IBM Spectrum Protect
Versión 8.1.0

Guía de soluciones de disco de sitio único

IBM Spectrum Protect
Versión 8.1.0

Guía de soluciones de disco de sitio único

Nota:
Antes de utilizar esta información y el producto al que da soporte, consulte la información de “Avisos” en la página 151.

Esta edición se aplica a la versión 8, release 1, modificación 0 de IBM Spectrum Protect (números de producto 5725-W98, 5725-W99, 5725-X15) y a todos los releases y modificaciones posteriores hasta que se indique lo contrario en nuevas ediciones.

Contenido

Acerca de esta publicación

Esta publicación proporciona información sobre la planificación, implementación, supervisión y funcionamiento de una solución de protección de datos que utiliza las prácticas recomendadas de IBM Spectrum Protect.

A quién está dirigida esta guía

Esta guía está concebida para cualquiera que esté registrado como administrador para IBM Spectrum Protect. Un único administrador puede gestionar IBM Spectrum Protect, o varias personas pueden compartir las responsabilidades administrativas.

Debe estar familiarizado con el sistema operativo en el que reside el servidor y con los protocolos de comunicación necesarios para el entorno del cliente o el servidor. También debe comprender las prácticas de gestión del almacenamiento de su organización, como el modo en el que se realizan copias de seguridad de los archivos de estación de trabajo y cómo se usan los dispositivos de almacenamiento.

Publicaciones

La familia de productos de IBM Spectrum Protect incluye IBM Spectrum Protect Snapshot, IBM Spectrum Protect for Space Management, IBM Spectrum Protect for Databases, y otros productos de gestión de almacenamiento de IBM®.

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

Novedades de este release

Este release de IBM Spectrum Protect presenta nuevas características y actualizaciones.

Si desea una lista de nuevas características y actualizaciones, consulte Novedades.

Parte 1. Planificación de una solución de protección de datos de disco de sitio único

Planifique una implementación de protección de datos que incluya un servidor en un único sitio que utilice la deduplicación de datos.

Opciones de implementación

Puede configurar el servidor para una solución de disco de sitio único de las siguientes maneras:

Configure el servidor utilizando el Centro de operaciones y los mandatos de administración

En esta documentación se incluyen los pasos necesarios para configurar un rango de sistemas de almacenamiento y el software de servidor de la solución. Las tareas de configuración se realizan mediante asistentes y opciones del Centro de operaciones y mandatos de IBM Spectrum Protect. Para obtener información sobre cómo empezar, consulte "Hoja de ruta de planificación".

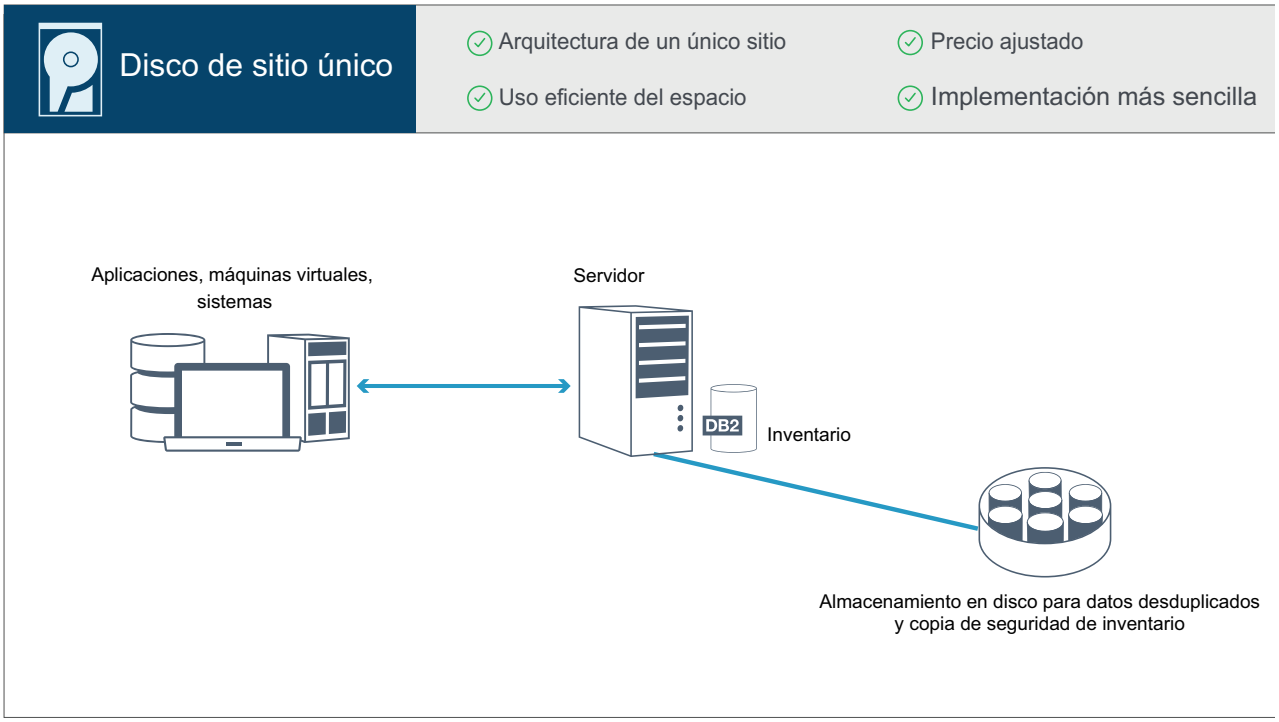
Configure el servidor utilizando scripts automatizados

Para obtener información detallada sobre cómo implementar una solución de disco de sitio único con sistemas de almacenamiento de IBM Storwize específicos y utilizando scripts automatizados para configurar el servidor, consulte los blueprints de IBM Spectrum Protect. La documentación y los scripts están disponibles en IBM developerWorks en: IBM Spectrum Protect Blueprints.

La documentación blueprint no incluye pasos para la instalación y configuración de Centro de operaciones, o el establecimiento de comunicaciones seguras utilizando la capa de seguridad de transporte (TLS). Se incluye una opción para utilizar Elastic Storage Server, que se basa en la tecnología IBM Spectrum Scale.

Hoja de ruta de planificación

Planifique una solución de disco en un único sitio revisando el diseño de arquitectura en la siguiente figura y, a continuación, completando las tareas de la hoja de ruta que siguen al diagrama.



Los pasos siguientes son necesarios para planificar un entorno de disco de sitio único.

1. Seleccionar el tamaño de sistema.
2. Cumplir los requisitos de sistema para hardware y software.
3. Registrar valores para la configuración de sistema en las hojas de trabajo de planificación.
4. Planificar el almacenamiento.
5. Planificar la seguridad.
   a. Planificar los roles de administrador.
   b. Planificar las comunicaciones seguras.
   c. Planificar el almacenamiento de datos cifrados.
   d. Planificar el acceso de cortafuegos.

Capítulo 1. Selección de un tamaño del sistema

Seleccione el tamaño del servidor de IBM Spectrum Protect basándose en la cantidad de datos que gestiona y los sistemas que se deben proteger.

Acerca de esta tarea

Puede utilizar la información de la tabla para determinar el tamaño del servidor que se necesita, en función de la cantidad de datos que gestione.

La tabla siguiente describe el volumen de datos que gestiona un servidor. Esta cantidad incluye todas las versiones. La cantidad diaria de datos es la cantidad de datos nuevos a la que hace copia de seguridad cada día. Los datos gestionados totales y la cantidad diaria de datos nuevos se miden como el tamaño antes de la reducción de datos.

Tabla 1. Determinación del tamaño del servidor

Total de datos gestionados	**Cantidad diaria de datos nuevos de los que se debe hacer copia de seguridad**	**Tamaño de servidor necesario**
45 TB - 180 TB	Hasta 6 TB al día	Pequeño
200 TB - 800 TB	6 - 20 TB al día	Mediano
1000 TB - 4000 TB	20 - 100 TB al día	Grande

Los valores de copia de seguridad diaria de la tabla se basan en los resultados de prueba con objetos de 128 MB de tamaño, utilizados por IBM Spectrum Protect for Virtual Environments. Es posible que las cargas de trabajo que constan de objetos que tienen menos de 128 KB no puedan conseguir estos límites diarios.

Capítulo 2. Requisitos del sistema para una solución de disco de sitio único

Después de seleccionar la solución IBM Spectrum Protect que mejor se ajuste a los requisitos de protección de datos, revise los requisitos de sistema para planificar la implementación de la solución de protección de datos.

Asegúrese de que el sistema cumple los requisitos previos de hardware y software para el tamaño de servidor que desea utilizar.

Información relacionada:

Sistemas operativos admitidos para IBM Spectrum Protect

Requisitos de hardware

Los requisitos de hardware para la solución IBM Spectrum Protect se basan en el tamaño del sistema. Elija componentes equivalentes o mejores que los listados para garantizar un rendimiento óptimo para el entorno.

Para obtener una definición de los tamaños de sistema, consulte Capítulo 1, “Selección de un tamaño del sistema”, en la página 3.

La tabla siguiente incluye requisitos de hardware mínimos para el servidor y el almacenamiento, en función del tamaño del servidor que planea crear. Si utiliza particiones locales (LPAR) o particiones de trabajo (WPAR), ajuste los requisitos de red para tener en cuenta los tamaños de las particiones.

Componente de hardware	Sistema pequeño	Sistema mediano	Sistema grande
Procesador de servidor	AIX 6 núcleos de procesador, 3,42 GHz o más rápido Linux Windows 12 núcleos de procesador, 1,9 GHz o más rápido	AIX 8 núcleos de procesador, 3,42 GHz o más rápido Linux Windows 16 núcleos de procesador, 2,0 GHz o más rápido	AIX 20 núcleos de procesador, 3,42 GHz Linux Windows 32 núcleos de procesador, 2,0 GHz o más rápido
Memoria de servidor	64 GB RAM	128 GB RAM	192 GB RAM
Red	• Ethernet de 10 GB (1 puerto) • Adaptador de canal de fibra de 8 GB (2 puertos)	• Ethernet de 10 GB (2 puertos) • Adaptador de canal de fibra de 8 GB (2 puertos)	• Ethernet de 10 GB (4 puertos) • Adaptador de canal de fibra de 8 GB (4 puertos)
Almacenamiento	• 1.3 TB de inventario, más espacio para registros de Centro de operaciones. • Agrupación de almacenamiento de contenedores de directorio deduplicada de 46 TB	• 2 TB de inventario, más espacio para registros de Centro de operaciones • Agrupación de almacenamiento de contenedores de directorio deduplicada de 200 TB	• 4 TB de inventario, más espacio para registros de Centro de operaciones • Agrupación de almacenamiento de contenedores de directorio deduplicada de 1000 TB

Estimación de requisitos de espacio de base de datos para Centro de operaciones

Los requisitos de hardware para Centro de operaciones se incluyen en la tabla anterior, excepto para la base de datos y el espacio de registro de archivado (inventario) que utiliza Centro de operaciones para contener registros para clientes gestionados.

Si no piensa instalar el Centro de operaciones en el mismo sistema que servidor, puede calcular requisitos de sistema por separado. Para calcular requisitos del sistema para Centro de operaciones, consulte la calculadora de requisitos del sistema en la nota técnica 1641684.

La gestión del Centro de operaciones en el servidor es una carga de trabajo que necesita espacio adicional para las operaciones de base de datos. La cantidad de espacio depende del número de clientes supervisados en un servidor. Revise las directrices siguientes para estimar cuánto espacio requiere el servidor.

Espacio de base de datos

El Centro de operaciones utiliza aproximadamente 1,2 GB de espacio de base de datos por cada 1000 clientes supervisados en un servidor. Por ejemplo, considere un servidor hub con 2000 clientes que gestione también tres servidores spoke, cada uno de ellos con 1500 clientes. Esta configuración tiene un total de 6500 clientes en los cuatro servidores y necesita aproximadamente 8,4 GB de espacio de base de datos. Este valor se calcula redondeando los 6500 clientes al 1000 más próximo, que es 7000:

```
7 x 1.2 GB=8.4 GB
```

Espacio de registro de archivado

El Centro de operaciones utiliza aproximadamente 8 GB de espacio de registro de archivado cada 24 horas por cada 1000 clientes. En el ejemplo de 6500 clientes en el servidor hub y los servidores spoke, se utilizan 56 GB de espacio de registro de archivado a lo largo de un período de 24 horas para el servidor hub.

Para cada servidor de radio en el ejemplo, el espacio del registro de archivado que se utiliza a lo largo de 24 horas es aproximadamente 16 GB. Estas estimaciones se basan en el intervalo de recopilación de estados predeterminado de 5 minutos. Si reduce el intervalo de recopilación de uno cada 5 minutos a uno cada 3 minutos, aumentan los requisitos de espacio. Los siguientes ejemplos muestran el aumento aproximado en el requisito de espacio de registro con un intervalo de recopilación de una vez cada 3 minutos:

- Servidor hub: de 56 GB a 94 GB aproximadamente
- Cada servidor spoke: de 16 GB a 28 GB aproximadamente

Aumente el espacio de registro de archivado para tener espacio suficiente para proporcionar soporte a Centro de operaciones, sin que afecte a las operaciones de servidor existentes.

Requisitos de software

La documentación para la solución IBM Spectrum Protect de disco en un único sitio incluye tareas de instalación y configuración para los siguientes sistemas operativos. Debe cumplir los requisitos de software mínimos que se indican.

Sistemas operativos y versiones: Las tablas siguientes muestran los sistemas operativos que se eligen como base para las instrucciones de implementación para la solución. Puede implementar la solución con cualquiera de los sistemas operativos y versiones que se admiten. Sin embargo, si utiliza un sistema operativo distinto, algunos de los pasos de implementación pueden diferir, o es posible que no se apliquen para distintas versiones del sistema operativo. Para obtener detalles respecto a otros sistemas operativos y versiones que se admiten para el servidor, consulte Sistemas operativos admitidos para IBM Spectrum Protect.

Sistemas AIX

Tipo de software	Requisitos mínimos de software
Sistema operativo	IBM AIX 7.1
Programa de utilidad gunzip	El programa de utilidad gunzip debe estar disponible en el sistema antes de instalar o actualizar el servidor de IBM Spectrum Protect . Asegúrese de que el programa de utilidad gunzip esté instalado y que la vía de acceso al mismo esté establecida en la variable de entorno PATH.
Tipo de sistema de archivos	Sistemas de archivos JFS2 Los sistemas AIX pueden almacenar en caché una gran cantidad de datos de sistema de archivos, lo que puede reducir la memoria que es necesaria para el servidor y los procesos de DB2. Para evitar la paginación con el servidor de AIX, utilice la opción de montaje `rbrw mount` para el sistema de archivos JFS2. Se utiliza menos memoria para la memoria caché de sistema de archivo y hay más disponible para IBM Spectrum Protect. No utilice las opciones de montaje del sistema de archivos, E/S simultáneas (CIO) y E/S directas (DIO), para sistemas de archivos que contengan la base de datos de IBM Spectrum Protect, registros o volúmenes de agrupaciones de almacenamiento. Estas opciones pueden producir la degradación del rendimiento de muchas operaciones de servidor. IBM Spectrum Protect y DB2 aún pueden utilizar DIO donde sea beneficioso hacerlo, pero IBM Spectrum Protect no necesita las opciones de montaje para aprovechar estas técnicas de forma selectiva.
Otro software	Shell Korn (ksh)

Sistemas Linux

Tipo de software	Requisitos mínimos de software
Sistema operativo	Red Hat Enterprise Linux 7 (x86_64)

Tipo de software	Requisitos mínimos de software
Bibliotecas	Bibliotecas de GNU C, versión 2.3.3-98.38 o posterior que está instalado en el sistema de IBM Spectrum Protect. Red Hat Enterprise Linux Servers: • **libaio** • **libstdc++.so.6** (se necesitan paquetes de 32 bits y 64 bits) • **numactl.x86_64**
Tipo de sistema de archivos	Formato de sistemas de archivos relacionados con bases de datos con ext3 o ext4. Para los sistemas de archivos relacionados con agrupaciones de almacenamiento, utilice XFS.
Otro software	Shell Korn (ksh)

Sistemas Windows

Tipo de software	Requisitos mínimos de software
Sistema operativo	Microsoft Windows 2012 R2 (64 bits)
Tipo de sistema de archivos	NTFS
Otro software	Windows 2012 R2 con .NET Framework 4.5 está instalado y habilitado. Se deben desactivar las siguientes políticas de Control de la cuenta de usuario: • Control de la cuenta de usuario: modo de aprobación de administrador para la cuenta de administrador integrada • Control de la cuenta de usuario: ejecute todos los administradores en el modo de aprobación de administrador

Tareas relacionadas:

Establecimiento de las opciones de red de AIX

Capítulo 3. Planificación de hojas de trabajo

Utilice las hojas de trabajo de planificación para registrar los valores que se utilizan para configurar el sistema y configurar el servidor de IBM Spectrum Protect. Utilice los valores predeterminados de prácticas recomendadas que aparecen en las hojas de trabajo.

Cada hoja de trabajo le ayuda a prepararse para diferentes partes de la configuración del sistema utilizando valores de las prácticas recomendadas:

Configuración previa de sistema servidor
Utilice las hojas de trabajo de configuración previa para planificar los sistemas de archivos y directorios que se crean al configurar sistemas de archivos para IBM Spectrum Protect durante la configuración del sistema. Todos los directorios que crea para el servidor deben estar vacíos.

Configuración del servidor
Utilice las hojas de trabajo de configuración cuando configure el servidor. Los valores predeterminados se recomiendan para la mayoría de los elementos, excepto donde se indica.

AIX

Tabla 2. Hoja de trabajo para configuración previa de un sistema servidor AIX

Elemento	Valor predeterminado	Valor	Tamaño mínimo de directorio	Notas
Dirección de puerto TCP/IP para comunicaciones con el servidor	1500		No aplicable	Asegúrese de que este puerto está disponible cuando instala y configura el sistema operativo El número de puerto puede ser un número dentro del rango 1024 - 32767.
Directorio para la instancia de servidor	`/home/tsminst1/tsminst1`		50 GB	Si cambia el valor para el directorio de instancia de servidor respecto al valor predeterminado, modifique también el valor de propietario de instancia de DB2 en Tabla 3 en la página 12.
Directorio para la instalación del servidor	`/`		Espacio disponible que es necesario para el directorio: 5 GB	
Directorio para la instalación del servidor	`/usr`		Espacio disponible que es necesario para el directorio: 5 GB	

Tabla 2. Hoja de trabajo para configuración previa de un sistema servidor AIX (continuación)

Elemento	Valor predeterminado	Valor	Tamaño mínimo de directorio	Notas
Directorio para la instalación del servidor	`/var`		Espacio disponible que es necesario para el directorio: 5 GB	
Directorio para la instalación del servidor	`/tmp`		Espacio disponible que es necesario para el directorio: 5 GB	
Directorio para la instalación del servidor	`/opt`		Espacio disponible que es necesario para el directorio: 10 GB	
Directorio para el registro activo	`/tsminst1/TSMalog`		• Pequeños y mediano: 140 GB • Grande: 300 GB	Cuando crea el registro activo durante la configuración inicial del servidor, establezca el tamaño en 128 GB.
Directorio para el registro de archivado	`/tsminst1/TSMarchlog`		• Pequeño: 1 TB • Mediano: 3 TB • Grande: 4 TB	

Directorios para la base de datos	`/tsminst1/TSMdbspace00`
	`/tsminst1/TSMdbspace01`
	`/tsminst1/TSMdbspace02`
	`/tsminst1/TSMdbspace03`
	...
			Espacio total mínimo para todos los directorios:
			• Pequeño: Al menos 1 TB
			• Mediano: Al menos 2 TB
			• Grande: 4 TB
				Cree un número mínimo de sistemas de archivos para la base de datos, dependiendo del tamaño del sistema:
				• Pequeño: Al menos 4 sistemas de archivos
				• Mediano: Al menos 4 sistemas de archivos
				• Grande: Al menos 8 sistemas de archivos

Tabla 2. Hoja de trabajo para configuración previa de un sistema servidor AIX (continuación)

Elemento	Valor predeterminado	Valor	Tamaño mínimo de directorio	Notas
Directorios para almacenamiento	/tsminst1/TSMfile00 /tsminst1/TSMfile01 /tsminst1/TSMfile02 /tsminst1/TSMfile03 ...		Espacio total mínimo para todos los directorios: • Pequeño: Al menos 38 TB • Mediano: Al menos 180 TB • Grande: Al menos 980 TB	Cree un número mínimo de sistemas de archivos para almacenamiento, dependiendo del tamaño del sistema: • Pequeño: Al menos 10 sistemas de archivos • Mediano: Al menos 20 sistemas de archivos • Grande: Al menos 40 sistemas de archivos
Directorios para la copia de seguridad de base de datos	/tsminst1/TSMbkup00 /tsminst1/TSMbkup01 /tsminst1/TSMbkup02 /tsminst1/TSMbkup03		Espacio total mínimo para todos los directorios: • Pequeño: Al menos 3 TB • Mediano: Al menos 10 TB • Grande: Al menos 16 TB	Cree un número mínimo de sistemas de archivos para hacer copia de seguridad de la base de datos, dependiendo del tamaño del sistema: • Pequeño: Al menos 2 sistemas de archivos • Mediano: Al menos 4 sistemas de archivos • Grande: Al menos 4 sistemas de archivos **Nota:** El primer directorio de la copia de seguridad de la base de datos también se utiliza para el directorio de migración tras error del registro de archivado.

