 describe** para comprobar el estado de restauración (`Restorestatus`) en la salida.

Si el valor del campo `Restorestatus` es `Invalid`, el campo `Errmsg` mostrará el motivo por el que se ha invalidado la solicitud de restauración. En el ejemplo siguiente, se ha especificado un valor incorrecto en el parámetro **VolumeStorageClass** del archivo YAML.

Por ejemplo, para mostrar el estado de restauración de la solicitud de restauración `copy-restore-pvc02` en el espacio de nombres `test`, emita el mandato siguiente:

```
kubect1 describe baasreq copy-restore-pvc02 -n test
```

La salida es similar a la que se muestra en el ejemplo siguiente:

```
Name:          copy-restore-pvc02
Namespace:     test
Labels:        <none>
Annotations:   <none>
API Version:   baas.io/v1alpha1
Backupstatus:  None
Errmsg:        VolumeStorageClass invalid
Kind:          BaaSReq
Metadata:
  Creation Timestamp:  2020-06-05T19:51:29Z
  Generation:         2
  Resource Version:    4396987
  Self Link:           /apis/baas.io/v1alpha1/namespaces/test/baasreqs/copy-restore-pvc02
  UID:                418cc8d5-7347-47ed-9436-9fe49f69b42a
Restorestatus:  Invalid
Spec:
  Inprogress:      None
  Origreqtype:     restore
  Pvcname:         pvc02
  Requesttype:     restore
  Restorepoint:    2020-06-05 17:22:35
  Restoretype:     copy
  Storageclass:    cirrus19-csi-rbd-sc
  Targetvolume:    pvc02-restored
Volumename:      pvc02
Events:           <none>
```



Para recuperarse de este tipo de error, suprima la solicitud de restauración no válida, corrija el archivo YAML y vuelva a crear la solicitud de restauración.

4. Revise los mensajes de error del servidor IBM Spectrum Protect Plus en el registro `onDemandRestore_timestamp`. Los mensajes de error suelen ser suficiente para ayudarlo a diagnosticar el problema.
5. Para solucionar problemas adicionales de una restauración de instantánea, puede buscar rastreos en el registro de trabajo `baas-spp-agent` del agente de aplicación que sean similares al ejemplo siguiente:

```
DEBUG pid:3402 MainThread restoreDatabase: Inicio de la restauración de instantánea
spp-1275-2213-17285db4b80 en test-snap-restore-pvc1
DEBUG pid:3402 MainThread restoreDatabase: Restauración de etiquetas pvc {'department':
'sales', 'team': 'green'}
DEBUG pid:3402 MainThread restoreDatabase: Restauración de instantánea llamada
spp-1275-2213-17285db4b80
DEBUG pid:3402 MainThread sendRestoreRequest: Envío de la solicitud de restauración a
https://baas-transaction-manager:5000/restorevolumebackup/test/test-snap-restore-pvc1?
storageclass=cirrus-csi-rbd-sc&restoretype=FAST
DEBUG pid:3402 MainThread sendRestoreRequest: Obtener respuesta de restauración
```

Compruebe el registro de contenedor `baas-transactionmanager` en el pod `baas-transaction-manager`. En el archivo de registro, busque texto similar al ejemplo siguiente:

```
/restorevolumebackup/test/test-snap-restore-pvc1 snapshot:spp-1275-2213-17285db4b80
restoretype:FAST
storageclass: cirrus-csi-rbd-sc
```

6. Para solucionar problemas adicionales de una restauración de copia, puede buscar rastreos en el registro de trabajo `baas-spp-agent` del agente de aplicación que sean similares al ejemplo siguiente:

```
JOBLOG_SUMMARY pid:4219 MainThread jobsummary: <CTGGK3005> Starting to restore a persistent
volume.
DEBUG pid:4219 MainThread copyRestore: Iniciando restauración de la base de datos
cirrus19:test:pvc02
DEBUG pid:4219 MainThread getPVC: PVC test:test-copy-restore-pvc02 not found.
DEBUG pid:4219 MainThread copyRestore: PVC does not exist, the restore can continue.
DEBUG pid:4219 MainThread createDatamover: PVC labels {'department': 'sales', 'team':
'green'}
INFO pid:4219 MainThread createDatamover: Create datamover request to https://baas-
transaction-manager:5000/datamover/test/test-copy-restore-pvc02
```

Compruebe el registro de contenedor `baas-transactionmanager` en el pod `baas-transaction-manager`. En el archivo de registro, busque texto similar al ejemplo siguiente:

```
main:createdatamover Line 1187][DEBUG] - Creating deployment
restore-pvc02-ondemandrestore-1591390864757-1591390865107 for PVC test:test-copy-restore-
pvc02
```

En el archivo de registro `transaction-manager-worker`, busque texto similar al ejemplo siguiente:

```
DEBUG/ForkPoolWorker-1] Restore worker
DEBUG/ForkPoolWorker-1] Create datamover test:restore-pvc02-
ondemandrestore-1591390864757-1591390865107
PVC=test-copy-restore-pvc02 isBackup=False
```

## Tareas relacionadas

[“Establecimiento del nivel de rastreo de los archivos de registro” en la página 551](#)

Puede establecer el nivel de rastreo de los archivos de registro locales para ayudarlo a resolver los problemas que puede encontrarse en Soporte de copia de seguridad de Kubernetes.

## Referencia relacionada

[“Consulta rápida de resolución de problemas” en la página 554](#)

Se proporcionan soluciones a problemas de Soporte de copia de seguridad de Kubernetes básicos.



## Capítulo 21. 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 69. 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
CTGGK	IBM Spectrum Protect Plus para contenedores
CTGGL	IBM Spectrum Protect Plus para Amazon EC2
CTGGR	IBM Spectrum Protect Plus para Microsoft Office 365
CTGGT	IBM Spectrum Protect Plus para sistemas de archivos

Para ver una lista de los mensajes, consulte el IBM Knowledge Center [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 `cadena`, `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 solo 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](http://www.w3.org/TR/wai-aria/) ([www.w3.org/TR/wai-aria/](http://www.w3.org/TR/wai-aria/)), para asegurar el cumplimiento de la [US Section 508](http://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/section-508-standards) ([www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/section-508-standards](http://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](http://www.w3.org/TR/WCAG20/) ([www.w3.org/TR/WCAG20/](http://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](http://www.ibm.com/support/knowledgecenter/about/releasenotes.html?view=kc#accessibility) ([www.ibm.com/support/knowledgecenter/about/releasenotes.html?view=kc#accessibility](http://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\(www.ibm.com/able\)](http://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 solo 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.

#### LICENCIA DE COPYRIGHT:

Esta información contiene programas de aplicación de ejemplo en lenguaje fuente, que ilustra las técnicas de programación en distintas plataformas operativas. Puede copiar, modificar y distribuir estos programas de ejemplo de cualquier forma sin previo pago a IBM, para fines de desarrollo, utilización, marketing o distribución de programas de aplicación conforme a la interfaz de programación de aplicaciones de la plataforma operativa para la que están escritos estos programas de ejemplo. Estos ejemplos no se han probado a fondo bajo todas las condiciones. Por tanto, IBM no puede garantizar ni implicar la fiabilidad, utilidad o función de estos programas. Los programas de ejemplo se proporcionan "TAL CUAL", sin garantía de ningún tipo. IBM no será responsable de ningún daño que surja del uso por parte del usuario de los programas de ejemplo.

Todas las copias o partes de estos programas de ejemplo o cualquiera de sus derivados deben incluir un aviso de copyright como el siguiente: © (nombre de la empresa) (año). Partes de este código se derivan de IBM Corp. Sample Programs. © Copyright IBM Corp. \_escriba el año o años\_.

#### **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](http://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.

La marca registrada Linux se utiliza de acuerdo con una sublicencia de Linux Foundation, el titular exclusivo de la licencia de Linus Torvalds, propietario de la marca en todo el mundo.