Tabla 3. Hoja de trabajo para la configuración de IBM Spectrum Protect

Elemento	Valor predeterminado	Valor	Notas
Propietario de instancia de DB2	`tsminst1`		Si ha cambiado el valor para el directorio de instancia de servidor en Tabla 2 en la página 9 respecto al valor predeterminado, modifique también el valor para el propietario de instancia de DB2.
Contraseña de propietario de instancia de DB2	`passw0rd`		Seleccione un valor diferente al predeterminado para la contraseña de propietario de instancia. Asegúrese de que registra este valor en una ubicación segura.
Grupo primario para el propietario de instancia de DB2	`tsmsrvrs`		
Nombre del servidor	El valor predeterminado para el nombre del servidor es el nombre de host del sistema.		
Contraseña del servidor	`passw0rd`		Seleccione un valor diferente al predeterminado para la contraseña de servidor. Asegúrese de que registra este valor en una ubicación segura.
ID de administrador: ID de usuario para la instancia de servidor	`admin`		
Contraseña de ID de administrador	`passw0rd`		Seleccione un valor diferente al predeterminado para la contraseña de administrador. Asegúrese de que registra este valor en una ubicación segura.

Tabla 3. Hoja de trabajo para la configuración de IBM Spectrum Protect (continuación)

Elemento	Valor predeterminado	Valor	Notas
Hora de inicio de la planificación	22:00		La hora de inicio de la planificación predeterminada empieza en la fase de cargar de trabajo de cliente, que es predominantemente la fase de actividades de archivado y copia de seguridad del cliente. Durante la fase de carga de trabajo del cliente, los recursos del servidor admiten las operaciones del cliente. Normalmente, estas operaciones se completan durante la ventana de planificación nocturna. Las planificaciones de las operaciones de mantenimiento de servidor se definen para empezar 10 horas después del inicio de la ventana de copia de seguridad de cliente.

Linux

Tabla 4. Hoja de trabajo para la configuración previa de un sistema servidor Linux

Elemento	Valor predeterminado	Valor	Tamaño mínimo de directorio	Notas
Dirección de puerto TCP/IP para comunicaciones con el servidor	1500		No aplicable	Asegúrese de que este puerto está disponible cuando instala y configura el sistema operativo El número de puerto puede ser un número dentro del rango 1024 - 32767.
Directorio para la instancia de servidor	/home/tsminst1/tsminst1		25 GB	Si cambia el valor para el directorio de instancia de servidor respecto al valor predeterminado, modifique también el valor de propietario de instancia de DB2 en Tabla 5 en la página 15.
Directorio para el registro activo	/tsminst1/TSMalog		• Pequeños y mediano: 140 GB • Grande: 300 GB	

Tabla 4. Hoja de trabajo para la configuración previa de un sistema servidor Linux (continuación)

Elemento	Valor predeterminado	Valor	Tamaño mínimo de directorio	Notas
Directorio para el registro de archivado	`/tsminst1/TSMarchlog`		• Pequeño: 1 TB • Mediano: 3 TB • Grande: 4 TB	

Directorios para la base de datos	`/tsminst1/TSMdbspace00`
	`/tsminst1/TSMdbspace01`
	`/tsminst1/TSMdbspace02`
	`/tsminst1/TSMdbspace03`
	...
			Espacio total mínimo para todos los directorios:
			• Pequeño: Al menos 1 TB
			• Mediano: Al menos 2 TB
			• Grande: 4 TB
				Cree un número mínimo de sistemas de archivos para la base de datos, dependiendo del tamaño del sistema:
				• Pequeño: Al menos 4 sistemas de archivos
				• Mediano: Al menos 4 sistemas de archivos
				• Grande: Al menos 8 sistemas de archivos

Directorios para almacenamiento	`/tsminst1/TSMfile00`
	`/tsminst1/TSMfile01`
	`/tsminst1/TSMfile02`
	`/tsminst1/TSMfile03`
	...
			Espacio total mínimo para todos los directorios:
			• Pequeño: Al menos 38 TB
			• Mediano: Al menos 180 TB
			• Grande: Al menos 980 TB
				Cree un número mínimo de sistemas de archivos para almacenamiento, dependiendo del tamaño del sistema:
				• Pequeño: Al menos 10 sistemas de archivos
				• Mediano: Al menos 20 sistemas de archivos
				• Grande: Al menos 40 sistemas de archivos

Tabla 4. Hoja de trabajo para la configuración previa de un sistema servidor Linux (continuación)

Elemento	Valor predeterminado	Valor	Tamaño mínimo de directorio	Notas

Directorios para la copia de seguridad de base de datos	`/tsminst1/TSMbkup00`
	`/tsminst1/TSMbkup01`
	`/tsminst1/TSMbkup02`
	`/tsminst1/TSMbkup03`
			Espacio total mínimo para todos los directorios:
			• Pequeño: Al menos 3 TB
			• Mediano: Al menos 10 TB
			• Grande: Al menos 16 TB
				Cree un número mínimo de sistemas de archivos para hacer copia de seguridad de la base de datos, dependiendo del tamaño del sistema:
				• Pequeño: Al menos 2 sistemas de archivos
				• Mediano: Al menos 4 sistemas de archivos
				• Grande: Al menos 4 sistemas de archivos
				Nota: El primer directorio de la copia de seguridad de la base de datos también se utiliza para el directorio de migración tras error del registro de archivado.

Tabla 5. Hoja de trabajo para la configuración de IBM Spectrum Protect

Elemento	Valor predeterminado	Valor	Notas
Propietario de instancia de DB2	`tsminst1`		Si ha cambiado el valor para el directorio de instancia de servidor en Tabla 4 en la página 13 respecto al valor predeterminado, modifique también el valor para el propietario de instancia de DB2.
Contraseña de propietario de instancia de DB2	`passw0rd`		Seleccione un valor diferente al predeterminado para la contraseña de propietario de instancia. Asegúrese de que registra este valor en una ubicación segura.
Grupo primario para el propietario de instancia de DB2	`tsmsrvrs`		
Nombre del servidor	El valor predeterminado para el nombre del servidor es el nombre de host del sistema.		

Tabla 5. Hoja de trabajo para la configuración de IBM Spectrum Protect (continuación)

Elemento	Valor predeterminado	Valor	Notas
Contraseña del servidor	`passw0rd`		Seleccione un valor diferente al predeterminado para la contraseña de servidor. Asegúrese de que registra este valor en una ubicación segura.
ID de administrador: ID de usuario para la instancia de servidor	`admin`		
Contraseña de ID de administrador	`passw0rd`		Seleccione un valor diferente al predeterminado para la contraseña de administrador. Asegúrese de que registra este valor en una ubicación segura.
Hora de inicio de la planificación	`22:00`		La hora de inicio de la planificación predeterminada empieza en la fase de cargar de trabajo de cliente, que es predominantemente la fase de actividades de archivado y copia de seguridad del cliente. Durante la fase de carga de trabajo del cliente, los recursos del servidor admiten las operaciones del cliente. Normalmente, estas operaciones se completan durante la ventana de planificación nocturna. Las planificaciones de las operaciones de mantenimiento de servidor se definen para empezar 10 horas después del inicio de la ventana de copia de seguridad de cliente.

Windows

Dado que muchos volúmenes se crean para el servidor, configure el servidor utilizando la característica de Windows de correlación de volúmenes de disco con directorios en lugar de letras de unidad.

Por ejemplo, `C:\tsminst1\TSMdbpsace00` es el punto de montaje para un volumen con su propio espacio. El volumen se correlaciona con un directorio bajo la unidad C:, pero no ocupa espacio de la unidad C:. La excepción es el directorio de instancia de servidor, `C:\tsminst1`, que puede ser un punto de montaje o un directorio normal.

Tabla 6. Hoja de trabajo para la configuración previa de un sistema servidor Windows

Elemento	Valor predeterminado	Valor	Tamaño mínimo de directorio	Notas
Dirección de puerto TCP/IP para comunicaciones con el servidor	1500		No aplicable	Asegúrese de que este puerto está disponible cuando instala y configura el sistema operativo El número de puerto puede ser un número dentro del rango 1024 - 32767.
Directorio para la instancia de servidor	`C:\tsminst1`		25 GB	Si cambia el valor para el directorio de instancia de servidor respecto al valor predeterminado, modifique también el valor de propietario de instancia de DB2 en Tabla 7 en la página 19.
Directorio para el registro activo	`C:\tsminst1\TSMalog`		• Pequeños y mediano: 140 GB • Grande: 300 GB	
Directorio para el registro de archivado	`C:\tsminst1\TSMarchlog`		• Pequeño: 1 TB • Mediano: 3 TB • Grande: 4 TB	

Directorios para la base de datos	`C:\tsminst1\TSMdbspace00`
	`C:\tsminst1\TSMdbspace01`
	`C:\tsminst1\TSMdbspace02`
	`C:\tsminst1\TSMdbspace03`
	...
			Espacio total mínimo para todos los directorios:
			• Pequeño: Al menos 1 TB
			• Mediano: Al menos 2 TB
			• Grande: 4 TB
				Cree un número mínimo de sistemas de archivos para la base de datos, dependiendo del tamaño del sistema:
				• Pequeño: Al menos 4 sistemas de archivos
				• Mediano: Al menos 4 sistemas de archivos
				• Grande: Al menos 8 sistemas de archivos

Tabla 6. Hoja de trabajo para la configuración previa de un sistema servidor Windows (continuación)

Elemento	Valor predeterminado	Valor	Tamaño mínimo de directorio	Notas

Directorios para almacenamiento	`C:\tsminst1\TSMfile00`
	`C:\tsminst1\TSMfile01`
	`C:\tsminst1\TSMfile02`
	`C:\tsminst1\TSMfile03`
	...
			Espacio total mínimo para todos los directorios:
			• Pequeño: Al menos 38 TB
			• Mediano: Al menos 180 TB
			• Grande: Al menos 980 TB
				Cree un número mínimo de sistemas de archivos para almacenamiento, dependiendo del tamaño del sistema:
				• Pequeño: Al menos 10 sistemas de archivos
				• Mediano: Al menos 20 sistemas de archivos
				• Grande: Al menos 40 sistemas de archivos

Directorios para la copia de seguridad de base de datos	`C:\tsminst1\TSMbkup00`
	`C:\tsminst1\TSMbkup01`
	`C:\tsminst1\TSMbkup02`
	`C:\tsminst1\TSMbkup03`
			Espacio total mínimo para todos los directorios:
			• Pequeño: Al menos 3 TB
			• Mediano: Al menos 10 TB
			• Grande: Al menos 16 TB
				Cree un número mínimo de sistemas de archivos para hacer copia de seguridad de la base de datos, dependiendo del tamaño del sistema:
				• Pequeño: Al menos 2 sistemas de archivos
				• Mediano: Al menos 4 sistemas de archivos
				• Grande: Al menos 4 sistemas de archivos
				Nota: El primer directorio de la copia de seguridad de la base de datos también se utiliza para el directorio de migración tras error del registro de archivado.

Tabla 7. Hoja de trabajo para la configuración de IBM Spectrum Protect

Elemento	Valor predeterminado	Valor	Notas
Propietario de instancia de DB2	`tsminst1`		Si ha cambiado el valor para el directorio de instancia de servidor en Tabla 6 en la página 17 respecto al valor predeterminado, modifique también el valor para el propietario de instancia de DB2.
Contraseña de propietario de instancia de DB2	`pAssW0rd`		Seleccione un valor diferente al predeterminado para la contraseña de propietario de instancia. Asegúrese de que registra este valor en una ubicación segura.
Nombre del servidor	El valor predeterminado para el nombre del servidor es el nombre de host del sistema.		
Contraseña del servidor	`passw0rd`		Seleccione un valor diferente al predeterminado para la contraseña de servidor. Asegúrese de que registra este valor en una ubicación segura.
ID de administrador: ID de usuario para la instancia de servidor	`admin`		
Contraseña de ID de administrador	`passw0rd`		Seleccione un valor diferente al predeterminado para la contraseña de administrador. Asegúrese de que registra este valor en una ubicación segura.

Tabla 7. Hoja de trabajo para la configuración de IBM Spectrum Protect (continuación)

Elemento	Valor predeterminado	Valor	Notas
Hora de inicio de la planificación	22:00		La hora de inicio de la planificación predeterminada empieza en la fase de cargar de trabajo de cliente, que es predominantemente la fase de actividades de archivado y copia de seguridad del cliente. Durante la fase de carga de trabajo del cliente, los recursos del servidor admiten las operaciones del cliente. Normalmente, estas operaciones se completan durante la ventana de planificación nocturna. Las planificaciones de las operaciones de mantenimiento de servidor se definen para empezar 10 horas después del inicio de la ventana de copia de seguridad de cliente.

Capítulo 4. Planificación de almacenamiento

Elegir la tecnología de almacenamiento más efectiva para componentes de IBM Spectrum Protect para asegurarse de que el rendimiento de servidor y las operaciones son eficientes.

Los dispositivos de hardware de almacenamiento tiene características de rendimiento y capacidad diferentes, lo que determina cómo se pueden utilizar de forma eficaz con IBM Spectrum Protect. Para obtener una orientación general sobre cómo seleccionar el hardware de almacenamiento apropiado y configurar la solución, revise las directrices siguientes.

Base de datos y registro activo

- Utilice un disco rápido para el registro activo y la base de datos de IBM Spectrum Protect, por ejemplo con las siguientes características:
  - Disco de alto rendimiento de 15k rpm con interfaz de canal de fibra o SCSI con conexión en serie (SAS)
  - Disco de estado sólido (SSD)
- Aísle el registro activo de la base de datos a menos que utilice el hardware de flash o SSD
- Al crear matrices para la base de datos, utilice RAID nivel 5

Agrupación de almacenamiento

- Puede utilizar discos menos caros y más lentos para la agrupación de almacenamiento
- La agrupación de almacenamiento puede compartir discos para el registro de archivado y el almacenamiento de copias de seguridad de base de datos.
- Utilice el nivel RAID 6 para las matrices de agrupación de almacenamiento para añadir protección frente a las anomalías de unidad doble cuando se utilizan tipos de disco de gran tamaño

Referencia relacionada:

Requisitos del sistema de almacenamiento y reducción del riesgo de corrupción de datos

Planificación de matrices de almacenamiento

Prepararse para la configuración de almacenamiento de disco planificando matrices RAID y volúmenes, de acuerdo con el tamaño del sistema IBM Spectrum Protect.

Diseñe matrices de almacenamiento con características de tamaño y rendimiento que son adecuadas para uno de los componentes de almacenamiento de servidor de IBM Spectrum Protect, como por ejemplo la base de datos de servidor o una agrupación de almacenamiento. La actividad de planificación del almacenamiento debe tener en cuenta el tipo de unidad, el nivel de RAID, el número de unidades, el número de unidades de repuesto, etc. En las configuraciones de la solución, los grupos de almacenamiento contienen matrices RAID de almacenamiento interno y constan de varios discos físicos que están presentes como volúmenes lógicos para el sistema. Cuando configure el sistema de discos, cree grupos de almacenamiento, o agrupaciones de almacenamiento de datos y, a continuación, cree matrices de almacenamiento en los grupos.

Cree volúmenes, o LUN, en los grupos de almacenamiento. El grupo de almacenamiento define qué discos proporcionan el almacenamiento que compone el volumen. Cuando cree volúmenes, asígnelos completamente. Se utilizan tipos de disco más rápidos para mantener los volúmenes de base de datos y los volúmenes de registro activos. Se pueden utilizar tipos de disco más lentos para los volúmenes de agrupación de almacenamiento, el registro de archivado y los volúmenes de copia de seguridad de base de datos.

Tabla 8 y Tabla 9 describen los requisitos de diseño para la configuración de grupos de almacenamiento y volúmenes.

Tabla 8. Configuración de los componentes de un grupo de almacenamiento

Componente	**Detalles**
Requisito de almacenamiento del servidor	Manera en que el servidor utiliza el almacenamiento.
Tipo de disco	Tamaño y velocidad para el tipo de disco que se utiliza para el requisito de almacenamiento.
Cantidad de discos	Número de cada tipo de disco necesario para el requisito de almacenamiento.
Capacidad de repuesto en caliente	Número de discos reservados como repuestos para una sustitución si se produce un error de disco.
Nivel de RAID	Nivel de matriz RAID que se utiliza para el almacenamiento lógico. El nivel RAID define el tipo de redundancia proporcionado por la matriz, por ejemplo 5 o 6.
Cantidad de matriz RAID	Número de matrices RAID para crear.
DDM por matriz RAID	Número de módulos de unidad de disco (DDM) que se utilizarán en cada una de las matrices RAID.
Tamaño útil por matriz RAID	Tamaño disponible para el almacenamiento de datos en cada matriz RAID después de contabilizar el espacio que se pierde para la redundancia.
Tamaño total útil	Tamaño total disponible para el almacenamiento de datos en las matrices RAID: [Cantidad x tamaño útil].
Nombres de matriz y de grupo de almacenamiento recomendados	Nombre preferido a utilizar para los MDisks y los grupos de MDisk.
Utilización	Componente de servidor que utiliza parte del disco físico.

Tabla 9. Componentes de la configuración de volumen

Componente	**Detalles**
Requisito de almacenamiento del servidor	Requisito para el que se usa el disco físico.
Nombre de volumen	Nombre exclusivo que se da a un volumen específico.
Grupo de almacenamiento	Nombre del grupo de almacenamiento desde el que se obtiene espacio para crear el volumen.
Tamaño	Tamaño de cada volumen.
Punto de montaje de servidor deseado	Directorio del sistema servidor donde está montado el volumen.

Tabla 9. Componentes de la configuración de volumen (continuación)

Componente	Detalles
Cantidad	Número de volúmenes a crear para un requisito específico. Utilice la misma denominación estándar para cada volumen que se crea para el mismo requisito.
Utilización	Componente de servidor que utiliza parte del disco físico.

Ejemplos

Hay ejemplos de configuración para grupos de almacenamiento y volúmenes disponibles en el enlace siguiente: Ejemplos de hojas de trabajo para planificar matrices de almacenamiento. Los ejemplos muestran cómo planificar el almacenamiento para distintos tamaños de servidor. En las configuraciones de ejemplo, hay una correlación uno a uno entre discos y grupos de almacenamiento. Puede descargar los ejemplos y editar las hojas de trabajo para planificar la configuración de almacenamiento de su servidor.

Capítulo 5. Planificación de la seguridad

Planee proteger la seguridad de los sistemas en la solución IBM Spectrum Protect con controles de acceso y autenticación y tenga en cuenta el cifrado de datos y la transmisión de contraseña.