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 registradas de VMware, Inc. o sus filiales en Estados Unidos u 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

## A

acceso de usuarios [11](#), [533](#)  
Actualización  
    Servidor vSnap [184](#)  
actualizaciones de disponibilidad anticipada, obtener y aplicar [190](#)  
actualizaciones en línea [187](#)  
actualizaciones fuera de línea [187](#)  
acuerdo de nivel de servicio, Véase políticas de SLA  
Acuerdos de nivel de servicio  
    Soporte de copia de seguridad de Kubernetes [331](#)  
Adición de MongoDB [449](#)  
Adición de un sistema de archivos [310](#)  
agrupación de almacenamiento de memoria caché de datos fríos [200](#)  
almacenamiento de copias de seguridad  
    opciones avanzadas, gestionar [124](#)  
    opciones de almacenamiento, gestión de discos [120](#)  
    opciones de almacenamiento, gestión de socios [122](#)  
Almacenamiento de objetos  
    Amazon S3 [192](#)  
Amazon EC2  
    cuentas  
        añadir [299](#)  
    detección de recursos [300](#)  
    trabajo de copia de seguridad, crear [300](#)  
    usuario de IAM, creación [298](#)  
añadir  
    cuenta de Amazon EC2 [299](#)  
    discos virtuales a una máquina virtual vCenter [228](#)  
    identidades [544](#)  
    instancias de vCenter Server [257](#)  
    servidor LDAP [216](#)  
    servidor SMTP [217](#)  
    servidores de aplicaciones de SQL Server [489](#)  
    servidores de aplicaciones Oracle [476](#)  
    servidores Hyper-V [284](#)  
    servidores vSnap [117](#)  
    sitios [213](#)  
añadir Db2 [378](#)  
añadir particiones Db2 [378](#)  
Archivado de registros  
    Db2 [388](#)  
archivos  
    buscar [567](#)  
    restaurar [305](#)  
archivos de registro de despliegueSoporte de copia de seguridad de Kubernetes [550](#)  
Archivos de registro de O365  
    Detallados [371](#)  
archivos YAML  
    Soporte de copia de seguridad de Kubernetes [348](#)  
AWS EC2  
    trabajo de restauración, crear [302](#)

## B

Búsqueda de Db2 [380](#)  
Búsqueda de unidades de sistema de archivos [312](#)

## C

caducidad de trabajos  
    Soporte de copia de seguridad de Kubernetes [344](#)  
característica VolumeSnapshotDataSource  
    Soporte de copia de seguridad de Kubernetes [153](#)  
características de accesibilidad [569](#)  
características de seguridad  
    Soporte de copia de seguridad de Kubernetes [333](#)  
Centro de operaciones  
    Acceso desde IBM Spectrum Protect Plus [16](#)  
    adición de IBM Spectrum Protect Plus a [17](#)  
    inicio desde IBM Spectrum Protect Plus [20](#)  
    supervisión de IBM Spectrum Protect Plus desde [16](#), [20](#)  
    URL, establecimiento [19](#)  
certificado  
    añadir [221](#)  
    suprimir [221](#)  
certificado SSL, cargar  
    desde la consola de administración [223](#)  
clave  
    añadir [220](#), [221](#)  
    suprimir [220](#), [223](#)  
claves [220](#)  
cliente objeto [207](#), [209](#)  
clúster Kubernetes  
    detección de recursos [337](#)  
Clúster Kubernetes  
    probar conexión con [338](#)  
Configuración de red [121](#)  
Configuración del almacenamiento de copias de seguridad  
    opciones de almacenamiento, adición de discos [121](#)  
configurar en Kubernetes  
    Soporte de copia de seguridad de Kubernetes [156](#)  
consola de administración, iniciar sesión en [219](#)  
control de acceso  
    MongoDB [447](#)  
copia de datos en cintas  
    configuración [200](#)  
copia de reserva  
    Soporte de copia de seguridad de Kubernetes [350](#)  
copia de seguridad  
    datos de contenedor [350](#)  
Copia de seguridad  
    datos del sistema de archivos [314](#)  
    Db2 [382](#)  
copia de seguridad bajo demanda  
    contenedores [353](#)  
copia de seguridad de instantánea  
    contenedores [353](#)  
    Soporte de copia de seguridad de Kubernetes [350](#)  
copia de seguridad de los datos de contenedor

copia de seguridad de los datos de contenedor (*continuación*)

bajo demanda [353](#)

planificar [338](#), [350](#)

por espacio de nombres [358](#)

por etiqueta [355](#)