Planificación de los roles de administración

Defina los niveles de autorización que desea asignar a los administradores que tienen acceso a la solución IBM Spectrum Protect.

Puede asignar uno de los siguientes niveles de autorización a los administradores:

Sistema
Los administradores que tienen autoridad del sistema tienen el nivel de autorización más alto. Los administradores con este nivel pueden realizar cualquier tarea. Pueden gestionar todos los dominios de política y agrupaciones de almacenamiento y otorgar autoridad a otros administradores.

Política
Los administradores que tienen autorización sobre políticas pueden gestionar todas las tareas relacionadas con la gestión de políticas. Este privilegio puede no tener restricciones o puede estar restringido a dominios de políticas específicos.

Almacenamiento
Los administradores que tienen autorización de almacenamiento pueden asignar y controlar recursos de almacenamiento para el servidor.

Operador
Los administradores que tienen autorización de Operador pueden controlar la operación inmediata del servidor y la disponibilidad de soporte de almacenamiento como unidades y bibliotecas de cintas.

Los escenarios de Tabla 10 proporcionan ejemplos de por qué es posible que desee asignar distintos niveles de autorización para que los administradores puedan realizar tareas:

Tabla 10. Escenarios para roles de administrador

Escenario	Tipo de ID de administrador a configurar
Un administrador de una pequeña empresa gestiona el servidor y es responsable de todas las actividades del servidor.	• Autoridad del sistema: 1 ID de administrador
Un administrador para varios servidores también gestiona el sistema en general. Otros diversos administradores gestionan sus propias agrupaciones de almacenamiento.	• Autoridad del sistema en todos los servidores: 1 ID de administrador para el administrador del sistema general • Autoridad de almacenamiento para agrupaciones de almacenamiento designadas: 1 ID de administrador para cada uno de los otros administradores

Tabla 10. Escenarios para roles de administrador (continuación)

Escenario	Tipo de ID de administrador a configurar
Un administrador gestiona 2 servidores. Otra persona ayuda con las tareas de administración. Dos ayudantes son responsables de ayudar a garantizar que se hace copia de seguridad de los sistemas importantes. Cada ayudante es responsable de supervisar las copias de seguridad planificadas en uno de los servidores de IBM Spectrum Protect.	• Autoridad del sistema en ambos servidores: 2 ID de administrador • Autoridad de operador: 2 ID de administrador para los ayudantes con acceso al servidor del que cada persona es responsable

Planificación para comunicaciones seguras

Planifique la protección de las comunicaciones entre los componentes de la solución IBM Spectrum Protect.

Determine el nivel de protección necesario para los datos, basándose en las regulaciones y requisitos empresariales bajo los que opera la compañía.

Si su empresa necesita un alto nivel de seguridad para las contraseñas y la transmisión de datos, planee implementar comunicaciones seguras con protocolos de seguridad de la capa de transporte (TLS) o de capa de sockets seguros (SSL).

TLS y SSL proporcionan comunicaciones seguras entre el servidor y el cliente, pero pueden afectar al rendimiento del sistema. TLS, una forma de SSL, se requiere para todas las comunicaciones de contraseñas LDAP. Si opta por utilizar TLS o SSL, utilice el protocolo únicamente para las sesiones en las que sea necesario y añada recursos de procesador en el servidor para gestionar los requisitos aumentados. También puede probar con otras opciones, como los dispositivos de red, por ejemplo, direccionadores o conmutadores, que proporcionan la función TLS o SSL.

Puede utilizar TLS y SSL para proteger todas o algunas de las distintas vías de acceso de comunicación posibles, por ejemplo:

- Centro de operaciones: De navegador a concentrador; de concentrador a radio
- Cliente a servidor
- Servidor a servidor: réplica de nodo en el servidor:

Tareas relacionadas:

Protección de las comunicaciones

Planificación de almacenamiento de datos cifrados

Determine si la compañía requiere que se cifren los datos almacenados y elija la opción que mejor se adapta a sus necesidades.

Si la empresa requiere que los datos de las agrupaciones de almacenamiento estén cifrados, tiene la opción de utilizar el cifrado IBM Spectrum Protect, o un dispositivo externo como una cinta para el cifrado.

Si elige IBM Spectrum Protect para cifrar los datos, se necesitan recursos informáticos adicionales en el cliente que pueden afectar al rendimiento de los procesos de copia de seguridad y restauración.

Información relacionada:

Nota técnica 1963635

Planificación del acceso de cortafuegos

Determine los cortafuegos que se han configurado y los puertos que deben estar abiertos para que funcione la solución IBM Spectrum Protect.

Tabla 11 describe los puertos utilizados por el servidor, el cliente y el Centro de operaciones.

Tabla 11. Puertos utilizados por el servidor, el cliente y Centro de operaciones

Elemento	Valor predeterminado	Dirección	Descripción
Puerto base (**TCPPORT**)	1500	Saliente/ Entrante	Cada instancia de servidor necesita un puerto TCP exclusivo. Puede especificar un número de puerto TCP alternativo. Puede utilizar la opción **TCPADMINPORT** y la opción **ADMINONCLIENTPORT** para establecer los valores de los puertos TCP.
Puerto base SSL (**SSLTCPPORT**)	No tiene valor predeterminado	Saliente/ Entrante	Este puerto se utiliza únicamente si está habilitada la comunicación SSL. Un servidor puede soportar las comunicaciones SSL y no SSL si se especifican tanto **TCPPORT** como **SSLTCPPORT**.
SMB	45	Entrante/ Saliente	Este puerto lo utilizan los asistentes de configuración que se comunican utilizando protocolos nativos con varios hosts.
SSH	22	Entrante/ Saliente	Este puerto lo utilizan los asistentes de configuración que se comunican utilizando protocolos nativos con varios hosts.
SMTP	25	Saliente	Este puerto se utiliza para enviar alertas de correo electrónico desde el servidor.
NDMP	No tiene valor predeterminado	Entrante/ Saliente	El servidor debe poder abrir una conexión de puerto de control NDMP de salida con el dispositivo NAS. El puerto de control de salida es la dirección de nivel inferior en la definición de transportador de datos para el dispositivo NAS. Durante una restauración NDMP de archivador a servidor, el servidor debe poder abrir una conexión de datos NDMP de salida con el dispositivo NAS. El puerto de conexión de datos que se utiliza durante una restauración puede configurarse en el dispositivo NAS. Durante las copias de seguridad NDMP de archivador a servidor, el dispositivo NAS debe poder abrir conexiones de datos de salida con el servidor y el servidor debe poder aceptar las conexiones de datos NDMP de entrada. Puede utilizar la opción de servidor **NDMPPORTRANGE** para restringir el conjunto de puertos disponibles para su uso como conexiones de datos NDMP. Puede configurar un cortafuegos para conexiones a estos puertos.

Tabla 11. Puertos utilizados por el servidor, el cliente y Centro de operaciones (continuación)

Elemento	Valor predeterminado	Dirección	Descripción
Réplica	No tiene valor predeterminado	Saliente/ Entrante	El puerto y el protocolo correspondientes al puerto de salida para la réplica de datos se definen mediante el mandato **DEFINE SERVER** que se utiliza para configurar la réplica. Los puertos de entrada para la réplica son los puertos TCP y SSL que el servidor de origen indique en el mandato **DEFINE SERVER**.
Puerto de planificación del cliente	Puerto de cliente: 1501	Saliente	El cliente escucha en el puerto que se menciona y comunica el número de puerto al servidor. El servidor establece contacto con el cliente si se utiliza la planificación solicitada por servidor. Puede especificar un número de puerto alternativo en el archivo de opciones de cliente.
Sesión de ejecución larga	Valor de **KEEPALIVE**: YES	Saliente	Cuando se habilita la opción **KEEPALIVE**, los paquetes de estado activo se envían durante las sesiones cliente-servidor para impedir que el software de cortafuegos cierre las conexiones inactivas de larga ejecución.
Centro de operaciones	HTTPS: 11090	Entrante	Estos puertos se utilizan por parte del navegador web de Centro de operaciones. Puede especificar un número de puerto alternativo.
Puerto de servicio de gestión de clientes	Puerto de cliente: 9028	Entrante	El puerto de servicio de gestión de clientes debe ser accesible desde el Centro de operaciones. Asegúrese de que no hay cortafuegos que puedan impedir las conexiones. El servicio de gestión de clientes utiliza el puerto TCP del servidor para el nodo cliente para la autenticación utilizando una sesión administrativa.

Parte 2. Implementación de disco de sitio único de una solución de protección de datos

La solución de disco de sitio único se configura en un sitio y utiliza la deduplicación de datos.

Hoja de ruta de la implementación

Los pasos siguientes son necesarios para configurar el entorno de disco de sitio único de IBM Spectrum Protect.

1. Configurar el sistema.
   a. Configurar el hardware de almacenamiento y las matrices de almacenamiento para el tamaño del entorno.
   b. Instalar el sistema operativo del servidor.
   c. Configurar la E/S de multivía de acceso.
   d. Crear el ID de usuario de la instancia de servidor.
   e. Preparar sistemas de archivos para IBM Spectrum Protect.
2. Instalar el servidor y el Centro de operaciones.
3. Configurar el servidor y el Centro de operaciones.
   a. Completar la configuración inicial del servidor.
   b. Configurar opciones de servidor.
   c. Configurar la capa de sockets seguros del servidor y el cliente.
   d. Configurar el Centro de operaciones.
   e. Registrar la licencia de IBM Spectrum Protect.
   f. Configurar la eliminación de duplicados de datos.
   g. Definir las reglas de retención de datos para su empresa.
   h. Definir programas de mantenimiento del servidor.
   i. Definir programas de cliente.
4. Instalar y configurar clientes.
   a. Registrar y asignar clientes a programas.
   b. Instalar y verificar el servicio de gestión de clientes.
   c. Configurar el Centro de operaciones para utilizar el servicio de gestión de clientes.
5. Completar la implementación.

Capítulo 6. Configuración del sistema

Para configurar el sistema, primero debe configurar el hardware de almacenamiento de disco y el sistema del servidor para IBM Spectrum Protect.

Configuración del hardware de almacenamiento

Para configurar el hardware de almacenamiento, revise la las directrices generales para los sistemas de disco y IBM Spectrum Protect.

Procedimiento

1. Proporcione una conexión entre el servidor y el almacenamiento.
   - Utilice un conmutador o conexión directa para las conexiones de canal de fibra.
   - Tenga en cuenta el número de puertos que están conectados y la cantidad de ancho de banda que se necesita.
   - Tenga en cuenta el número de puertos en el servidor y el número de puertos de host en el sistema de discos que están conectados.
2. Verifique que los controladores de dispositivo y firmware para el sistema de servidor, adaptadores y sistema operativo son actuales y están en los niveles recomendados.
3. Configure matrices de almacenamiento. Asegúrese de que ha planificado correctamente para garantizar un rendimiento óptimo. Consulte el apartado Capítulo 4, “Planificación de almacenamiento”, en la página 21 para obtener más información al respecto.
4. Asegúrese de que el sistema servidor tiene acceso a los volúmenes de disco que se han creado. Realice los pasos siguientes:
   a. Si el sistema está conectado a un conmutador de canal de fibra, divida el servidor por zonas para ver los discos.
   b. Correlacione todos los volúmenes para indicar al sistema de discos que este servidor específico está autorizado para ver cada disco.

Instalación del sistema operativo del servidor

Instale el sistema operativo en el sistema de servidor y asegúrese de que se cumplan los requisitos del servidor de IBM Spectrum Protect. Ajuste los valores del sistema operativo siguiendo las instrucciones.

Instalación en sistemas AIX

Complete los pasos siguientes para instalar AIX en el sistema del servidor.

Procedimiento

1. Instale AIX Versión 7.1 TL4, SP2 o posterior de acuerdo con las instrucciones del fabricante.
2. Configure los valores de TCP/IP según las instrucciones de instalación del sistema operativo.
3. Abra el archivo `/etc/hosts` y complete las siguientes acciones:
   - Actualice el archivo para incluir la dirección IP y el nombre de host para el servidor. Por ejemplo:

```
192.0.2.7  server.yourdomain.com  server
```

- Verifique que el archivo contiene una entrada para localhost con una dirección de 127.0.0.1. Por ejemplo:

```
127.0.0.1  localhost
```

4. Habilite los puertos de terminación de E/S de AIX emitiendo el siguiente mandato:

```
chdev -l iocp0 -P
```

5. Opcional: El rendimiento de servidor puede verse afectado por la definición de huso horario de Olson. Si el rendimiento es un factor en el entorno, puede cambiar el formato de huso horario de sistema de Olson a POSIX. Realice los pasos siguientes:
   a. Utilice el siguiente formato de mandato para actualizar el valor de huso horario:

      ```
      chtz=local_timezone,date/time,date/time
      ```

      Por ejemplo, si ha vivido en Tucson, Arizona, donde se utiliza la franja horaria de las Rocosas, deberá emitir el siguiente mandato para cambiar el formato POSIX:

      ```
      chtz MST7MDT,M3.2.0/2:00:00,M11.1.0/2:00:00
      ```

   b. Añada una entrada en el `.profile` del usuario de la instancia para que se defina el entorno siguiente:

      ```
      export MALLOCOPTIONS=multiheap:16
      ```

   c. Defina el sistema para crear archivos principales de aplicación completos. Emita el mandato siguiente:

      ```
      chdev -l sys0 -a fullcore=true -P
      ```

6. Para las comunicaciones con el servidor y Centro de operaciones, asegúrese de que los siguientes puertos están abiertos en todos los cortafuegos que puedan existir:
   - Para las comunicaciones con el servidor, abra el puerto 1500
   - Para las comunicaciones seguras con Centro de operaciones, abra el puerto 11090 en el servidor hub

   Si no está utilizando los valores de puerto predeterminados, asegúrese de que los puertos que está utilizando están abiertos.

7. Habilite las mejoras de alto rendimiento de TCP. Emita el mandato siguiente:

```
no -p -o rfc1323=1
```

8. Para obtener una fiabilidad y un rendimiento óptimos, vincule cuatro puertos Ethernet de 10 Gb. A través de la SMIT, enlace los puertos juntos utilizando Etherchannel. Durante las pruebas se utilizaron los siguientes valores:

```
mode            8023ad
auto_recovery   yes             Habilitar la recuperación automática tras
                                la migración tras error.
backup_adapter  NONE            Adaptador utilizado cuando falla todo
                                el canal.
hash_mode       src_dst_port    Determina cómo se elige el adaptador
                                saliente.
interval        long            Determina el valor de intervalo para
                                IEEE.
                                Modalidad de 802.3ad
mode            8023ad          Modalidad de funcionamiento de
                                EtherChannel
netaddr         0               Dirección para el ping
noloss_failover yes             Habilitar migración tras error sin
                                pérdidas tras anomalía
                                del ping
```

```
num_retries     3             Veces que reintentar el ping antes de
                              considerarlo un error
retry_time      1             Tiempo de espera (en segundos) entre pings
use_alt_addr    no            Habilitar dirección EtherChannel
                              alternativa
use_jumbo_frame no            Habilitar tramas de gran tamaño de Gigabit
                              Ethernet
```

9. Verifique que los límites de recursos de proceso de usuario, también conocidos como *ulimits*, se han establecido de acuerdo con las directrices en Tabla 12. Si los valores ulimit no se establecen correctamente, es posible que experimente inestabilidad del servidor o un fallo en la respuesta del servidor.

Tabla 12. Valores de los límites de usuario (ulimit)

Tipo de límite de usuario	**Valor**	**Valor**	**Mandato del valor de consulta**
Tamaño máximo de archivos principales creados	`core`	Ilimitado	`ulimit -Hc`
Tamaño máximo de un segmento de datos para un proceso	`datos`	Ilimitado	`ulimit -Hd`
Tamaño de archivo máximo	`fsize`	Ilimitado	`ulimit -Hf`
Número máximo de archivos abiertos	`nofile`	65536	`ulimit -Hn`
La cantidad máxima de tiempo del procesador en segundos	`cpu`	Ilimitado	`ulimit -Ht`
Número máximo de procesos de usuario	`nproc`	16384	`ulimit -Hu`

Si necesita modificar los valores de límite de usuario, siga las instrucciones de la documentación para el sistema operativo.

Instalación en sistemas Linux

Complete los pasos siguientes para instalar Linux x86_64 en el sistema servidor.

Antes de empezar

El sistema operativo está instalado en los discos duros internos. Configure los discos duros internos utilizando una matriz de hardware de RAID 1. Por ejemplo, si está configurando un sistema pequeño, los dos discos internos de 300 GB se duplican en RAID 1 de modo que aparece disponible un único disco de 300 GB para el instalador del sistema operativo.

Procedimiento

1. Instale Red Hat Enterprise Linux Versión 7.1 o posterior, de acuerdo con las instrucciones del fabricante. Obtenga un DVD arrancable que contiene Red Hat Enterprise Linux Versión 7.1 e inicie el sistema desde el DVD. Consulte las siguientes directrices para ver las opciones de instalación. Si un elemento no se menciona en la lista siguiente, deje la selección predeterminada.
   a. Después de iniciar el DVD, elija **Instalar o actualizar un sistema existente** en el menú.

b. En la pantalla de bienvenida, seleccione **Probar este soporte e instalar Red Hat Enterprise Linux 7.1**.

c. Seleccione las preferencias de idioma y teclado.

d. Seleccione la ubicación para establecer el huso horario correcto.

e. Seleccione **Selección de software** y, a continuación, en la siguiente pantalla, seleccione **Servidor con GUI**.

f. Desde la página de resumen de la instalación, pulse **Destino de instalación** y verifique los elementos siguientes:

- El disco local de 300 GB se ha seleccionado como destino de instalación.
- En Otras opciones de almacenamiento, `Configurar particionamiento automáticamente` está seleccionada.

Pulse **Terminado**.

g. Pulse **Empezar instalación**. Una vez iniciada la instalación, establezca la contraseña raíz para la cuenta de usuario root.

Una vez que se haya completado la instalación, reinicie el sistema e inicie una sesión como el usuario root. Emita el mandato **df** para verificar el particionamiento básico. Por ejemplo, en un sistema de prueba, el particionamiento inicial ha generado el resultado siguiente:

```
[root@tvapp02]# df –h
Filesystem                    Size  Used  Avail  Use%  Mounted on
/dev/mapper/rhel-root   50G  3.0G   48G   6% /
devtmpfs                32G     0   32G   0% /dev
tmpfs                   32G   92K   32G   1% /dev/shm
tmpfs                   32G  8.8M   32G   1% /run
tmpfs                   32G     0   32G   0% /sys/fs/cgroup
/dev/mapper/rhel-home  220G   37M  220G   1% /home
/dev/sda1              497M  124M  373M  25% /boot
```

2. Configure los valores de TCP/IP según las instrucciones de instalación del sistema operativo.

   Para obtener un rendimiento y fiabilidad óptimos, considere la posibilidad de vincular varios puertos de red. Esto se puede conseguir creando la conexión de red del protocolo de control de agregación de enlaces (LACP), que agregar varios puertos subordinados a una sola conexión lógica. Las recomendaciones de configuración incluyen el uso de una modalidad de vínculo de 802.3ad, el valor de **miimon** de 100 y un valor de **xmit_hash_policy** de layer3+4.

   Si desea instrucciones adicionales sobre cómo configurar conexiones de red vinculadas con Red Hat Enterprise Linux Versión 7, consulte Crear una interfaz de acoplamiento de canal.

3. Abra el archivo `/etc/hosts` y complete las siguientes acciones:

   - Actualice el archivo para incluir la dirección IP y el nombre de host para el servidor. Por ejemplo:

     ```
     192.0.2.7  server.yourdomain.com  server
     ```

   - Verifique que el archivo contiene una entrada para localhost con una dirección de 127.0.0.1. Por ejemplo:

     ```
     127.0.0.1  localhost
     ```

4. Instale los componentes que son necesarios para la instalación de servidor. Complete los pasos siguientes para crear un repositorio Yellowdog Updater Modified (YUM) e instale los paquetes de requisitos previos.

   a. Monte el DVD de instalación de Red Hat Enterprise Linux en el directorio del sistema. Por ejemplo, para montarlo en el directorio `/mnt`, emita el siguiente mandato:

      ```
      mount -t iso9660 -o ro /dev/cdrom /mnt
      ```

b. Verifique que el DVD se ha montado emitiendo el mandato **mount**. Debería ver una salida similar al ejemplo siguiente:

```
/dev/sr0 on /mnt type iso9660
```

c. Cambie al directorio de repositorio YUM emitiendo el siguiente mandato:

```
cd /etc/yum/repos.d
```

Si el directorio `repos.d` no existe, créelo.

d. Liste el contenido de directorio:

```
ls rhel-source.repo
```

e. Cambie el nombre del archivo repo original emitiendo el mandato **mv**. Por ejemplo:

```
mv rhel-source.repo rhel-source.repo.orig
```

f. Cree un nuevo archivo repo utilizando un editor de texto. Por ejemplo, para utilizar el editor vi, emita el siguiente mandato:

```
vi rhel71_dvd.repo
```

g. Añada las líneas siguientes al nuevo archivo repo. El parámetro **baseurl** especifica el punto de montaje del directorio:

```
[rhel71_dvd]
name=DVD Redhat Enterprise Linux 7.1
baseurl=file:///mnt
enabled=1
gpgcheck=0
```

h. Instale el paquete de requisito previo `ksh.x86_64`, emitiendo el mandato **yum**. Por ejemplo:

```
yum install ksh.x86_64
```

Excepción: No necesita instalar las bibliotecas `compat-libstdc++-33-3.2.3-69.el6.i686` y `libstdc++.i686` para Red Hat Enterprise Linux Versión 7.1.

5. Cuando se completa la instalación de software, puede restaurar los valores de repositorio YUM originales completando los pasos siguientes:
   a. Desmonte el DVD de instalación de Red Hat Enterprise Linux emitiendo el siguiente mandato:

```
unmount /mnt
```

   b. Cambie al directorio de repositorio YUM emitiendo el siguiente mandato:

```
cd /etc/yum/repos.d
```

   c. Cambie el nombre del archivo repo que ha creado:

```
mv rhel71_dvd.repo rhel71_dvd.repo.orig
```

   d. Cambie el nombre del archivo original al nombre original:

```
mv rhel-source.repo.orig rhel-source.repo
```

6. Determine si son necesarios cambios de parámetro de kernel. Realice los pasos siguientes:
   a. Utilice el mandato **sysctl -a** para listar los valores de parámetro.
   b. Analice los resultados utilizando las directrices en Tabla 13 en la página 36 para determinar si es necesario algún cambio.
   c. Si se necesitan cambios, establezca los parámetros en el archivo `/etc/sysctl.conf`. Los cambios de archivo se aplican cuando se inicia el sistema.

Sugerencias:

- Los valores de parámetro de kernel listados en Tabla 13 incluyen comas para facilitar la lectura. No incluya comas para ningún valor que actualice en el archivo `/etc/sysctl.conf`.
- En Linux, el producto DB2 podría aumentar automáticamente los valores del parámetro de kernel de comunicación entre procesos (IPC) a los valores preferidos. Si el producto DB2 actualiza los valores que ha establecido, no es necesario volver a cambiarlos por los valores que están listados en Tabla 13.

Tabla 13. Valores óptimos del parámetro de kernel Linux

Parámetro	Descripción	Valor recomendado
kernel.shmmni	El número máximo de segmentos.	256 x *tamaño de RAM en GB* Valores para cada tamaño de sistema: • Pequeño: 16.384 • Mediano: 32.768 • Grande: 49.152
kernel.shmmax	El tamaño máximo de un segmento de memoria compartida (bytes). Este parámetro debe establecerse antes de iniciar automáticamente el servidor IBM Spectrum Protect durante el arranque del sistema.	*Tamaño de RAM en bytes* Valores para cada tamaño de sistema: • Pequeño: 68.719.476.736 • Mediano: 137.438.953.472 • Grande: 206.158.430.208
kernel.shmall	La asignación máxima de páginas de memoria compartida (páginas)	2 x *tamaño de RAM en bytes* (el valor está en páginas de 4 KB) Valor para todos los tamaños del sistema: 4,294,967,296 Los cambios en los valores de fábrica para este parámetro no son necesarios.

kernel.sem
 	
Debe especificar cuatro valores para el parámetro **kernel.sem**. Cuando actualice este parámetro, incluya todos los valores en una línea en el orden siguiente:
`kernel.sem = SEMMSL SEMMNS SEMOPM SEMMNI`
 	
Por ejemplo, para actualizar el parámetro para un sistema mediano, entre lo siguiente en una línea en el archivo `/etc/sysctl.conf`:
`kernel.sem = 250 256000 32 32768`
	(SEMMSL)
	
	Número de semáforos máximo por batería.
		250

	(SEMMNS) El número máximo de semáforos por sistema	256.000
	(SEMOPM) El número máximo de operaciones por llamada a semáforo	32
	(SEMMNI) Número máximo de baterías	256 x *tamaño de RAM en GB* Valores para cada tamaño de sistema: • Pequeño: 16.384 • Mediano: 32.768 • Grande: 49.152

Tabla 13. Valores óptimos del parámetro de kernel Linux (continuación)

Parámetro	Descripción	Valor recomendado
kernel.msgmni	El número máximo de colas de mensajes a nivel de sistema	1024 x *tamaño de RAM en GB* Valores para cada tamaño de sistema: • Pequeño: 65.536 • Mediano: 131.072 • Grande: 196.608
kernel.msgmax	Tamaño máximo de los mensajes (bytes).	65.536
kernel.msgmnb	El tamaño máximo predeterminado de colas (bytes)	65.536
kernel.randomize_va_space	El parámetro **kernel.randomize_va_space** configura el uso del ASLR de memoria para el kernel. Inhabilite ASLR, porque puede provocar errores para el software de DB2. Para obtener más detalles sobre Linux ASLR y DB2, consulte la nota técnica 1365583.	0
vm.swappiness	El parámetro **vm.swappiness** define si el kernel puede intercambiar memoria de aplicación de la memoria física de acceso aleatorio (RAM). Para obtener más información sobre los parámetros del kernel, consulte Información del producto DB2.	0
vm.overcommit_memory	El parámetro **vm.overcommit_memory** influye en la cantidad de memoria virtual que permite asignar el kernel. Para obtener más información sobre los parámetros del kernel, consulte Información del producto DB2.	0

7. Abra puertos de cortafuegos para comunicarse con el servidor. Realice los pasos siguientes:
   a. Determine la zona utilizada por la interfaz de red. De forma predeterminada, la zona es pública.

      Emita el mandato siguiente:

      ```
      #  firewall-cmd --get-active-zones
      public
        interfaces: ens4f0
      ```

   b. Para utilizar la dirección de puerto predeterminada para las comunicaciones con el servidor, abra el puerto TCP/IP 1500 en el cortafuegos de Linux.

      Emita el mandato siguiente:

      ```
      firewall-cmd --zone=public --add-port=1500/tcp --permanent
      ```

      Si desea utilizar un valor distinto del predeterminado, puede especificar un número en el rango 1024 - 32767. Si abre un puerto distinto del predeterminado, tendrá que especificar ese puerto cuando ejecute el script de configuración.

   c. Si piensa utilizar este sistema como concentrador, abra el puerto 11090, que es el puerto predeterminado para las comunicaciones seguras (https).

      Emita el mandato siguiente:

      ```
      firewall-cmd --zone=public --add-port=11090/tcp --permanent
      ```

   d. Vuelva a cargar las definiciones de cortafuegos para que los cambios entren en vigor.

Emita el mandato siguiente:

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

8. Verifique que los límites de recursos de proceso de usuario, también conocidos como *ulimits*, se han establecido de acuerdo con las directrices en Tabla 14. Si los valores ulimit no se establecen correctamente, es posible que experimente inestabilidad del servidor o un fallo en la respuesta del servidor.

Tabla 14. Valores de los límites de usuario (ulimit)

Tipo de límite de usuario	Valor	Valor	Mandato del valor de consulta
Tamaño máximo de archivos principales creados	`core`	Ilimitado	`ulimit -Hc`
Tamaño máximo de un segmento de datos para un proceso	`datos`	Ilimitado	`ulimit -Hd`
Tamaño de archivo máximo	`fsize`	Ilimitado	`ulimit -Hf`
Número máximo de archivos abiertos	`nofile`	65536	`ulimit -Hn`
La cantidad máxima de tiempo del procesador en segundos	`cpu`	Ilimitado	`ulimit -Ht`
Número máximo de procesos de usuario	`nproc`	16384	`ulimit -Hu`

Si necesita modificar los valores de límite de usuario, siga las instrucciones de la documentación para el sistema operativo.

Instalación en sistemas Windows

Instalar Microsoft Windows Server 2012 Standard Edition en el sistema del servidor y preparar el sistema para la instalación y configuración del servidor IBM Spectrum Protect.

Procedimiento

1. Instale Microsoft Windows Server 2012 R2 Standard Edition, de acuerdo con las instrucciones del fabricante.
2. Cambie las políticas de control de cuenta Windows completando los pasos siguientes.
   a. Abra el editor de política de seguridad local ejecutando `secpol.msc`.
   b. Pulse **Políticas locales** > **Opciones de seguridad** y asegúrese de que están inhabilitadas las políticas siguientes de control de cuenta de usuario:
      - Modo de aprobación de administrador para la cuenta de administrador integrado
      - Ejecute todos los administradores en Modo de aprobación de administrador
3. Configure los valores de TCP/IP según las instrucciones de instalación para el sistema operativo.
4. Aplique actualizaciones de Windows y habilite las funciones opcionales completando los pasos siguientes:

a. Aplique las últimas actualizaciones de Windows 2012 R2.
b. Instale y habilite la característica de Windows 2012 R2 Microsoft .NET Framework 3.5 de Windows Server Manager.
c. Si es necesario, actualice los controladores de dispositivo FC y Ethernet HBA a niveles más nuevos.
d. Instale el controlador de E/S de multivía de acceso que es adecuado para el sistema de disco que está utilizando.

5. Abra el puerto TCP/IP predeterminado, 1500, para las comunicaciones con el servidor IBM Spectrum Protect. Por ejemplo, emita el siguiente comando:

```
netsh advfirewall firewall add rule name="Backup server port 1500"
dir=in action=allow protocol=TCP localport=1500
```

6. En el servidor hub de Centro de operaciones, abra el puerto predeterminado para comunicaciones seguras (https) con Centro de operaciones. El número de puerto es 11090. Por ejemplo, emita el siguiente comando:

```
netsh advfirewall firewall add rule name="Centro de operaciones port 11090"
dir=in action=allow protocol=TCP localport=11090
```

Configuración de E/S de la multivía de acceso

Complete los pasos siguientes para habilitar y configurar las multivías de acceso para el almacenamiento de disco. Utilice la documentación que se proporciona con el hardware para obtener instrucciones detalladas.

Sistemas AIX

Procedimiento

1. Determine la dirección de puerto de canal de fibra que debe utilizar para la definición de host en el subsistema de disco. Emita el mandato **lscfg** para cada puerto.
   - En sistemas pequeños y medianos, emita los siguientes mandatos:

     ```
     lscfg -vps -l fcs0 | grep "Network Address"
     lscfg -vps -l fcs1 | grep "Network Address"
     ```

   - En sistemas grandes, emita los siguientes mandatos:

     ```
     lscfg -vps -l fcs0 | grep "Network Address"
     lscfg -vps -l fcs1 | grep "Network Address"
     lscfg -vps -l fcs2 | grep "Network Address"
     lscfg -vps -l fcs3 | grep "Network Address"
     ```

2. Asegúrese de que los siguientes conjuntos de archivos AIX están instalados:
   - devices.common.IBM.mpio.rte
   - devices.fcp.disk.array.rte
   - devices.fcp.disk.rte
3. Emita el mandato **cfgmgr** para hacer que AIX vuelva a explorar el hardware y descubrir los discos disponibles. Por ejemplo:

   ```
   cfgmgr
   ```

4. Para listar los discos disponibles, emita el siguiente mandato:

   ```
   lsdev -Ccdisk
   ```

   Deberá obtener unos resultados parecidos a los siguientes:

   ```
   hdisk0  Available 00-00-00 SAS Disk Drive
   hdisk1  Available 00-00-00 SAS Disk Drive
   hdisk2  Available 01-00-00 SAS Disk Drive
   ```

```
hdisk3  Available 01-00-00 SAS Disk Drive
hdisk4  Available 06-01-02 MPIO IBM 2076 FC Disk
hdisk5  Available 07-01-02 MPIO IBM 2076 FC Disk
...
```

5. Utilice la salida del mandato **lsdev** para identificar y listar ID de dispositivo para cada dispositivo de disco.

   Por ejemplo, `hdisk4`. Guarde la lista de ID de dispositivo a utilizar cuando crea sistemas de archivos para el servidor IBM Spectrum Protect.

6. Correlacione los ID de dispositivo SCSI para especificar los LUN de disco del sistema de discos listando la información detallada sobre todos los volúmenes físicos del sistema. Emita el mandato siguiente:

   ```
   lspv -u
   ```

   En un sistema IBM Storwize, la información siguiente es un ejemplo de lo que se muestra para cada dispositivo:

   ```
   hdisk4  00f8cf083fd97327  None  active
    3321360050763008101057800000000000030042145O3IBMfcp
   ```

   En el ejemplo, *600507630081010578000000000000030* es el ID de usuario para el volumen, como informa la interfaz de gestión Storwize.

   Para verificar el tamaño de disco en MB y compararlo con lo que se lista para el sistema, emita el siguiente mandato:

   ```
   bootinfo -s hdisk4
   ```

Sistemas Linux

Procedimiento

1. Edite el archivo `/etc/multipath.conf` para habilitar las multivías de acceso para los host de Linux. Si el archivo `multipath.conf` no existe, puede crearlo emitiendo el siguiente mandato:

   ```
   mpathconf --enable
   ```

   Los parámetros siguientes se han establecido en `multipath.conf` para realizar pruebas en un sistema IBM Storwize:

   ```
   defaults {
           user_friendly_names no
   }

   devices {
           device {
                   vendor "IBM "
                   product "2145"
                   path_grouping_policy group_by_prio
                   user_friendly_names no
           }
   }
   ```

2. Establezca la opción de multivía de acceso para iniciarse cuando se inicia el sistema. Emita los comandos siguientes:

   ```
   systemctl enable multipathd.service
   systemctl start multipathd.service
   ```

3. Para verificar que los discos están visibles para el sistema operativo y gestionados por una multivía de acceso, emita el siguiente mandato:

   ```
   multipath -l
   ```

4. Asegúrese de que se lista cada uno de los dispositivos y de que tiene tantas vías de acceso como esperaba. Puede utilizar la información de ID de dispositivo y tamaño para identificar qué discos se listan.

   Por ejemplo, la salida siguiente muestra que un disco de 2 TB tiene dos grupos de vías de acceso y cuatro vías de acceso activas. El tamaño de 2 TB confirma que el disco se corresponde con un sistema de archivos de la agrupación. Utilice parte del número ID de dispositivo largo (12, en este ejemplo) para buscar el volumen en la interfaz de gestión del sistema de discos.

   ```
   [root@tapsrv01 code]# multipath -l
   36005076802810c509800000000000012 dm-43 IBM,2145
    size=2.0T features='1 queue_if_no_path' hwhandler='0' wp=rw
   |-+- policy='round-robin 0' prio=0 status=active
   | |- 2:0:1:18 sdcw 70:64   active undef running
   | `- 4:0:0:18 sdgb 131:112 active undef running
   `-+- policy='round-robin 0' prio=0 status=enabled
     |- 1:0:1:18 sdat 66:208  active undef running
     `- 3:0:0:18 sddy 128:0   active undef running
   ```

   a. Si es necesario, corrija las asignaciones de host de LUN de disco y fuerce una reexploración. Por ejemplo:

      ```
      echo "- - -" > /sys/class/scsi_host/host0/scan
      echo "- - -" > /sys/class/scsi_host/host1/scan
      echo "- - -" > /sys/class/scsi_host/host2/scan
      ```

      También puede reiniciar el sistema para volver a explorar las asignaciones de host de LUN de disco.

   b. Confirme que los discos están ahora disponibles para la E/S de multivía de acceso volviendo a emitir el mandato **multipath -l**.

5. Utilice la salida de multivía de acceso para identificar y listar los ID de dispositivo para cada dispositivo de disco.

   Por ejemplo, el ID de dispositivo para el disco de 2 TB es 36005076802810c509800000000000012.

   Guarde la lista de ID de dispositivo para utilizarla en el paso siguiente.

Sistemas Windows

Procedimiento

1. Asegúrese de que la función de E/S de multivía de acceso está instalada. Si es necesario, instale controladores con varias vías de acceso específicas del proveedor adicionales.
2. Para verificar que los discos están visibles para el sistema operativo y gestionados por una E/S de multivía de acceso, emita el siguiente mandato:

   ```
   c:\program files\IBM\SDDDSM\datapath.exe query device
   ```

3. Revise la salida de multivía de acceso y asegúrese de que cada dispositivo está listado y de que tiene tantas vías de acceso como esperaba. Puede utilizar la información de serie del dispositivo y el tamaño para identificar qué discos se listan.

   Por ejemplo, utilizando parte del número de serie del dispositivo largo (34, en este ejemplo), puede buscar el volumen en la interfaz de gestión del sistema de discos. El tamaño de 2 TB confirma que el disco se corresponde con un sistema de archivos de la agrupación de almacenamiento.

   ```
   DEV#:   4  DEVICE NAME: Disk5 Part0   TYPE: 2145    POLICY: OPTIMIZED
   SERIAL: 60050763008101057800000000000034          LUN SIZE: 2.0TB
   ============================================================================
   Path#          Adapter/Hard Disk       State   Mode    Select  Errors
       0   Scsi Port2 Bus0/Disk5 Part0    OPEN    NORMAL       0       0
   ```

```
    1   Scsi Port2 Bus0/Disk5 Part0    OPEN    NORMAL   27176       0
    2   Scsi Port3 Bus0/Disk5 Part0    OPEN    NORMAL   28494       0
    3   Scsi Port3 Bus0/Disk5 Part0    OPEN    NORMAL       0       0
```

4. Cree una lista de ID de dispositivo de disco mediante los números de serie que se devuelven de la salida de multivía de acceso en el paso anterior.

   Por ejemplo, el ID de dispositivo para el disco de 2 TB es `600507630081010578000000000000034`

   Guarde la lista de ID de dispositivo para utilizarla en el paso siguiente.

5. Una vez que se han añadido los discos nuevos, es posible que tenga que activarlos y borrar el atributo de solo lectura. Ejecute `diskpart.exe` con los siguientes mandatos. Repítalo para cada uno de los discos:

```
diskpart
   select Disk 1
   online disk
   attribute disk clear readonly
   select Disk 2
   online disk
   attribute disk clear readonly
   < ... >
   select Disk 49
   online disk
   attribute disk clear readonly
   exit
```

Creación del ID de usuario para el servidor

Cree el ID de usuario que es propietario de la instancia de servidor de IBM Spectrum Protect. Especifique este ID de usuario cuando cree la instancia de servidor durante la configuración inicial del servidor.

Acerca de esta tarea

Solo puede especificar letras en minúsculas (a-z), números (0-9), y el carácter subrayado (_) para el ID de usuario. El ID de usuario y nombre de grupo deben cumplir las siguientes normas:

- La longitud debe ser de 8 caracteres o menos.
- El ID de usuario y el nombre del grupo no pueden empezar por *ibm*, *sql*, *sys* o un número.
- El ID de usuario y el nombre del grupo no pueden ser *user*, *admin*, *guest*, *public*, *local* o cualquier palabra reservada por SQL.

Procedimiento

1. Utilice mandatos del sistema operativo para crear un ID de usuario.
   - AIX Linux Cree un grupo y un ID de usuario en el directorio de inicio del usuario que es propietario de la instancia de servidor.