Copia de seguridad de registro de Db2 [388](#)

copia de seguridad por espacio de nombres

Soporte de copia de seguridad de Kubernetes [358](#)

copia de seguridad por etiqueta

Soporte de copia de seguridad de Kubernetes [355](#)

copias de seguridad de copia

Kubernetes [338](#)

copias de seguridad de instantánea

Kubernetes [338](#)

cortafuegos [108](#)

creación de un secreto de extracción de imagen

Soporte de copia de seguridad de Kubernetes [153](#)

crear

grupos de recursos [534](#)

informes [529](#)

políticas de SLA [244](#), [248](#), [250](#)

proxies VADP [268](#)

roles [539](#)

usuarios

grupo LDAP [543](#)

individuales [542](#)

## D

Db2

requisitos del sistema [62](#)

definición de copias de seguridad de SLA

Kubernetes [338](#)

demo

sitio [238](#)

SLA [238](#)

vSnap [238](#)

Desinstalación de

Soporte de copia de seguridad de Kubernetes [162](#)

desplegar en Kubernetes

Soporte de copia de seguridad de Kubernetes [156](#)

destrucción de copias de seguridadSoporte de copia de seguridad de Kubernetes [366](#)

Detección

Db2 [380](#)

Recursos de sistema de archivos [312](#)

discapacidad [569](#)

dispositivo virtual

acceder

en Hyper-V [226](#)

en VMware [225](#)

añadir capacidad de almacenamiento [229](#)

añadir un disco a [228](#)

instalar

en Hyper-V [105](#)

en VMware [103](#)

Dispositivo virtual

actualizar [187](#)

dispositivo virtual vCenter basado en Linux, copia de seguridad [267](#)

## E

editar

grupos de recursos [537](#)

identidades [545](#)

políticas de SLA [255](#)

roles [541](#)

servidor LDAP [218](#)

servidor SMTP [218](#)

sitios [214](#)

trabajos y planificaciones de trabajos [515](#)

usuarios [543](#)

valores [218](#)

efix [190](#)

ejecución de informes

trabajos de copia de seguridad de contenedor [345](#)

eliminación

demo [238](#)

eliminación de asignaciones de política de SLA

Kubernetes [338](#)

entornos virtuales [207](#), [209](#)

Establecimiento de Db2

Opciones de SLA [387](#)

establecimiento de niveles de rastreo

Soporte de copia de seguridad de Kubernetes [551](#)

Exchange Server

requisitos del sistema [68](#)

## G

gestión de trabajos

copias de seguridad y restauraciones de contenedor [363](#)

grupos de recursos

crear [534](#)

editar [537](#)

suprimir [537](#)

tipos de [535](#)

## H

habilitar rastreo

Soporte de copia de seguridad de Kubernetes [551](#)

hacer caducar la sesión de trabajo [507](#)

huso horario, establecer [224](#)

Hyper-V

añadir [284](#)

dispositivo virtual

acceder [226](#)

instalar en dispositivo virtual [105](#)

servidores

detectar recursos para [285](#)

habilitar WinRM [285](#)

probar conexión con [286](#)

trabajo de copia de seguridad, crear [286](#)

trabajo de restauración, crear [290](#)

## I

IBM Knowledge Center [ix](#)

IBM Spectrum Protect Operations Center

Acceso desde IBM Spectrum Protect Plus [16](#)

adición de IBM Spectrum Protect Plus a [17](#)