     Por ejemplo, para crear el ID de usuario `tsminst1` en el grupo `tsmsrvrs` con una contraseña de `tsminst1`, emita los siguientes mandatos desde un ID de usuario de administración:

     AIX

```
mkgroup id=1001 tsmsrvrs
mkuser id=1002 pgrp=tsmsrvrs home=/home/tsminst1 tsminst1
passwd tsminst1
```

     Linux

```
groupadd tsmsrvrs
useradd -d /home/tsminst1 -m -g tsmsrvrs -s /bin/bash tsminst1
passwd tsminst1
```

Cierre sesión y, a continuación, inicie sesión en el sistema. Vaya a la cuenta de usuario que ha creado. Utilice un programa de conexión interactivo, como Telnet, para que se le pida la contraseña y pueda cambiarla en caso de ser necesario.

- Windows Cree un ID de usuario y, a continuación, añada el nuevo ID a los grupos de administradores. Por ejemplo, para crear el ID de usuario `tsminst1`, emita el siguiente mandato:

  ```
  net user tsminst1 * /add
  ```

  Después de crear y verificar una contraseña para el nuevo usuario, añada el ID de usuario al grupo Administradores emitiendo los siguientes mandatos:

  ```
  net localgroup Administrators tsminst1 /add
  net localgroup DB2ADMNS tsminst1 /add
  ```

2. Cierre la sesión con el nuevo ID de usuario.

Preparación de sistemas de archivos para el servidor

Debe completar la configuración del sistema de archivos para el almacenamiento de disco que va a utilizar el servidor.

Sistemas AIX

Debe crear grupos de volúmenes, volúmenes lógicos y sistemas de archivos para el servidor utilizando el gestor de volúmenes lógicos de AIX.

Procedimiento

1. Aumente la profundidad de cola y el tamaño de transferencia máximo para todos los discos *hdiskX* disponibles listados en el paso anterior. Emita los siguientes mandatos para cada disco:

   ```
   chdev -l hdisk4 -a max_transfer=0x100000
   chdev -l hdisk4 -a queue_depth=32
   chdev -l hdisk4 -a reserve_policy=no_reserve
   chdev -l hdisk4 -a algorithm=round_robin
   ```

   No ejecute estos mandatos para discos internos del sistema operativo, por ejemplo, *hdisk0*.

2. Cree grupos de volúmenes para la base de datos, registro activo, registro de archivado, copia de seguridad de base de datos y agrupación de almacenamiento de IBM Spectrum Protect. Emita el mandato **mkvg**, especificando los ID de dispositivo para discos correspondientes que ha identificado previamente.

   Por ejemplo, si los nombres de dispositivo *hdisk4, hdisk5* y *hdisk6* corresponden a discos de base de datos, inclúyalos en el grupo de volúmenes de base de datos y, así, sucesivamente.

   Tamaño del sistema: Los siguientes mandatos se basan en la configuración del sistema mediano. Para sistemas pequeños y grandes, debe ajustar la sintaxis como sea necesario.

```
mkvg -S -y tsmdb hdisk2 hdisk3 hdisk4
mkvg -S -y tsmactlog hdisk5
mkvg -S -y tsmarchlog hdisk6
mkvg -S -y tsmdbback hdisk7 hdisk8 hdisk9 hdisk10
mkvg -S -y tsmstgpool hdisk11 hdisk12 hdisk13 hdisk14 ... hdisk49
```

3. Determine los nombres de volumen físico y el número de particiones físicas libre para utilizarlos cuando cree volúmenes lógicos. Emita **lsvg** para cada grupo de volúmenes que ha creado en el paso anterior.

   Por ejemplo:

   ```
   lsvg -p tsmdb
   ```

   La salida es similar a la siguiente. La columna *FREE PPs* representa las particiones físicas libres:

   ```
   tsmdb:
   PV_NAME  PV STATE   TOTAL PPs  FREE PPs  FREE DISTRIBUTION
   hdisk4   active     1631       1631      327..326..326..326..326
   hdisk5   active     1631       1631      327..326..326..326..326
   hdisk6   active     1631       1631      327..326..326..326..326
   ```

4. Cree volúmenes lógicos en cada grupo de volúmenes utilizando el mandato **mklv**. El tamaño de volumen, el grupo de volúmenes y los nombres de dispositivo varían, en función del tamaño del sistema y de las variaciones en la configuración de disco.

   Por ejemplo, para crear los volúmenes para la base de datos de IBM Spectrum Protect en un sistema mediano, emita los mandatos siguientes:

   ```
   mklv -y tsmdb00 -t jfs2 -u 1 -x 1631 tsmdb 1631 hdisk2
   mklv -y tsmdb01 -t jfs2 -u 1 -x 1631 tsmdb 1631 hdisk3
   mklv -y tsmdb02 -t jfs2 -u 1 -x 1631 tsmdb 1631 hdisk4
   ```

5. De formato a los sistemas de archivo en cada volumen lógico utilizando el mandato **crfs**.

   Por ejemplo, para formatear sistemas de archivos para la base de datos en un sistema mediano, emita los mandatos siguientes:

   ```
   crfs -v jfs2 -d tsmdb00 -p rw -a logname=INLINE -a options=rbrw
    -a agblksize=4096 -m /tsminst1/TSMdbspace00 -A yes
   crfs -v jfs2 -d tsmdb01 -p rw -a logname=INLINE -a options=rbrw
    -a agblksize=4096 -m /tsminst1/TSMdbspace01 -A yes
   crfs -v jfs2 -d tsmdb02 -p rw -a logname=INLINE -a options=rbrw
    -a agblksize=4096 -m /tsminst1/TSMdbspace02 -A yes
   ```

6. Monte todos los sistemas de archivo recién creados emitiendo el siguiente mandato:

   ```
   mount -a
   ```

7. Liste todos los sistemas de archivos emitiendo el mandato **df**. Verifique que los sistemas de archivos están montados en el LUN correcto y el punto de montaje correcto. Además, verifique el espacio disponible.

   El ejemplo siguiente de la salida del mandato muestra que la cantidad de espacio utilizado normalmente es un uno por ciento:

   ```
   tapsrv07> df -g /tsminst1/*
   Filesystem      GB blocks  Free     %Used   Iused   %Iused   Mounted on
   /dev/tsmact00   195.12     194.59   1%      4       1%       /tsminst1/TSMalog
   ```

8. Verifique que el ID de usuario que ha creado en “Creación del ID de usuario para el servidor” en la página 42 tiene acceso de lectura y escritura en los directorios para el servidor.

Sistemas Linux

Debe formatear los sistemas de archivos `ext4` o `xfs` en cada uno de los LUN de disco que va a utilizar el servidor IBM Spectrum Protect.

Procedimiento

1. Utilizando la lista de ID de dispositivo que ha generado en el paso anterior, emita el mandato **mkfs** para crear y dar formato a un sistema de archivos para cada dispositivo LUN de almacenamiento. Especifique el ID de dispositivo en el mandato. Consulte los ejemplos siguientes. Para la base de datos, formatee los sistemas de archivos `ext4`:

   ```
   mkfs -t ext4 -T largefile -m 2 /dev/mapper/36005076802810c509800000000000012
   ```

   Para las LUN de agrupación de almacenamiento, formatee los sistemas de archivos `xfs`:

   ```
   mkfs -t xfs /dev/mapper/3600507630081010578000000000002c3
   ```

   Puede emitir el mandato **mkfs** hasta 50 veces, dependiendo de cuántos dispositivos diferentes tiene.

2. Cree directorios de punto de montaje para sistemas de archivos.

   Emita el mandato **mkdir** para cada directorio que debe crear. Utilice los valores de directorio que ha registrado en las hojas de trabajo de planificación. Por ejemplo, para crear el directorio de instancia de servidor utilizando el valor predeterminado, emita el mandato siguiente

   ```
   mkdir /tsminst1
   ```

   Repita el mandato **mkdir** para cada sistema de archivos.

3. Añada una entrada en el archivo `/etc/fstab` para cada sistema de archivos para que los sistemas de archivos se monten automáticamente cuando se inicia el servidor.

   Por ejemplo:

   ```
   /dev/mapper/36005076802810c509800000000000012 /tsminst1/TSMdbspace00 ext4 defaults 0 0
   ```

4. Monte los sistemas de archivos que ha añadido al archivo `/etc/fstab` emitiendo el mandato **mount -a**.

5. Liste todos los sistemas de archivos emitiendo el mandato **df**. Verifique que los sistemas de archivos están montados en el LUN correcto y el punto de montaje correcto. Además, verifique el espacio disponible.

   El ejemplo siguiente en un sistema IBM Storwize muestra que la cantidad de espacio utilizado normalmente es uno por ciento:

   ```
   [root@tapsrv04 ~]# df -h /tsminst1/*
   Filesystem                                      Size  Used Avail Use% Mounted on
   /dev/mapper/3600507630081010578000000000000003 134G  188M 132G  1%   /tsminst1/TSMalog
   ```

6. Verifique que el ID de usuario que ha creado en “Creación del ID de usuario para el servidor” en la página 42 tiene acceso de lectura y escritura en los directorios para el servidor IBM Spectrum Protect.

Sistemas Windows

Debe formatear sistemas de archivos NTFS en cada una de las LUN de disco que va a utilizar el servidor IBM Spectrum Protect.

Procedimiento

1. Cree directorios de punto de montaje para sistemas de archivos.

   Emita el mandato **md** para cada directorio que debe crear. Utilice los valores de directorio que ha registrado en las hojas de trabajo de planificación. Por ejemplo, para crear el directorio de instancia de servidor utilizando el valor predeterminado, emita el mandato siguiente

   ```
   md c:\tsminst1
   ```

   Repita el mandato **md** para cada sistema de archivos.
2. Cree un volumen para cada LUN de disco que se correlaciona a un directorio bajo el directorio de instancia de servidor utilizando el gestor de volúmenes de Windows.

   Vaya a **Gestor de servidores** > **Servicios de archivo y almacenamiento** y complete los pasos siguientes para cada disco que corresponde a la correlación de LUN que se ha creado en el paso anterior:

   a. Ponga el disco en línea.
   b. Inicialice el disco en el tipo básico GPT, que es el valor predeterminado.
   c. Crear un volumen simple que ocupa todo el espacio en el disco. Dé formato al sistema de archivos utilizando NTFS y asignando una etiqueta que coincida con la finalidad del volumen, como `TSMfile00`. No asigna el nuevo volumen a la letra de unidad. En su lugar, correlacione el volumen a un directorio bajo el directorio de instancia, como `C:\tsminst1\TSMfile00`.

      Consejo: Determine la etiqueta de volumen y las etiquetas de correlación de directorio en función del tamaño del disco del que se informa.
3. Verifique que los sistemas de archivos están montados en el LUN correcto y el punto de montaje correcto. Liste todos los sistemas de archivos emitiendo el mandato **mountvol** y, a continuación, revise la salida. Por ejemplo:

   ```
   \\?\Volume{8ffb9678-3216-474c-a021-20e420816a92}\
     C:\tsminst1\TSMdbspace00\
   ```
4. Una vez se ha completado la configuración de disco, reinicie el sistema.

Qué hacer a continuación

Puede confirmar la cantidad de espacio libre para cada volumen utilizando Windows Explorer.

Capítulo 7. Instalación del servidor y Centro de operaciones

Utilice el asistente gráfico de IBM Installation Manager para instalar los componentes.

Instalación en sistemas AIX y Linux

Instalar el servidor IBM Spectrum Protect y Centro de operaciones en el mismo sistema.

Antes de empezar

Compruebe que el sistema operativo esté establecido en el idioma que necesita. De forma predeterminada, el idioma del sistema operativo es el idioma del asistente de instalación.

Procedimiento

1. AIX Verifique que los archivo RPM necesarios están instalados en el sistema.

   Consulte "Instalación de archivos RPM de requisitos previos para el asistente gráfico" en la página 48 para obtener más detalles.
2. Antes de descargar el paquete de instalación, verifique que tiene espacio suficiente para almacenar los archivos de instalación cuando estos sean extraídos del paquete del producto. Para los requisitos de espacio, consulte el documento de descarga en nota técnica 4042992.
3. Vaya a Passport Advantage y descargue el archivo de paquete en un directorio vacío de su elección.
4. Asegúrese de que el permiso ejecutable está establecido para el paquete. Si es necesario, cambie las autorizaciones del archivo al emitir el mandato siguiente:

   ```
   chmod a+x package_name.bin
   ```
5. Extraiga el paquete emitiendo el siguiente mandato:

   ```
   ./nombre_paquete.bin
   ```

   donde *package_name* es el nombre del archivo descargado.
6. AIX Asegúrese de que el mandato siguiente está habilitado, de forma que los asistentes funcionen correctamente:

   ```
   lsuser
   ```

   De manera predeterminada, el mandato está habilitado.
7. Cambie al directorio en el que colocó el archivo ejecutable.
8. Inicie el asistente de instalación emitiendo el mandato siguiente:

   ```
   ./install.sh
   ```

   Cuando seleccione los paquetes a instalar, elija el servidor y Centro de operaciones.

Qué hacer a continuación

- Si se producen errores durante el proceso de instalación, los errores se registran en los archivos de registro se almacenan en el directorio de registros del Gestor de instalación de IBM.

  Para ver archivos de registro de instalación desde la herramienta de Installation Manager, pulse **Archivo** > **Ver registro**. Para recopilar estos archivos de registro desde la herramienta Installation Manager, pulse **Ayuda** > **Exportar datos para el análisis de problemas**.
- Tras instalar el servidor y antes de personalizarlo para su uso, vaya a Sitio de soporte de IBM Spectrum Protect. Pulse **Soporte y descargas** y aplique todo arreglo aplicable.

Tareas relacionadas:

Otros métodos para instalar componentes de IBM Spectrum Protect (AIX)

Otros métodos para instalar componentes de IBM Spectrum Protect (Linux)

Instalación de archivos RPM de requisitos previos para el asistente gráfico

AIX

Los archivos RPM son necesarios para el asistente gráfico Gestor de instalación de IBM.

Procedimiento

1. Verifique que los siguientes archivos están instalados en el sistema. Si los archivos no están instalados, vaya al Paso 2.

   ```
   atk-1.12.3-2.aix5.2.ppc.rpm
   cairo-1.8.8-1.aix5.2.ppc.rpm
   expat-2.0.1-1.aix5.2.ppc.rpm
   fontconfig-2.4.2-1.aix5.2.ppc.rpm
   freetype2-2.3.9-1.aix5.2.ppc.rpm
   gettext-0.10.40-6.aix5.1.ppc.rpm
   glib2-2.12.4-2.aix5.2.ppc.rpm
   gtk2-2.10.6-4.aix5.2.ppc.rpm
   libjpeg-6b-6.aix5.1.ppc.rpm
   libpng-1.2.32-2.aix5.2.ppc.rpm
   libtiff-3.8.2-1.aix5.2.ppc.rpm
   pango-1.14.5-4.aix5.2.ppc.rpm
   pixman-0.12.0-3.aix5.2.ppc.rpm
   xcursor-1.1.7-3.aix5.2.ppc.rpm
   xft-2.1.6-5.aix5.1.ppc.rpm
   xrender-0.9.1-3.aix5.2.ppc.rpm
   zlib-1.2.3-3.aix5.1.ppc.rpm
   ```
2. Asegúrese de que existan al menos 150 MB de espacio libre en el sistema de archivos `/opt`.
3. Desde el directorio donde se extrae el archivo de paquete de instalación, vaya al directorio de `gtk`.
4. Descargue los archivos RPM en el directorio de trabajo actual del sitio web de IBM AIX Toolbox for Linux Applications emitiendo el mandato siguiente:

   ```
   download-prerequisites.sh
   ```
5. Desde el directorio que contiene los archivos RPM que ha descargado, instálelos emitiendo el siguiente mandato:

   ```
   rpm -Uvh *.rpm
   ```

Instalación en sistemas Windows

Instalar el servidor IBM Spectrum Protect y Centro de operaciones en el mismo sistema.

Antes de empezar

Asegúrese de que se cumplen los siguientes requisitos previos:

- Compruebe que el sistema operativo esté establecido en el idioma que necesita. De forma predeterminada, el idioma del sistema operativo es el idioma del asistente de instalación.
- Asegúrese de que el ID de usuario que piensa utilizar durante la instalación es un usuario con autoridad de administrador local.

Procedimiento

1. Antes de descargar el paquete de instalación, verifique que tiene espacio suficiente para almacenar los archivos de instalación cuando estos sean extraídos del paquete del producto. Para los requisitos de espacio, consulte el documento de descarga en nota técnica 4042993.
2. Vaya a Passport Advantage y descargue el archivo de paquete en un directorio vacío de su elección.
3. Cambie al directorio en el que colocó el archivo ejecutable.
4. Efectúe doble pulsación en el archivo ejecutable para extraerlo al directorio actual.
5. En el directorio donde se han extraído los archivos de instalación, inicie el asistente de instalación efectuando una doble pulsación en el archivo `install.bat`. Cuando seleccione los paquetes a instalar, elija el servidor y Centro de operaciones.

Qué hacer a continuación

- Si se producen errores durante el proceso de instalación, los errores se registran en los archivos de registro se almacenan en el directorio de registros del Gestor de instalación de IBM.

  Para ver archivos de registro de instalación desde la herramienta de Installation Manager, pulse **Archivo** > **Ver registro**. Para recopilar estos archivos de registro desde la herramienta Installation Manager, pulse **Ayuda** > **Exportar datos para el análisis de problemas**.
- Tras instalar el servidor y antes de personalizarlo para su uso, vaya a Sitio de soporte de IBM Spectrum Protect. Pulse **Soporte y descargas** y aplique todo arreglo aplicable.

Tareas relacionadas:

Otros métodos para instalar componentes de IBM Spectrum Protect

Capítulo 8. Configuración del servidor y el Centro de operaciones

Después de instalar los componentes, complete la configuración del servidor de IBM Spectrum Protect y el Centro de operaciones.

Configuración de la instancia de servidor

Utilice el asistente de configuración de instancia de servidor IBM Spectrum Protect para completar la configuración inicial del servidor.

Antes de empezar

Asegúrese de que se cumplen los siguientes requisitos:

AIX Linux

- El sistema en el que instaló IBM Spectrum Protect debe tener el cliente sistema X Windows. Además, debe estar ejecutando un servidor de sistema X Windows en su escritorio.
- El sistema debe tener el protocolo Secure Shell (SSH) habilitado. Asegúrese de que el puerto está establecido en el valor predeterminado, 22, y que el puerto no está bloqueado por un cortafuegos. Debe habilitar la autenticación de contraseña en el archivo `sshd_config` en el directorio de `/etc/ssh/`. También, asegúrese de que el servicio de daemon SSH tiene derechos de acceso para conectarse al sistema utilizando el valor *localhost*.
- Debe poder iniciar sesión en IBM Spectrum Protect con el ID de usuario que ha creado para la instancia del servidor, mediante el protocolo SSH. Cuando utilice el asistente, debe proporcionar el ID de usuario y la contraseña para acceder a ese sistema.
- Si ha cambiado cualquier valor en los pasos anteriores, reinicie el servidor antes de continuar con el asistente de configuración.

Windows Verifique que el servicio de registro remoto se ha iniciado completando los pasos siguientes:

1. Pulse **Inicio** > **Herramientas administrativas** > **Servicios**. En la ventana Servicios, seleccione **Registro remoto**. Si no se ha iniciado, pulse **Inicio**.
2. Asegúrese de que los puertos 137, 139 y 445 no están bloqueados por un cortafuegos:
   a. Pulse **Inicio** > **Panel de control** > **Cortafuegos de Windows**.
   b. Seleccione **Configuración avanzada**.
   c. Seleccione **Reglas de entrada**.
   d. Seleccione **Nueva regla**.
   e. Cree una regla de puerto para los puertos TCP 137, 139 y 445 para permitir conexiones para redes de dominio y privadas.
3. Configure el control de cuenta de usuario accediendo a las opciones de política de seguridad local y completando los siguientes pasos.
   a. Pulse **Inicio** > **Herramientas administrativas** > **Política de seguridad local**. Expanda **Políticas locales** > **Opciones de seguridad**.

b. Si no se ha habilitado, habilite la cuenta de administrador incorporada seleccionando **Cuentas: Estado de cuenta de administrador** > **Habilitar** > **Aceptar**.

c. Si aún no se ha inhabilitado, inhabilite el control de cuenta de usuario para todos los administradores de Windows seleccionando **Control de cuenta de usuario: Ejecutar todos los administradores en modo de aprobación de administrador** > **Inhabilitar** > **Aceptar** .

d. Si aún no se ha inhabilitado, inhabilite el Control de cuenta de usuario para la cuenta de administrador incorporada seleccionando **Control de cuenta de usuario: Modo de aprobación de administrador para la cuenta de administrador incorporada** > **Inhabilitar** > **Aceptar**.

4. Si ha cambiado cualquier valor en los pasos anteriores, reinicie el servidor antes de continuar con el asistente de configuración.

Acerca de esta tarea

El asistente se puede detener y reiniciar, pero el servidor no funcionará hasta que no haya finalizado completamente el proceso de configuración.

Procedimiento

1. Inicie la versión local del asistente.
   - AIX Linux Abra el programa `dsmicfgx` en el directorio `/opt/tivoli/tsm/server/bin`. Este asistente sólo puede ejecutarse como usuario root.
   - Windows Pulse **Inicio** > **Todos los programas** > **IBM Spectrum Protect** > **Asistente de configuración**.
2. Siga las instrucciones para completar la configuración. Utilice la información que ha registrado en Capítulo 3, “Planificación de hojas de trabajo”, en la página 9 para la configuración del sistema IBM Spectrum Protect para especificar directorios y opciones en el asistente.

   AIX Linux En la ventana Información de servidor, establezca el servidor para que se inicie automáticamente utilizando el ID de usuario de instancia cuando se arranca el sistema.

   Windows Utilizando el asistente de configuración, el servidor se configura para iniciarse de forma automática cuando se reinicia.

Instalación del cliente de archivado y copia de seguridad

Se recomienda instalar el cliente de archivado y copia de seguridad de IBM Spectrum Protect en el sistema servidor para que el cliente de línea de mandatos administrativos y el planificador estén disponibles?

Procedimiento

Para instalar el cliente de archivado y copia de seguridad, siga las instrucciones de instalación para el sistema operativo.

- Instalación de los clientes de archivado y copia de seguridad de UNIX y Linux
- Instalación del cliente de archivado y copia de seguridad de Windows

Configuración de opciones para el servidor

Revise el archivo de opciones de servidor que está instalado con el servidor IBM Spectrum Protect para verificar que se han establecido los valores correctos para el sistema.

Procedimiento

1. Vaya al directorio de instancia de servidor y abra el archivo `dsmserv.opt`.
2. Revise los siguientes valores de tabla y verifique los valores de opciones de servidor, basándose en el tamaño del sistema.

Opción de servidor	Valor del sistema pequeño	Valor del sistema mediano	Valor del sistema grande
ACTIVELOGDIRECTORY	Vía de acceso de directorio especificada durante la configuración	Vía de acceso de directorio especificada durante la configuración	Vía de acceso de directorio especificada durante la configuración
ACTIVELOGSIZE	131072	131072	262144
ARCHLOGCOMPRESS	Sí	No	No
ARCHLOGDIRECTORY	Vía de acceso de directorio especificada durante la configuración	Vía de acceso de directorio especificada durante la configuración	Vía de acceso de directorio especificada durante la configuración
COMMMETHOD	TCPIP	TCPIP	TCPIP
COMMTIMEOUT	3600	3600	3600
DEDUPREQUIRESBACKUP	No	No	No
DEVCONFIG	`devconf.dat`	`devconf.dat`	`devconf.dat`
EXPINTERVAL	0	0	0
IDLETIMEOUT	60	60	60
MAXSESSIONS	250	500	1000
NUMOPENVOLSALLOWED	20	20	20
TCPADMINPORT	1500	1500	1500
TCPPORT	1500	1500	1500
VOLUMEHISTORY	`volhist.dat`	`volhist.dat`	`volhist.dat`

   Actualice los valores de opción de servidor si es necesario, para que coincidan con los valores de la tabla. Para realizar actualizaciones, cierre el archivo `dsmserv.opt` y utilice el mandato **SETOPT** desde la interfaz de línea de mandatos de administración para establecer las opciones.

   Por ejemplo, para actualizar la opción `IDLETIMEOUT` a 60, emita el siguiente mandato:

   ```
   setopt idletimeout 60
   ```

3. Para configurar comunicaciones seguras para el servidor, clientes y Centro de operaciones, verifique las opciones de la tabla siguiente.

Opción de servidor	Todos los tamaños del sistema
SSLDISABLELEGACYTLS	YES
SSLFIPSMODE	NO

Opción de servidor	Todos los tamaños del sistema
SSLTCPPORT	Especifique el número de puerto SSL. La unidad de comunicación TCP/IP del servidor espera peticiones en este puerto para sesiones con SSL activada del cliente.
SSLTCPADMINPORT	Especifique la dirección del puerto en la que el servidor esperará las solicitudes de sesiones habilitadas para SSL del cliente de administración de línea de mandatos.
SSLTLS12	YES

Si alguno de los valores de opción debe actualizarse, edite el archivo `dsmserv.opt` utilizando las siguientes directrices:

- Elimine el asterisco del principio de la línea para habilitar una opción.
- En cada línea, especifique solo una opción y el valor especificado para la opción.
- Si se produce una opción en varias entradas del archivo, el servidor utiliza la última entrada.

Guarde los cambios y cierre el archivo. Si edita el archivo `dsmserv.opt` directamente, tendrá que reiniciar el servidor para que se apliquen los cambios.

Referencia relacionada:

Referencia de opciones de servidor

SETOPT (Establecer una opción de servidor para actualización dinámica)

Configuración de comunicaciones seguras con Seguridad de la capa de transporte

Si el entorno requiere las comunicaciones seguras, puede configurar SSL (Capa de sockets seguros) y TLS (Seguridad de la capa de transporte) en el cliente de archivado y copia de seguridad y el servidor de IBM Spectrum Protect para cifrar los datos. Se utiliza un certificado SSL para verificar las solicitudes de comunicación entre el servidor y el cliente.

Acerca de esta tarea

Tal como se indica en la figura siguiente, puede configurar comunicaciones SSL/TLS entre el servidor y el cliente de archivado y copia de seguridad definiendo opciones en los archivos de opciones de servidor y cliente y, después, transfiriendo el certificado firmado automáticamente que se ha generado en el servidor al cliente.

Cuando se actualiza el archivo de opciones de servidor en "Configuración de opciones para el servidor" en la página 53, las opciones de servidor **SSLTLS12** y **SSLDISABLELEGACYTLS** se establecen para restringir comunicaciones seguras para utilizar TLS 1.2. Este valor impide el uso de niveles de protocolo TLS anteriores, que son menos seguros.

Procedimiento

Para configurar el servidor y los clientes para SSL o TLS, complete los pasos siguientes:

1. Cree el archivo de base de datos de claves, `dsmcert.kdb` en cada cliente. Emita el mandato siguiente en el directorio `bin` en el cliente:

   ```
   gsk8capicmd_64 -keydb -create -populate
   -db dsmcert.kdb -pw password -stash
   ```

2. Cambie el certificado predeterminado en el archivo de base de datos de conjunto de claves `cert.kdb` por la etiqueta `"TSM Server SelfSigned SHA Key"`. Emita el siguiente mandato desde el directorio de instancia de servidor:

   ```
   gsk8capicmd_64 -cert -setdefault -db cert.kdb
   -stashed -label "TSM Server SelfSigned SHA Key"
   ```

3. Transfiera manualmente el archivo `cert256.arm` del servidor IBM Spectrum Protect a los sistemas de cliente.

   `cert256.arm` se crea en el directorio de instancia de servidor cuando se especifica la opción de servidor **SSLTCPPORT**.

4. Especifique las opciones siguientes en el archivo de opciones de cliente:
   - Establezca la opción **ssl** en `yes`.
   - Establezca el valor de la opción **tcpport** para que coincida con el valor de la opción **SSLTCPPORT** que está establecido en el servidor.

Configuración de Centro de operaciones

Después de instalar el Centro de operaciones, complete los siguientes pasos de configuración para iniciar la gestión del entorno de almacenamiento.

Antes de empezar

Cuando se conecte a Centro de operaciones por primera vez, debe proporcionar la siguiente información:

- La información de conexión para el servidor que desea designar como servidor concentrador.
- Credenciales de inicio de sesión para un ID de administrador que está definido para dicho servidor

Procedimiento

1. Designe el servidor concentrador. En un navegador web, introduzca la siguiente dirección:

   `https://hostname:secure_port/oc`

   donde:

   - *nombre_host* representa el nombre del sistema donde está instalado Centro de operaciones
   - *puerto_seguro* representa el número de puerto que utiliza Centro de operaciones para una comunicación HTTPS en ese sistema

   Por ejemplo, si el nombre de host es tsm.storage.mylocation.com y está utilizando el puerto seguro predeterminado para Centro de operaciones, que es 11090, la dirección es:

   `https://tsm.storage.mylocation.com:11090/oc`

   Al iniciar sesión en Centro de operaciones por primera vez, un asistente le guiará a través de la configuración inicial para establecer un nuevo administrador con la autoridad del sistema en el servidor.
2. Establezca comunicaciones seguras entre Centro de operaciones y el servidor hub configurando el protocolo de la capa de sockets seguros (SSL).

   Siga las instrucciones de "Protección de las comunicaciones entre el Centro de operaciones y el servidor hub".
3. Opcional: Para recibir un informe de correo electrónico diario que resuma el estado del sistema, configure los valores de correo electrónico en Centro de operaciones.

   Siga las instrucciones de Capítulo 14, "Seguimiento del estado del sistema mediante informes de correo electrónico", en la página 91.

Protección de las comunicaciones entre el Centro de operaciones y el servidor hub

Para proteger las comunicaciones entre el Centro de operaciones y el servidor hub utilizando el protocolo de Capa de sockets seguros (SSL), añada el certificado SSL del servidor hub al archivo de almacén de confianza del Centro de operaciones.

Antes de empezar

El archivo de almacén de confianza de Centro de operaciones es un contenedor para certificados SSL a los que Centro de operaciones puede acceder. Contiene el certificado SSL que Centro de operaciones usa para la comunicación HTTPS con los navegadores web.

Durante la instalación de Centro de operaciones, cree una contraseña para el archivo del almacén de confianza. Para configurar la comunicación SSL entre Centro de operaciones y el servidor central, debe usar la misma contraseña para agregar el certificado SSL del servidor central al archivo del almacén de confianza. Si no recuerda la contraseña, puede restaurarla.

La figura siguiente ilustra los componentes para configurar SSL entre el Centro de operaciones y el servidor hub.

Acerca de esta tarea

Este procedimiento proporciona pasos para implementar las comunicaciones seguras utilizando certificados autofirmados. Para utilizar certificados de entidad emisora de certificados (CA), siga las instrucciones de Configuración de SSL y TLS utilizando certificados firmados por CA.

Procedimiento

Para configurar la comunicación SSL utilizando certificados autofirmados, complete los pasos siguientes.

1. Especifique el certificado `cert256.arm` como certificado predeterminado en el archivo de base de datos de claves del servidor hub:
   a. Emita el siguiente mandato desde el directorio de la instancia del servidor central:

      ```
      gsk8capicmd_64 -cert -setdefault -db cert.kdb -stashed
           -label "TSM Server SelfSigned SHA Key"
      ```

   b. Reinicie el servidor central de manera que pueda recibir los cambios en el archivo de la base de datos clave.
   c. Verifique que el certificado `cert256.arm` se establece como predeterminado. Emita el mandato siguiente:

      ```
      gsk8capicmd_64 -cert -list -db cert.kdb -stashed
      ```

2. Detenga el servidor web de Centro de operaciones.
3. Abra la línea de mandatos de sistema operativo en el sistema donde se ha instalado el Centro de operaciones y cambie al siguiente directorio:
   - AIX Linux *dir_instalación*/ui/jre/bin
   - Windows *dir_instalación*\ui\jre\bin

   Donde *dir_instalación* representa el directorio en el que se ha instalado Centro de operaciones.
4. Abra la ventana de IBM Key Management emitiendo el siguiente mandato:
   ```
   ikeyman
   ```
5. Pulse **Archivo de base de datos de claves** > **Abrir**.
6. Pulse **Examinar** y vaya al siguiente directorio donde *dir_instalación* representa el directorio en el que está instalado Centro de operaciones:
   - AIX Linux *dir_instalación*/ui/Liberty/usr/servers/guiServer
   - Windows *dir_instalación*\ui\Liberty\usr\servers\guiServer
7. En el directorio `guiServer`, seleccione el archivo `gui-truststore.jks`.
8. Pulse **Abrir**, y pulse **Aceptar**.
9. Especifique la contraseña del archivo de almacén de confianza y pulse **Aceptar**.
10. En el área de contenidos de la base de datos de claves de la ventana IBM Key Management, pulse la flecha y seleccione **Certificados de firmante** de la lista. Pulse **Añadir**.
11. En la ventana Abrir, pulse **Examinar** y vaya al directorio de instancia del servidor hub:
    - AIX Linux `/opt/tivoli/tsm/server/bin`
    - Windows `c:\Program Files\Tivoli\TSM\server1`

    El directorio contiene los siguientes certificados de SSL:
    ```
    cert.arm
    cert256.arm
    ```

    Si no puede acceder al directorio de instancia del servidor hub desde la ventana Abrir, complete los pasos siguientes:
    a. Utilice FTP u otro método de transferencia de archivos para copiar los archivos `cert256.arm` desde el servidor hub al siguiente directorio en el sistema donde está instalado Centro de operaciones:
       - AIX Linux *dir_instalación*/ui/Liberty/usr/servers/guiServer
       - Windows *dir_instalación*\ui\Liberty\usr\servers\guiServer

    b. En la ventana Abrir, vaya al directorio `guiServer`.
12. Seleccione el certificado `cert256.arm` como certificado SSL.
13. Pulse **Abrir**, y pulse **Aceptar**.
14. Escriba una etiqueta para el certificado. Por ejemplo, escriba el nombre del servidor central.
15. Pulse **Aceptar**. El certificado SSL del servidor hub se añade al archivo de almacén de confianza y la etiqueta se visualiza en el área de contenidos de la base de datos de claves de la ventana IBM Key Management.
16. Cierre la ventana IBM Key Management.
17. Inicie el servidor web Centro de operaciones.

18. Complete los pasos siguientes en la ventana de inicio de sesión del asistente de configuración:
    a. En el campo **Conectar a**, entre el valor de la opción de servidor **SSLTCPADMINPORT** como el número de puerto.
    b. Seleccione **Usar SSL**.

Tareas relacionadas:

"Inicio y detención del servidor web" en la página 96

Registro de la licencia de producto

Para registrar la licencia para el producto IBM Spectrum Protect, utilice el mandato **REGISTER LICENSE**.

Acerca de esta tarea

Las licencias se almacenan en archivos de certificados de inscripción, que contienen información de licencias para el producto. Los archivos de certificado de inscripción se encuentran en el soporte de instalación y se colocan en el servidor durante la instalación. Al registrar el producto, las licencias se almacenan en un archivo NODELOCK en el directorio actual.

Procedimiento

Registre una licencia especificando el nombre del archivo de certificado de inscripción que contiene la licencia. Para utilizar el creador de mandato del Centro de operaciones para esta tarea, realice los pasos siguientes.

1. Abra el Centro de operaciones.
2. Abra el creador de mandatos del Centro de operaciones pasando el cursor por encima del icono de configuración y pulsando **Creador de mandatos**.
3. Emita el mandato **REGISTER LICENSE**. Por ejemplo, para registrar una licencia de base de IBM Spectrum Protect, emita el siguiente mandato:

```
register license file=tsmbasic.lic
```

Qué hacer a continuación

Guarde el soporte de instalación que contiene los archivos de certificados de inscripción. Es posible que tenga que registrar la licencia de nuevo si, por ejemplo, se produce una de las condiciones siguientes:

- El servidor e ha trasladado a otro sistema.
- El archivo NODELOCK está dañado. El servidor almacena información de licencia en el archivo NODELOCK, que está en el directorio desde el cual se ha iniciado el servidor.
- Linux Si cambia el chip del procesador que está asociado al servidor en el cual está instalado el servidor.

Referencia relacionada:

REGISTER LICENSE (Registrar una nueva licencia)

Configuración de la optimización de almacenamiento de datos

Crear una agrupación de almacenamiento de contenedores de directorio y al menos un directorio para utilizar la deduplicación de datos en línea.

Antes de empezar

Utilice la información de directorio de agrupación de almacenamiento que ha registrado en Capítulo 3, “Planificación de hojas de trabajo”, en la página 9 para esta tarea.

Procedimiento

1. Abra el Centro de operaciones.
2. En la barra de menús de Centro de operaciones, pase el cursor por encima de **Almacenamiento**.
3. En la lista que se visualiza, pulse **Agrupaciones de almacenamiento**.
4. Pulse el botón **+Agrupación de almacenamiento**.
5. Complete los pasos del asistente Añadir agrupación de almacenamiento:
   - Para utilizar la deduplicación de datos en línea, seleccione una agrupación de almacenamiento de **Directorio** bajo el almacenamiento basado en contenedor.
   - Cuando configure directorios para la agrupación de almacenamiento de contenedores de directorio, especifique las vías de acceso de directorio que ha creado para el almacenamiento durante la configuración del sistema.
6. Tras configurar la nueva agrupación de almacenamiento de contenedor de directorio, pulse **Cerrar y ver políticas** para actualizar una clase de gestión y empezar a utilizar la agrupación de almacenamiento.

Definición de las reglas de retención de datos para su empresa

Después de crear una agrupación de almacenamiento de contenedores de directorio para deduplicación de datos, actualice la política de servidor predeterminada para utilizar la nueva agrupación de almacenamiento. El asistente Añadir agrupación de almacenamiento abre la página Servicios en el Centro de operaciones para completar esta tarea.

Procedimiento

1. En la página Servicios del Centro de operaciones, seleccione el dominio STANDARD y pulse **Detalles**.
2. En la página Resumen del dominio de políticas, pulse el separador **Conjuntos de políticas**. La página Conjuntos de políticas indica el nombre del conjunto de políticas activo y lista todas las clases de gestión pare ese conjunto de políticas.
3. Pulse el conmutador **Configurar** y realice los cambios siguientes:
   - Cambie el destino de copia de seguridad para la clase de gestión STANDARD a la agrupación de almacenamiento de contenedor de directorio.
   - Cambie el valor de la columna de copias de seguridad a **Sin límite**.
   - Cambie el periodo de retención. Establezca la columna para conservar copias de seguridad adicionales en 30 días o más, en función de los requisitos empresariales.
4. Guarde los cambios y haga clic de nuevo en el conmutador **Configurar** para que el conjunto de políticas ya no se pueda editar.
5. Activar el conjunto de políticas pulsando **Activar**.

Definición de planificaciones para actividades de mantenimiento del servidor

Cree planificaciones para cada operación de mantenimiento de servidor utilizando el mandato **DEFINE SCHEDULE** en el generador de mandatos de Centro de operaciones.

Acerca de esta tarea

Planifique operaciones de mantenimiento de servidor para ejecutar después de las copias de seguridad de cliente. Puede controlar la temporización de planificaciones para las tareas de mantenimiento estableciendo la hora de inicio en combinación con la duración para cada operación.

El ejemplo siguiente muestra cómo puede planificar los procesos de mantenimiento de servidor en combinación con la planificación de copia de seguridad de cliente para una solución de disco de un sitio único.

Operación	Planificación
Copia de seguridad del cliente	Empieza a las 22:00.
Proceso para archivos de recuperación ante siniestro y de base de datos	• La copia de seguridad de base de datos se inicia a las 11:00, o 13 horas después del comienzo de la copia de seguridad de cliente. Este proceso se ejecuta hasta completarse. • La información de configuración de dispositivos y la copia de seguridad del historial de volumen comienza a las 17:00 o 6 horas después del inicio de la copia de seguridad de la base de datos. • La supresión del historial de volumen comienza a las 20:00 o 9 horas después del inicio de la copia de seguridad de la base de datos.
Caducidad de inventario	Se inicia a las 12:00, o 14 horas después del comienzo de la copia de seguridad del cliente. Este proceso se ejecuta hasta completarse.