- IBM Spectrum Protect Operations Center (*continuación*)
  - inicio desde IBM Spectrum Protect Plus [20](#)
  - supervisión de IBM Spectrum Protect Plus desde [16](#), [20](#)
  - URL, establecimiento [19](#)
- identidades
  - añadir [544](#)
  - editar [545](#)
  - suprimir [545](#)
- informes
  - ejecutar
    - bajo demanda [528](#)
    - según lo planificado [530](#)
  - máquinas virtuales en ejecución [527](#)
  - personalizados, crear [529](#)
  - tipos de
    - protección [522](#)
    - sistema [525](#)
    - utilización del almacenamiento de copias de seguridad [521](#)
- iniciar
  - IBM Spectrum Protect Plus [167](#)
  - trabajos
    - bajo demanda [512](#)
    - según lo planificado [244](#), [248](#), [250](#)
- inicio rápido [165](#)
- inscripción
  - clústeres Kubernetes [335](#)
  - servidores vSnap [117](#)
- instalación
  - Soporte de copia de seguridad de Kubernetes [153](#)
- instalar
  - descargar paquetes, obtener [102](#)
  - dispositivo virtual
    - en Hyper-V [105](#)
    - en VMware [103](#)
  - servidores vSnap
    - entorno físico [111](#)
    - entorno Hyper-V [114](#)
    - entorno VMware [112](#)
- instalar en Kubernetes
  - Soporte de copia de seguridad de Kubernetes [156](#)
- inventario
  - sistemas de archivos [312](#)

## K

- Knowledge Center [ix](#)
- Kubernetes
  - clústeres
    - modificar propiedades [335](#)
    - registrar manualmente [335](#)

## L

- LDAP
  - grupo, crear una cuenta de usuario para [543](#)
  - servidor
    - añadir [216](#)
    - suprimir [219](#)
    - valores, editar [218](#)
- localhost
  - vSnap [238](#)

## M

- mandato DEFINE STGPOOL [200](#)
- mensaje
  - prefijos [565](#)
- mensajes [565](#)
- modificación de propiedades
  - clústeres Kubernetes [335](#)
- MongoDB
  - requisitos del sistema [74](#)
- multitenencia
  - Soporte de copia de seguridad de Kubernetes [329](#), [333](#)

## N

- NIC [121](#)
- Novedades de IBM Spectrum Protect Plus Versión Versión 10.1.6 [xi](#)

## O

- Office 365 [369](#)
- Opciones de copia de seguridad avanzadas [124](#)
- Opciones de SLA
  - Db2 [387](#)
- Ops Manager
  - MongoDB [451](#)
- Oracle
  - bases de datos multihebra [476](#)
  - requisitos del sistema [85](#)
  - servidores de aplicaciones
    - añadir [476](#)
    - detectar recursos para [477](#)
    - probar conexión con [478](#)
  - trabajo de copia de seguridad, crear [478](#)
  - trabajo de restauración, crear [481](#)

## P

- planificar copias de seguridad
  - Kubernetes [338](#)
  - Soporte de copia de seguridad de Kubernetes [350](#)
- planificar trabajos
  - copia de seguridad [384](#), [407](#), [455](#)
- políticas de copia de seguridad, Véase políticas de SLA
- políticas de SLA
  - añadir [244](#), [248](#), [250](#)
  - editar [255](#)
  - Soporte de copia de seguridad de Kubernetes [350](#)
  - suprimir [255](#)
- Políticas de SLA
  - Soporte de copia de seguridad de Kubernetes [331](#)
- preferencias
  - globales
    - configuración [232](#)
  - preferencias globales
    - configuración [232](#)
- Probando conexión
  - Db2 [381](#)
- Programa beta
  - ventajas [xiii](#)
  - visión general [xiii](#)
- programa de usuario patrocinador