Procedimiento

Tras configurar la clase de dispositivo para las copias de seguridad de base de datos, cree planificaciones para la copia de seguridad de la base de datos y otras operaciones de mantenimiento necesarias utilizando el mandato **DEFINE SCHEDULE**. En función del tamaño del entorno, es posible que tenga que ajustar las horas de inicio para cada planificación del ejemplo.

1. Defina una clase de dispositivo para la operación de seguridad antes de crear la planificación para copias de seguridad de base de datos. Utilice el mandato **DEFINE DEVCLASS** para crear una clase de dispositivo que se denomine DBBACK_FILEDEV:

   ```
   define devclass dbback_filedev devtype=file
     directory=directorios_copia_seguridad_bd
   ```

   donde *directorios_copia_seguridad_bd* es una lista de los directorios que ha creado para la copia de seguridad de base de datos.

AIX Linux Por ejemplo, si tiene cuatro directorios para copias de seguridad de base de datos, empezando por el mandato `/tsminst1/TSMbkup00`, emita el mandato siguiente:

```
define devclass dbback_filedev devtype=file
  directory=/tsminst1/TSMbkup00,
  /tsminst1/TSMbkup01,/tsminst1/TSMbkup02,
  /tsminst1/TSMbkup03"
```

Windows Por ejemplo, si tiene cuatro directorios para copias de seguridad de base de datos, empezando con `C:\tsminst1\TSMbkup00`, emita el mandato siguiente:

```
define devclass dbback_filedev devtype=file
  directory="c:\tsminst1\TSMbkup00,
  c:\tsminst1\TSMbkup01,c:\tsminst1\TSMbkup02,c:\tsminst1\TSMbkup03"
```

2. Establezca la clase de dispositivo para copias de seguridad de base de datos automáticas. Utilice **SET DBRECOVERY** para especificar la clase de dispositivo que ha creado para la copia de seguridad de base de datos en el paso anterior. Por ejemplo, si la clase de dispositivo es dbback_filedev, emita el mandato siguiente:

   ```
   set dbrecovery dbback_filedev
   ```

3. Cree planificaciones para las operaciones de mantenimiento utilizando el mandato **DEFINE SCHEDULE**. Consulte la tabla siguiente para las operaciones necesarias con ejemplos de los mandatos.

Operación	Mandato de ejemplo
Realizar una copia de seguridad de la base de datos.	Cree una planificación para ejecutar el mandato **BACKUP DB**. Si está configurando un sistema pequeño, establezca el parámetro **COMPRESS** en YES. Por ejemplo, en un sistema pequeño, emita el mandato siguiente para crear una planificación de copia de seguridad que utiliza la nueva clase de dispositivo: `define schedule DBBACKUP type=admin cmd="backup db devclass=dbback_filedev type=full numstreams=3 wait=yes compress=yes" active=yes desc="Back up the database." startdate=today starttime=11:00:00 duration=45 durunits=minutes`
Realice una copia de seguridad de la información de configuración del dispositivo.	Cree una planificación para ejecutar el mandato **BACKUP DEVCONFIG**: `define schedule DEVCONFIGBKUP type=admin cmd="backup devconfig filenames=devconfig.dat" active=yes desc="Backup the device configuration file." startdate=today starttime=17:00:00 duration=45 durunits=minutes`
Haga una copia de seguridad del historial de volumen.	Cree una planificación para ejecutar el mandato **BACKUP VOLHISTORY**: `define schedule VOLHISTBKUP type=admin cmd="backup volhistory filenames=volhist.dat" active=yes desc="Back up the volume history." startdate=today starttime=17:00:00 duration=45 durunits=minutes`
Elimine versiones más antiguas de copias de seguridad de base de datos que ya no son necesarias.	Cree una planificación para ejecutar el mandato **DELETE VOLHISTORY**: `define schedule DELVOLHIST type=admin cmd="delete volhistory type=dbb todate=today-6 totime=now" active=yes desc="Remove old database backups." startdate=today starttime=20:00:00 duration=45 durunits=minutes`

Operación	Mandato de ejemplo
Elimine objetos que exceden su retención permitida.	Cree una planificación para ejecutar el mandato **EXPIRE INVENTORY**. Defina el parámetro **RESOURCE** en función del tamaño del sistema que va a configurar: • Sistemas pequeños: 10 • Sistemas medianos: 30 • Sistemas grandes: 40 Por ejemplo, en un sistema de tamaño mediano, emita el siguiente mandato para crear una planificación que se denomine EXPINVENTORY: `define schedule EXPINVENTORY type=admin cmd="expire inventory wait=yes resource=30 duration=120" active=yes desc="Remove expired objects." startdate=today starttime=12:00:00 duration=45 durunits=minutes`

Qué hacer a continuación

Después de crear planificaciones para las tareas de mantenimiento de servidor, puede verlas en el Centro de operaciones completando los pasos siguientes:

1. En la barra de menús de Centro de operaciones, pase el ratón por encima de **Servidores**.
2. Pulse **Mantenimiento**.

Referencia relacionada:

DEFINE SCHEDULE (Definir una planificación para un comando de administración)

Definición de planificaciones de cliente

Utilice el Centro de operaciones para crear planificaciones para operaciones de cliente.

Procedimiento

1. En la barra de menús del Centro de operaciones, pase el cursor por encima de **Clientes**.
2. Pulse **Planificaciones**.
3. Pulse **+Planificación**.
4. Complete los pasos en el asistente Crear planificación. Establezca que las planificaciones de copia de seguridad de cliente se inicien a las 22:00, basándose en las actividades de mantenimiento del servidor que ha planificado en “Definición de planificaciones para actividades de mantenimiento del servidor” en la página 61.

Capítulo 9. Instalación y configuración de clientes

Tras la configuración correcta del sistema servidor de IBM Spectrum Protect, instale y configure el software de cliente para empezar a realizar la copia de seguridad de los datos.

Procedimiento

Para instalar el cliente de archivado y copia de seguridad, siga las instrucciones de instalación para el sistema operativo.

- Instalación de los clientes de archivado y copia de seguridad de UNIX y Linux
- Instalación del cliente de archivado y copia de seguridad de Windows

Qué hacer a continuación

Registrar y asignar los clientes a planificaciones.

Registro y asignación de clientes a planificaciones

Añada y registre cliente mediante Centro de operaciones utilizando el asistente Añadir cliente.

Antes de empezar

Determine si el cliente requiere un ID de usuario administrativo con autorización de propietario de cliente en el nodo de cliente. Para determinar qué clientes requieren un ID de usuario administrativo, consulte nota técnica 7048963.

Restricción: Para algunos tipos de clientes, el nombre de nodo de cliente y el ID de usuario administrativo deben coincidir. No se pueden autenticar los clientes utilizando el método de autenticación Lightweight Directory Access Protocol que se ha introducido en V7.1.7. Para obtener detalles sobre este método de autenticación, lo que a veces se denomina modalidad integrada, consulte Autenticación de los usuarios mediante una base de datos Active Directory.

Procedimiento

Para registrar un cliente, realice una de las siguientes acciones.

- Si el cliente necesita un ID de usuario administrativo, registre el cliente mediante el mandato **REGISTER NODE** y especifique el parámetro **USERID**:

  ```
  register node nombre_nodo contraseña userid=nombre_nodo
  ```

  donde *nombre_nodo* especifica el nombre de nodo y *contraseña* especifica la contraseña del nodo. Si desea obtener más información al respecto, consulte el apartado Registrar un nodo.
- Si el cliente no requiere un ID de usuario administrativo, registre el cliente mediante el asistente Agregar cliente de Centro de operaciones. Realice los pasos siguientes:
  1. En la barra de menús de Centro de operaciones, pulse **Clientes**.
  2. En la tabla Clientes, pulse **+ Cliente**.
  3. Complete los pasos en el asistente Añadir cliente:

a. Especifique que los datos redundantes se puedan eliminar en el cliente y en el servidor. En el área de eliminación de duplicados de datos del lado del cliente, active la casilla de verificación **Habilitar**.
b. En la ventana Configuración, copie los valores de opción **TCPSERVERADDRESS**, **TCPPORT**, **NODENAME** y **DEDUPLICATION**.

   Consejo: Anote los valores de opción y guárdelos en un lugar seguro. Después de completar el registro de cliente e instalar el software en el nodo de cliente, utilice los valores para configurar el cliente.
c. Siga las instrucciones del asistente para especificar el dominio de políticas y un conjunto de opciones.
d. Defina cómo se mostrarán los riesgos para el cliente especificando el valor de en riesgo.
e. Pulse **Añadir cliente**.

Instalación del servicio de gestión de cliente

Instale el servicio de gestión de cliente para clientes de archivado y copia de seguridad que se ejecutan en los sistemas operativos Linux y Windows. El servicio de gestión de cliente recopila información de diagnóstico sobre clientes de archivado y copia de seguridad y deja la información disponible en el Centro de operaciones para la funcionalidad de supervisión básica.

Procedimiento

Instale el servicio de gestión de cliente en el mismo sistema que el cliente de archivado y copia de seguridad completando los pasos siguientes:

1. Obtenga el paquete de instalación para el servicio de gestión de cliente en el DVD del producto. Como alternativa, puede descargar el paquete de instalación para el servicio de gestión de cliente desde un sitio de descarga de IBM como IBM Passport Advantage® o IBM Fix Central. Busque un nombre de archivo que sea similar a *versión*-TIV-TSMCMS-*sistema_operativo*.bin.
2. Cree un directorio en el sistema cliente que desea gestionar y copie allí el paquete de instalación.
3. Extraiga el contenido del archivo del paquete de instalación.
4. Ejecute el archivo de proceso por lotes de instalación desde el directorio donde ha extraído los archivos de instalación y los archivos asociados. Este es el directorio que ha creado en el paso 2.
5. Para instalar el servicio de gestión de cliente, siga las instrucciones en el asistente del Gestor de instalación de IBM. Si el Gestor de instalación de IBM no está instalado en el sistema cliente, debe seleccionar el Gestor de instalación de IBM y los Servicios de gestión de cliente de IBM Spectrum Protect.

Tareas relacionadas:

Configuración del servicio de gestión clientes para instalaciones de cliente personalizadas

Verificación de que el servicio de gestión de clientes está instalado correctamente

Antes de utilizar el servicio de gestión de cliente para recopilar información de diagnóstico sobre un cliente de archivado y copia de seguridad, puede verificar que el servicio de gestión de cliente está instalado y configurado correctamente.

Procedimiento

En el sistema cliente, en la línea de mandatos, ejecute los mandatos siguientes para ver la configuración del servicio de gestión de clientes:

- En los sistemas cliente Linux, emita el mandato siguiente:

  dir_instalación_cliente/cms/bin/CmsConfig.sh list

  donde *dir_instalación_cliente* es el directorio donde está instalado el cliente de archivado y copia de seguridad. Por ejemplo, en el caso de la instalación de cliente predeterminada, ejecute el siguiente mandato:

  ```
  /opt/tivoli/tsm/cms/bin/CmsConfig.sh list
  ```

  La salida es similar al texto siguiente:

  ```
  Listado de la configuración de CMS

  server1.example.com:1500 NO_SSL HOSTNAME
  Capabilities: [LOG_QUERY]
      Opt Path: /opt/tivoli/tsm/client/ba/bin/dsm.sys

      Log File: /opt/tivoli/tsm/client/ba/bin/dsmerror.log
          en_US MM/dd/aaaa HH:mm:ss Windows-1252

      Log File: /opt/tivoli/tsm/client/ba/bin/dsmsched.log
          en_US MM/dd/aaaa HH:mm:ss Windows-1252
  ```

- En los sistemas cliente Windows, emita el mandato siguiente:

  dir_instalación_cliente\cms\bin\CmsConfig.bat list

  donde *dir_instalación_cliente* es el directorio donde está instalado el cliente de archivado y copia de seguridad. Por ejemplo, en el caso de la instalación de cliente predeterminada, ejecute el siguiente mandato:

  ```
  C:\"Archivos de programa"\Tivoli\TSM\cms\bin\CmsConfig.bat list
  ```

  La salida es similar al texto siguiente:

  ```
  Listado de la configuración de CMS

  server1.example.com:1500 NO_SSL HOSTNAME
  Capabilities: [LOG_QUERY]
      Opt Path: C:\Program Files\Tivoli\TSM\baclient\dsm.opt

      Log File: C:\Program Files\Tivoli\TSM\baclient\dsmerror.log
          en_US MM/dd/aaaa HH:mm:ss Windows-1252

      Log File: C:\Program Files\Tivoli\TSM\baclient\dsmsched.log
          en_US MM/dd/aaaa HH:mm:ss Windows-1252
  ```

Si el servicio de gestión de clientes se ha instalado y configurado correctamente, la salida visualiza la ubicación del archivo de registro de errores.
El texto de salida se extrae del siguiente archivo de configuración:

- En sistemas cliente de Linux:

  client_install_dir/cms/Liberty/usr/servers/cmsServer/client-configuration.xml

- En sistemas cliente de Windows:

client_install_dir\cms\Liberty\usr\servers\cmsServer\client-configuration.xml

Si la salida no contiene ninguna entrada, debe configurar el archivo `client-configuration.xml`. Para obtener instrucciones para configurar este archivo, consulte Configuración del servicio de gestión clientes para instalaciones de cliente personalizadas. Puede utilizar el mandato **CmsConfig verify** para comprobar que una definición de nodo se ha creado correctamente en el archivo `client-configuration.xml`.

Configuración de Centro de operaciones para utilizar el servicio de gestión de cliente

Si no ha utilizado la configuración predeterminada para el servicio de gestión de cliente, debe configurar Centro de operaciones para acceder al servicio de gestión de cliente.

Antes de empezar

Asegúrese de que el servicio de gestión de cliente está instalado y se ha iniciado en el sistema cliente. Verifique si se ha utilizado la configuración predeterminada. La configuración predeterminada no se utiliza si se cumple alguna de las condiciones siguientes:

- El servicio de gestión de cliente no utiliza el número de puerto predeterminado, 9028.
- Al cliente de archivado y copia de seguridad no se accede mediante la misma dirección IP que al sistema cliente donde está instalado el cliente de archivado y copia de seguridad. Por ejemplo, es posible que se utilice una dirección IP diferente en las situaciones siguientes:
  - El sistema tiene dos tarjetas de red. El cliente de archivado y copia de seguridad está configurado para comunicarse por una red, mientras que el servicio de gestión de cliente se comunica por la otra red.
  - El sistema cliente se ha configurado con el DHCP (Dynamic Host Configuration Protocol - Protocolo de configuración dinámica de host). Como resultado, se le asigna dinámicamente al sistema cliente una dirección IP, que se guarda en el servidor durante la operación de cliente de archivado y copia de seguridad anterior. Cuando se reinicia el sistema cliente, se le puede asignar una dirección IP diferente. Para asegurarse de que el Centro de operaciones puede encontrar siempre el sistema cliente, especifique un nombre de dominio completo.

Procedimiento

Para configurar Centro de operaciones para utilizar el servicio de gestión de cliente, complete los pasos siguientes:

1. En la página Clientes de Centro de operaciones, seleccione el cliente.
2. Pulse **Detalles** > **Propiedades**.
3. En el campo URL de diagnóstico remoto de la sección General, especifique la URL para el servicio de gestión de cliente en el sistema cliente. La dirección debe empezar con `https`. La tabla siguiente muestra ejemplos del URL de diagnóstico remoto.

Tipo de URL	Ejemplo
Con nombre de host de DNS y puerto predeterminado, 9028	`https://server.example.com`

Tipo de URL	Ejemplo
Con el nombre de host de DNS y puerto no predeterminado	`https://server.example.com:1599`
Con la dirección IP y puerto no predeterminado	`https://192.0.2.0:1599`

4. Pulse **Guardar**.

Qué hacer a continuación

Puede acceder a la información de diagnóstico de cliente, por ejemplo archivos de registro de cliente, desde el separador **Diagnóstico** del Centro de operaciones.

Capítulo 10. Finalización de la implementación

Después de configurar y ejecutar la solución IBM Spectrum Protect, pruebe las operaciones de copia de seguridad y configure la supervisión para asegurarse de que todo se ejecuta sin problemas.

Procedimiento

1. Pruebe las operaciones de copia de seguridad para verificar que los datos están protegidos del modo que esperaba.
   a. En la página Clientes del Centro de operaciones, seleccione los clientes de los que desea hacer copia de seguridad y pulse **Copia de seguridad**.
   b. En la página Servidores de Centro de operaciones, seleccione el servidor para el cual desea realizar la copia de seguridad de la base de datos. Pulse **Copia de seguridad** y siga las instrucciones de la ventana Copia de seguridad de la base de datos del servidor.
   c. Verifique que las copias de seguridad se han completado correctamente si ningún mensaje de aviso o error.
2. Configure la supervisión de la solución siguiendo las instrucciones de Parte 3, “Supervisión de una solución de disco de sitio único”, en la página 73.

Parte 3. Supervisión de una solución de disco de sitio único

Después de implementar una solución de disco en un único sitio con IBM Spectrum Protect, supervise la solución para su funcionamiento correcto. Al supervisar la solución diariamente y de forma periódica, puede identificar problemas existentes y potenciales. La información que recopila se puede utilizar para resolver problemas y optimizar el rendimiento del sistema.

Acerca de esta tarea

El método preferido para supervisar una solución es utilizando Centro de operaciones, que proporciona el estado del sistema detallado y general en una interfaz gráfica de usuario. Además, puede configurar el Centro de operaciones para generar un informe de correo electrónico diario que resume el estado del sistema.

En algunos casos, es posible que desee utilizar herramientas de supervisión avanzadas para completar tareas de supervisión o resolución de problemas específicas.

Consejo: Si piensa diagnosticar problemas con clientes de archivado y copia de seguridad en sistemas operativos Linux o Windows, instale los servicios de gestión de cliente de IBM Spectrum Protect en cada sistema donde esté instalado un cliente de archivado y copia de seguridad. De esta forma, puede garantizar que el botón **Diagnosticar** está disponible en Centro de operaciones para diagnosticar problemas con los clientes de archivado y copia de seguridad. Para instalar el servicio de gestión de cliente, siga las instrucciones en Instalación del servicio de gestión de cliente.

Procedimiento

1. Complete las tareas de supervisión diariamente. Para obtener instrucciones, consulte Lista de comprobación diaria.
2. Complete las tareas de supervisión periódicamente. Para obtener instrucciones, consulte Lista de comprobación periódica.
3. Para verificar que la solución de IBM Spectrum Protect cumple con los requisitos de licencia, siga las instrucciones en Verificación de la conformidad de licencia.
4. Si desea configurar el Centro de operaciones para generar informes de estado de correo electrónico, consulte Seguimiento del estado del sistema mediante informes de correo electrónico

Qué hacer a continuación

Resuelva cualquier problema que encuentre. Para resolver un problema cambiando la configuración de la solución, siga las instrucciones en Parte 4, “Gestión de operaciones”, en la página 93. Los siguientes recursos están también disponibles:

- Para resolver problemas de rendimiento, consulte Rendimiento.
- Para resolver otros tipos de problemas, consulte Resolución de problemas.

Capítulo 11. Lista de comprobación de supervisión diaria

Para asegurarse de que está completando las tareas de supervisión diarias para la solución IBM Spectrum Protect, revise la lista de comprobación de supervisión diaria.

Complete las tareas de supervisión diariamente desde la página Centro de operaciones Descripción general. Puede acceder a la página Descripción general abriendo Centro de operaciones y pulsando **Descripciones generales**.

La siguiente figura muestra la ubicación para completar cada una de las tareas.

Consejo: Para ejecutar mandatos administrativos para tareas de supervisión avanzadas, utilice el creador de mandatos de Centro de operaciones. El creador de mandatos proporciona una función anticipada para guiarle cuando entra mandatos. Para abrir el creador de mandatos, vaya a la página Centro de operaciones Descripción general. En la barra de menús, pase el ratón sobre el icono de configuración y pulse **Creador de mandatos**.