- programa de usuario patrocinador (*continuación*)
  - ventajas [xiii](#)
  - visión general [xiii](#)
- programas de utilidad iSCSI
  - instalación [110](#)
- protección de datos [207](#), [209](#)
- proveedor de nube
  - editar [198](#)
  - suprimir [198](#)
- proveedor de servidores de repositorio
  - editar [212](#)
  - suprimir [212](#)
- proxies VADP
  - actualizar [189](#)
  - crear [268](#)
  - desinstalar [272](#)
  - opciones, establecer [271](#)
- Prueba de conexión sistemas de archivos [314](#)
- publicaciones [ix](#)
- puntos de restauración, gestionar [506](#)
- puntos de restauración, suprimir [507](#)

## R

- RBAC
  - MongoDB [447](#)
- recopilación de archivos de registro de depuraciónSoporte de copia de seguridad de Kubernetes [550](#)
- recuperación de vSnap [131](#)
- red
  - probar [226](#), [227](#)
- red delimitada, crear [280](#)
- registro manual
  - clústeres Kubernetes [335](#)
- registros
  - auditar
    - descargar [531](#)
    - visualizar [531](#)
  - sistema
    - descargar [549](#)
    - visualizar [549](#)
- Registros de procesos detallados
  - O365 [371](#)
- reparar vSnap [131](#)
- requisitos del sistema
  - componentes [23](#)
  - Db2 [62](#)
  - Exchange Server [68](#)
  - hipervisores [41](#)
  - indexación y restauración de archivos [44](#)
  - MongoDB [74](#)
  - Oracle [85](#)
  - sistemas de archivos [51](#)
  - Soporte de copia de seguridad de Kubernetes [56](#)
  - SQL Server [93](#)
- requisitos previos
  - Db2 [375](#)
  - MongoDB [446](#), [447](#)
  - sistemas de archivos [309](#)
  - Soporte de copia de seguridad de Kubernetes [153](#)
- resolución de problemas
  - operaciones Soporte de copia de seguridad de Kubernetes [558](#)
  - Soporte de copia de seguridad de Kubernetes [550](#)

- resolución de problemas (*continuación*)
  - visualización de registros de Soporte de copia de seguridad de Kubernetes [558](#)
- Restauración
  - Db2 [389](#), [395](#), [399](#)
  - sistema de archivos [321](#)
- restauración de copia
  - datos de contenedor [360](#)
  - volúmenes persistentes [341](#)
- restauración de datos [341](#)
- restauración de datos de contenedor
  - Soporte de copia de seguridad de Kubernetes [360](#)
- Restauración de Db2
  - Instancia alternativa [399](#)
  - Instancia original [395](#)
- restauración de instantánea
  - volúmenes persistentes [341](#)
- restauración de volúmenes persistentes
  - Kubernetes [341](#)
- restauración rápida
  - datos de contenedor [360](#)
- retención de instantáneas [507](#)
- roles
  - crear [539](#)
  - editar [541](#)
  - suprimir [542](#)
  - tipos de permisos [539](#)
- roles de usuario
  - Soporte de copia de seguridad de Kubernetes [332](#)

## S

- scripts para operaciones de copia de seguridad y restauración
  - cargar [519](#)
- servidor de almacenamiento de copias de seguridad
  - opciones de almacenamiento, gestionar [121](#), [123](#)
- servidor de aplicaciones
  - Db2 [375](#)
- servidor de aplicaciones MongoDB [446](#)
- servidor de nube
  - adición de Amazon S3 [192](#)
  - adición de un recurso de nube de s3 compatible [196](#)
  - añadir un recurso de IBM Cloud Object Storage [193](#)
  - añadir un recurso de nube de Microsoft Azure [195](#)
- servidor IBM Spectrum Protect
  - añadir un servidor de repositorio [210](#)
  - registro de un servidor de repositorio [210](#)
- servidor vSnap
  - administrar
    - administración de almacenamiento [133](#)
    - administración de red [136](#)
  - agrupaciones de almacenamiento, expandir [130](#)
  - Anulación del registro [118](#)
  - editar [118](#)
  - inicializar
    - avanzado [129](#)
    - simple [129](#)
  - modificar rendimiento [130](#)
- Servidor vSnap
  - administrar
    - administración de usuarios [132](#)
    - cabeceras de kernel
    - herramientas de kernel [137](#)

- servidores vSnap
    - añadir [117](#)
    - desinstalar [115](#)
    - inscripción [117](#)
    - instalar
      - entorno físico [111](#)
      - entorno Hyper-V [114](#)
      - entorno VMware [112](#)
  - sistemas de archivos
    - requisitos del sistema [51](#)
  - sitios
    - añadir [213](#)
    - editar [214](#)
    - regulación [213](#), [214](#)
    - suprimir [215](#)
  - SLA [384](#), [407](#), [455](#)
  - SMTP
    - servidor
      - añadir [217](#)
      - suprimir [219](#)
      - valores, editar [218](#)
  - Socios de replicación [122](#)
  - Soporte de copia de seguridad de Kubernetes
    - acciones en cascada [153](#)
    - archivo de configuración [156](#)
    - caducidad de trabajos [344](#)
    - cifrado [333](#)
    - copia de reserva [350](#)
    - copia de seguridad de instantánea [350](#), [353](#)
    - copia de seguridad de los datos de contenedor [350](#)
    - copia de seguridad de PVC por espacio de nombres [358](#)
    - copia de seguridad de PVC por etiqueta [355](#)
    - copia de seguridad por espacio de nombres [358](#)
    - copia de seguridad por etiqueta [355](#)
    - creación de un secreto de extracción de imagen [153](#)
    - desinstalar [162](#)
    - destruir solicitud [366](#)
    - ejecución de informes [345](#)
    - establecimiento de niveles de rastreo [551](#)
    - estado de copia de seguridad [365](#)
    - estado de la restauración [365](#)
    - gestión de trabajos [363](#)
    - habilitar característica VolumeSnapshotDataSource [153](#)
    - habilitar rastreo [551](#)
    - instalación [153](#)
    - instalar en Kubernetes [156](#)
    - multitenencia [333](#)
    - planificar copias de seguridad [350](#)
    - políticas de SLA [350](#)
    - Políticas de SLA [331](#)
    - recopilación de archivos de registro de depuración [550](#)
    - registros de despliegue [550](#)
    - requisitos del sistema [56](#)
    - requisitos previos [153](#)
    - resolución de problemas [550](#)
    - resolución de trabajos de copia de seguridad [558](#)
    - resolución de trabajos de restauración [558](#)
    - restauración de copia [360](#)
    - restauración de datos [360](#)
    - restauración rápida [360](#)
    - roles de usuario [332](#)
    - seguridad [333](#)
    - solicitudes baas [348](#)
    - supervisión de trabajos [345](#)
  - Soporte de copia de seguridad de Kubernetes (*continuación*)
    - supresión de copias de seguridad [366](#)
    - tipos de copia de seguridad y restauración [330](#)
    - tipos de solicitud [348](#)
    - verificación de Metrics Server [153](#)
    - visión general [329](#)
    - visualización de archivos de registro [558](#)
    - visualización de registros de trabajos [345](#), [552](#)
    - visualización del estado de copia de seguridad [363](#)
    - visualización del estado de la restauración [363](#)
    - visualización del historial de copia de seguridad [346](#)
  - SQL Server
    - requisitos del sistema [93](#)
    - requisitos para la protección de datos [488](#)
    - servidores de aplicaciones
      - añadir [489](#)
      - detectar recursos para [491](#)
      - probar conexión con [491](#)
      - trabajo de copia de seguridad, crear [491](#)
      - trabajo de restauración, crear [496](#)
  - supervisión
    - trabajos de copia de seguridad de contenedor [345](#)
  - supresión de copias de seguridad
    - Soporte de copia de seguridad de Kubernetes [366](#)
  - suprimir
    - demo [238](#)
    - demo de SLA [255](#)
    - grupos de recursos [537](#)
    - identidades [545](#)
    - políticas de SLA [255](#)
    - roles [542](#)
    - servidor LDAP [219](#)
    - servidor SMTP [219](#)
    - sitios [215](#)
    - trabajos [516](#)
    - usuarios [544](#)
- ## T
- teclado [569](#)
  - tipos de copia de seguridad
    - Soporte de copia de seguridad de Kubernetes [330](#)
  - tipos de restauración
    - Soporte de copia de seguridad de Kubernetes [330](#)
  - tipos de solicitud
    - Soporte de copia de seguridad de Kubernetes [348](#)
  - trabajos
    - cancelar [516](#)
    - crear [510](#)
    - editar [515](#)
    - iniciar
      - bajo demanda [512](#)
      - según lo planificado [244](#), [248](#), [250](#)
    - liberar [515](#)
    - nombres de [509](#)
    - pausa [515](#)
    - planificaciones, edición [515](#)
    - progreso, visualización [513](#)
    - registros
      - descargar [514](#)
      - visualizar [514](#)
    - simultáneo, visualización [515](#)
    - suprimir [516](#)
    - tipos [509](#)

- trabajos (*continuación*)
  - visualizar [512](#)
  - volver a ejecutar [517](#)
- trabajos ad hoc
  - crear [517](#)
- trabajos de copia de seguridad
  - crear
    - Amazon EC2 [300](#)
    - Hyper-V [286](#)
    - IBM Spectrum Protect Plus [505](#)
    - Oracle [478](#)
    - SQL Server [491](#)
    - VMware [262](#)
  - excluir VMDK de [266](#)
  - iniciar
    - bajo demanda [512](#)
    - según lo planificado [244](#), [248](#), [250](#)
  - volver a ejecutar
    - bajo demanda [517](#)
- trabajos de restauración
  - crear
    - AWS EC2 [302](#)
    - Hyper-V [290](#)
    - IBM Spectrum Protect Plus [505](#)
    - Oracle [481](#)
    - SQL Server [496](#)
    - VMware [273](#)
  - ejecutar
    - AWS EC2 [302](#)
    - Hyper-V [290](#)
    - Oracle [481](#)
    - SQL Server [496](#)
    - VMware [273](#)
- Trabajos y operaciones [509](#)

## U

- usuarios
  - editar [543](#)
  - grupo LDAP, crear [543](#)
  - grupos de recursos
    - crear [534](#)
    - editar [537](#)
    - suprimir [537](#)
    - tipos de [535](#)
  - individual, crear [542](#)
  - roles
    - crear [539](#)
    - editar [541](#)
    - suprimir [542](#)
    - tipos de permisos [539](#)
  - suprimir [544](#)

## V

- verificación de Metrics Server
  - Soporte de copia de seguridad de Kubernetes [153](#)
- visión general
  - Soporte de copia de seguridad de Kubernetes [329](#)
- visualización de registros de trabajos
  - copias de seguridad de contenedor [345](#)
  - Soporte de copia de seguridad de Kubernetes [552](#)
- visualización del estado de copia de seguridad

- visualización del estado de copia de seguridad (*continuación*)
  - Soporte de copia de seguridad de Kubernetes [363](#), [365](#)
- visualización del estado de la restauración
  - Soporte de copia de seguridad de Kubernetes [363](#), [365](#)
- visualización del historial de copia de seguridad
  - copias de seguridad de contenedor [346](#)
- VMware
  - dispositivo virtual
    - acceder [225](#)
  - instalar en dispositivo virtual [103](#)
  - instancias de vCenter Server
    - añadir [257](#)
  - privilegios de máquinas virtuales, necesarios [259](#)
  - trabajo de copia de seguridad, crear [262](#)
  - trabajo de copia de seguridad, excluir VMDK de la política de SLA [266](#)
  - trabajo de restauración
    - crear una red delimitada [280](#)
  - trabajo de restauración, crear [273](#)
  - vCenter Server, detectar recursos [261](#)
  - vCenter Server, probar conexión con [261](#)
- volver a ejecutar
  - trabajos
    - bajo demanda [517](#)
- vSnap
  - actualizar [186](#)

## W

- WinRM, habilitar para conexión con servidores Hyper-V [285](#)





Número de Programa: 5737-F11

Impreso en EE.UU.