La tabla siguiente lista las tareas de supervisión diarias y proporciona instrucciones para completar cada tarea.

Tabla 15. Tareas de supervisión diarias

Tarea	Procedimientos básicos	Procedimientos avanzados e información sobre solución de problemas
1 Determine si los clientes corren riesgo de estar desprotegidos debido a operaciones de seguridad que han fallado o que se han perdido.	Para verificar si los clientes están en riesgo, en el área Clientes, busque una notificación **En riesgo**. Para ver detalles, pulse el área Clientes. Si ha instalado el servicio de gestión de cliente en un cliente de archivado y copia de seguridad, puede ver y analizar los registros de planificación y errores de cliente completando los pasos siguientes: 1. En la tabla Clientes, seleccione el cliente y pulse **Detalles** . 2. Para diagnosticar un problema, pulse **Diagnóstico**.	Para clientes que no tienen instalado el servicio de gestión de cliente, acceda al sistema de cliente para revisar los registros de error de cliente.
2 Determine si los errores relacionados con el cliente o relacionados con el servidor requieren atención.	Para determinar la gravedad de cualquier alerta notificada, en el área Alertas, pase el ratón por encima de las columnas.	Para ver información adicional sobre alertas, complete los pasos siguientes: 1. Pulse el área Alertas. 2. En la tabla Alertas, seleccione una alerta. 3. En el panel Registro de actividad, revise los mensajes. El panel muestra mensajes relaciones que se han emitido antes y después de que se produjera la alerta seleccionada.
3 Determine si los servidores gestionados por Centro de operaciones están disponibles para proporcionar servicios de protección de datos a los clientes.	1. Para verificar si los clientes están en riesgo, en el área Servicios, busque una notificación **No disponible**. 2. Para ver información adicional, pulse el área Servidores. 3. Seleccione un servidor en la tabla Servidores y pulse **Detalles**.	**Consejo:** Si detecta un problema relacionado con las propiedades de servidor, actualice las propiedades de servidor: 1. En la tabla Servidores, seleccione un servidor y pulse **Detalles**. 2. Para actualizar las propiedades de servidor, pulse **Propiedades**.

Tabla 15. Tareas de supervisión diarias (continuación)

Tarea	Procedimientos básicos	Procedimientos avanzados e información sobre solución de problemas
4 Determine si hay suficiente espacio disponible para el inventario del servidor, que consta de la base de datos del servidor, del registro activo y del registro de archivado.	1. Pulse el área Servidores. 2. En la columna Estado de la tabla, consulte el estado del servidor y resuelva los problemas que puedan surgir: • **Normal** Hay suficiente espacio para la base de datos de servidor, el registro activo y el registro de archivado. • **Crítico** No hay suficiente espacio para la base de datos de servidor, el registro activo o el registro de archivado. Debe añadir espacio inmediatamente o se interrumpirán los servicios de protección de datos proporcionados por el servidor. • **Aviso** La base de datos de servidor, el registro activo o el registro de archivado se están quedando sin espacio. Si esta condición persiste, deberá añadir espacio. • **No disponible** No se puede obtener el estado. Asegúrese de que el servidor se está ejecutando y de que no hay problemas de red. Este estado se muestra también si el ID de administrador de supervisión está bloqueado o,por el contrario, no disponible en el servidor. Este ID se llama nombre_nombre_concentrador _IBM-OC. • **No supervisado** Los servidores no supervisados se definen para el servidor hub, pero no están configurados para la gestión por parte de Centro de operaciones. Para configurar un servidor sin supervisar, selecciónelo, y pulse **Supervisar servidor de radio**.	También puede buscar alertas relacionadas en la página Alertas. Para obtener instrucciones adicionales sobre la resolución de problemas, consulte Resolución de problemas de servidor.

Tabla 15. Tareas de supervisión diarias (continuación)

Tarea	Procedimientos básicos	Procedimientos avanzados e información sobre solución de problemas
5 Verifique las operaciones de seguridad de la base de datos del servidor.	Para determinar la última vez que se hizo copia de seguridad del servidor, complete los pasos siguientes: 1. Pulse el área Servidores. 2. En la tabla Servidores, revise la columna Última copia de seguridad de base de datos.	Para obtener información más detallada sobre operaciones de copia de seguridad, complete los pasos siguientes: 1. En la tabla Servidores, seleccione una fila y pulse **Detalles**. 2. En el área de copia de seguridad de base de datos, pase el ratón por encima de las marcas de selección para revisar la información sobre las operaciones de copia de seguridad. Si no se ha hecho copia de seguridad de la base de datos recientemente (por ejemplo, en las últimas 24 horas), puede iniciar una operación de seguridad: 1. En la página Centro de operaciones Descripción general, pulse el área Servidores. 2. En la tabla, seleccione un servidor y pulse **Hacer copia de seguridad**. Para determinar si la base de datos del servidor se ha configurado para operaciones de copia de seguridad automáticas, realice los siguientes pasos: 1. En la barra de menús, pase el ratón sobre el icono de configuración y pulse **Creador de mandatos**. 2. Emita el mandato **QUERY DB**: `query db f=d` 3. En la salida, revise el campo `Nombre de clase de dispositivo completo`. Si se especifica una clase de dispositivo, el servidor se configura para copias de seguridad de base de datos automáticas.
6 Supervise otras tareas de mantenimiento del servidor. Las tareas de mantenimiento del servidor pueden incluir planificaciones de mandatos administrativos en ejecución, scripts de mantenimiento y mandatos relacionados.	Para buscar información sobre los procesos que han fallado debido a problemas de servidor, complete los pasos siguientes: 1. Pulse **Servidores** > **Mantenimiento**. 2. Para obtener el historial de dos semanas de un proceso, visualice la columna Historial. 3. Para obtener más información sobre un proceso planificado, pase el ratón por encima de la casilla de verificación asociada al proceso.	Para obtener información sobre la supervisión de procesos y la resolución de problemas, consulte la ayuda en línea de Centro de operaciones.

Tabla 15. Tareas de supervisión diarias (continuación)

Tarea	Procedimientos básicos	Procedimientos avanzados e información sobre solución de problemas
7 Verifique que la cantidad de datos que se ha enviado recientemente a y desde los servidores está dentro del rango esperado.	• Para obtener una descripción general de una actividad en las últimas 24 horas, vea el área Actividad. • Para comparar la actividad en las últimas 24 horas con la actividad de las últimas 24 horas, revise las cifras en las áreas Actuales y Anteriores.	• Si se han enviado más datos al servidor de los que esperaba, determine qué clientes están haciendo copia de seguridad de más datos e investigue la causa. Es posible que la deduplicación de datos del lado del clientes no esté funcionando correctamente. • Si se han enviado al servidor menos datos de los que esperaba, investigue si las operaciones de seguridad del cliente están procediendo tal como estaba planificado.
8 Verifique que las agrupaciones de almacenamiento están disponibles para hacer copia de seguridad de los datos de cliente.	1. Si se indican problemas en el área Almacenamiento & Disponibilidad de datos, pulse **Agrupaciones** para ver los detalles: • Si se visualiza un estado **Crítico** ⊗, se muestra el estado, no hay suficiente espacio disponible en la agrupación de almacenamiento o el estado de acceso no está disponible. • Si se visualiza un estado de **Aviso** ⚠, se muestra el estado, la agrupación de almacenamiento se está quedando sin espacio o su estado de acceso es de solo lectura. 2. Para ver el espacio utilizado, libre y total para la agrupación de almacenamiento seleccionada, pase el cursor por encima de las entradas de la columna Capacidad utilizada.	Para ver la capacidad de la agrupación de almacenamiento que se ha utilizado en las dos últimas semanas, seleccione una fila en la tabla Agrupaciones de almacenamiento y pulse **Detalles**.

Tabla 15. Tareas de supervisión diarias (continuación)

Tarea	Procedimientos básicos	Procedimientos avanzados e información sobre solución de problemas
9 Verifique que los dispositivos de almacenamiento están disponibles para operaciones de seguridad.	En el área Almacenamiento & Disponibilidad de datos, en la sección Volúmenes, en las barras de capacidad, revise el estado del que se ha informado junto a los **Dispositivos**. Si se visualiza un estado **Crítico** o **Aviso** El estado se muestra para cualquier dispositivo, investigue el problema. Para ver detalles, pulse **Dispositivos**.	Los dispositivos de disco pueden tener un estado crítico o de aviso por los siguientes motivos: • En las clases de dispositivo DISK, es posible que los volúmenes estén fuera de línea o tengan un estado de acceso de solo lectura. La columna Almacenamiento de disco de la tabla Dispositivos de disco muestra el estado de los volúmenes. • En las clases de dispositivo FILE no compartidas, es posible que los directorios estén fuera de línea. Además, puede que no haya suficiente espacio libre disponible para asignar volúmenes reutilizables. La columna Almacenamiento de disco de la tabla Dispositivos de disco muestra el estado de los directorios. • Para las clases de dispositivos FILE que se comparten, es posible que las unidades no estén disponibles. Una unidad no estará disponible si está fuera de línea, si deja de responder al servidor, o si su vía de acceso está fuera de línea. Otras columnas de la tabla Dispositivos de disco muestran el estado de las unidades y de las vías de acceso.

Capítulo 12. Lista de comprobación de supervisión periódica

Para asegurarse de que la solución IBM Spectrum Protect opera correctamente, complete las tareas de la lista de comprobación de supervisión periódica. Planifique las tareas periódicas con la suficiente frecuencia para que pueda detectar problemas potenciales antes de que se conviertan en problemáticos.

Consejo: Para ejecutar mandatos administrativos para tareas de supervisión avanzadas, utilice el creador de mandatos de Centro de operaciones. El creador de mandatos proporciona una función anticipada para guiarle cuando entra mandatos. Para abrir el creador de mandatos, vaya a la página Centro de operaciones Descripción general. En la barra de menús, pase el ratón sobre el icono de configuración  y pulse **Creador de mandatos**.

Tabla 16. Tareas de supervisión periódicas

Tarea	Procedimientos básicos	Procedimientos avanzados y solución de problemas
Supervise el rendimiento del sistema.	Determine la longitud de tiempo necesaria para las operaciones de copia de seguridad de cliente: 1. En la página de Centro de operaciones Visión general, pulse **Clientes**. Busque el servidor asociado al cliente. 2. Pulse **Servidores**. Seleccione el servidor y pulse **Detalles**. 3. Para ver la duración de las tareas completadas en las últimas 24 hora, pulse **Tareas completadas**. 4. Para ver la duración de las tareas completadas hace más de 24 horas, utilice el mandato **QUERY ACTLOG**. Siga las instrucciones en QUERY ACTLOG (Consultar las anotaciones de actividades). 5. Si la duración de las operaciones de copia de seguridad de cliente está aumentando y los motivos no está claros, investigue la causa. Si ha instalado el servicio de gestión de cliente en un cliente de archivado y copia de seguridad, puede diagnosticar problemas de rendimiento para el cliente de archivado y copia de seguridad completando los pasos siguientes: 1. En la página de Centro de operaciones Visión general, pulse **Clientes**. 2. Seleccione un cliente de archivado y copia de seguridad y pulse **Detalles**. 3. Para recuperar registros de cliente, pulse **Diagnóstico**.	Para obtener instrucciones sobre la reducción del tiempo que tarda el cliente en hacer copia de seguridad de los datos en el servidor, consulte Resolución de problemas de rendimiento comunes del cliente. Busque cuellos de botella de rendimiento. Para ver instrucciones, consulte Identificación de cuellos de botella de rendimiento. Para obtener información sobre la identificación y resolución de otros problemas de rendimiento, consulte Rendimiento.

Tabla 16. Tareas de supervisión periódicas (continuación)

Tarea	Procedimientos básicos	Procedimientos avanzados y solución de problemas
Determine el ahorro de disco proporcionado por la deduplicación de datos.	1. En la página Centro de operaciones Descripción general, pulse **Agrupaciones**. 2. Seleccione una agrupación y pulse **Vista rápida**. 3. En el área Optimización de almacenamiento de datos, vea la fila Espacio guardado.	En la supervisión avanzada, para obtener estadísticas detalladas sobre el proceso de deduplicación de datos para una agrupación de almacenamiento de contenedores de directorio o agrupación de almacenamiento de contenedores de nube específica, complete los siguientes pasos: 1. En la página Descripción general de Centro de operaciones, pase el ratón sobre el icono de configuración y pulse **Creador de mandatos**. 2. Obtenga un informe estadístico emitiendo el mandato **GENERATE DEDUPSTATS**. Siga las instrucciones en GENERATE DEDUPSTATS (Generar estadísticas de deduplicación de datos respecto a una agrupación de almacenamiento de contenedores de directorio). 3. Vea el informe estadístico emitiendo el mandato **QUERY DEDUPSTATS**. Siga las instrucciones de QUERY DEDUPSTATS (Consultar las estadísticas de deduplicación de datos).

Tabla 16. Tareas de supervisión periódicas (continuación)

Tarea	Procedimientos básicos	Procedimientos avanzados y solución de problemas

Verifique que se han guardado los archivos de copia de seguridad actuales para la configuración del dispositivo y la información del historial de volumen.	Acceda a las ubicaciones de almacenamiento para asegurarse de que hay archivos disponibles. El método preferido es guardar los archivos de copia de seguridad en dos ubicaciones.
	
	Para ubicar los archivos de historial de volumen y de configuración de dispositivo, complete los pasos siguientes:
	1. En la página Descripción general de Centro de operaciones, pase el ratón sobre el icono de configuración y pulse **Creador de mandatos**.
	2. Para ubicar los archivos de historial de volumen y de configuración de dispositivo, emita los siguientes mandatos:
	`query option volhistory`
	`query option devconfig`
	3. En la salida, revise la columna Valor de opción para encontrar las ubicaciones de archivo.
	
	Si se produce un desastre, se necesita el archivo de historial de volumen y el archivo de configuración de dispositivo para restaurar la base de datos del servidor.	

Tabla 16. Tareas de supervisión periódicas (continuación)

Tarea	Procedimientos básicos	Procedimientos avanzados y solución de problemas

Determine si está disponible espacio suficiente para el sistema de archivos del directorio de la instancia.	Verifique que al menos el 20% de espacio libre está disponible en el sistema de archivos del directorio de instancia. Realice la acción adecuada para el sistema operativo:
	• AIX Para ver el espacio disponible en el sistema de archivos, en la línea de mandatos del sistema operativo emita el siguiente mandato:
	`df -g instance_directory`
	donde *instance_directory* especifica el directorio de instancia.
	• Linux Para ver el espacio disponible en el sistema de archivos, en la línea de mandatos del sistema operativo emita el siguiente mandato:
	`df -h instance_directory`
	donde *instance_directory* especifica el directorio de instancia.
	• Windows En el programa Windows Explorer, pulse el botón derecho del ratón en el sistema de archivos y, después, **Propiedades**. Vea la información de capacidad.
	La ubicación preferida del directorio de instancia depende del sistema operativo donde está instalado el servidor:
	• AIX Linux `/home/tsminst1/tsminst1`
	• Windows `C:\tsminst1`
	Consejo: Si ha completado una hora de trabajo de planificación, la ubicación del directorio de instancia se registra en la hoja de trabajo.	

Tabla 16. Tareas de supervisión periódicas (continuación)

Tarea	Procedimientos básicos	Procedimientos avanzados y solución de problemas
Identifique la actividad de cliente inesperada.	Para supervisar la actividad de cliente para determinar si los volúmenes de datos superan la cantidad esperada, complete los pasos siguientes: 1. En la página Centro de operaciones Descripción general, pulse el área Clientes. 2. Para ver la actividad durante las dos últimas semanas, efectúe una doble pulsación en cualquier cliente. 3. Para ver el número de bytes enviados al cliente, pulse la pestaña **Propiedades**. 4. En el área Última sesión, visualice la fila Enviado a cliente.	Cuando efectúe doble pulsación en un cliente en la tabla Clientes, el área Actividad durante dos semanas muestra la cantidad de datos que el cliente ha enviado al servidor cada día.

Tabla 16. Tareas de supervisión periódicas (continuación)

Tarea	Procedimientos básicos	Procedimientos avanzados y solución de problemas
Supervise el crecimiento de la agrupación de almacenamiento a lo largo del tiempo.	1. En la página Centro de operaciones Descripción general, pulse el área Agrupaciones. 2. Para ver la capacidad utilizada durante las dos últimas semanas, seleccione una agrupación y pulse **Detalles**.	**Sugerencias:** • Para especificar el periodo de tiempo que debe transcurrir antes de que se eliminen todas las extensiones deduplicadas de una agrupación de almacenamiento de contenedor de directorios o de la agrupación de almacenamiento del contenedor de nube, después de que el inventario haya dejado de hacer referencia a las mismas, siga estos pasos: 1. En la página **Agrupaciones de almacenamiento** del Centro de operaciones, seleccione la agrupación de almacenamiento. 2. Pulse **Detalles** > **Propiedades**. 3. Especifique la duración en el campo `Período de retardo para la reutilización del contenedor`. • Para determinar el rendimiento de deduplicación de datos para las agrupaciones de almacenamiento del contenedor de la nube y del contenedor del directorio, utilice el mandato **`GENERATE DEDUPSTATS`**. • Para ver las estadísticas de deduplicación de datos para una agrupación de almacenamiento, siga estos pasos: 1. En la página **Agrupaciones de almacenamiento** del Centro de operaciones, seleccione la agrupación de almacenamiento. 2. Pulse **Detalles** > **Propiedades**. De forma alternativa, utilice el mandato **`QUERY EXTENTUPDATES`** para visualizar información sobre las actualizaciones en las extensiones de datos en agrupaciones de almacenamiento de contenedores de directorio o contenedores de nube. La salida del mandato puede ayudarle a determinar qué extensiones de datos ya no están referenciadas y cuáles son elegibles para suprimirse del sistema. En la salida, supervise el número de extensiones de datos elegibles para suprimirse del sistema. Esta métrica tiene una correlación directa con la cantidad de espacio libre que estará disponible dentro de la agrupación de almacenamiento de contenedores. • Para mostrar la cantidad de espacio físico ocupado por un espacio de archivos tras la eliminación del ahorro de deduplicación de datos, utilice el mandato **`select * from occupancy`**. La salida del mandato incluye el valor LOGICAL_MB. LOGICAL_MB es la cantidad de espacio utilizado por el espacio de archivos.

Tabla 16. Tareas de supervisión periódicas (continuación)

Tarea	Procedimientos básicos	Procedimientos avanzados y solución de problemas
Evalúe la temporización de las planificaciones de cliente. Asegúrese de que las horas de inicio y finalización de las planificaciones de cliente cumplen las necesidades de negocio.	En la página Centro de operaciones Descripción general, pulse **Clientes** > **Planificaciones**. En la tabla Planificaciones, la columna Inicio muestra la hora de inicio configurada para la operación planificada. Para ver cuándo se ha iniciado la operación más reciente, pase el ratón por encima del icono de reloj.	**Consejo:** Puede recibir un mensaje de aviso si una operación de cliente ejecutan más tiempo de lo esperado. Realice los pasos siguientes: 1. En la página Descripción general de Centro de operaciones, pase el ratón por encima de **Clientes** y pulse **Planificaciones**. 2. Seleccione una planificación y pulse **Detalles**. 3. Vea los detalles de una planificación pulsando la flecha azul al lado de la fila. 4. En el campo **Ejecutar alerta de hora**, especifique la hora a la que se emitirá un mensaje de aviso si la operación planificada no se ha completado. 5. Pulse **Guardar**.
Evalúe la temporización de las tareas de mantenimiento. Asegúrese de que las horas de inicio y finalización de las tareas de mantenimiento cumplen las necesidades de negocio.	En la página Centro de operaciones Descripción general, pulse **Servidores** > **Mantenimiento**. En la tabla Mantenimiento, revise la información en la columna Hora de la última ejecución. Para ver cuándo se ha iniciado la última tarea de mantenimiento, pase el ratón por encima del icono de reloj.	**Consejo:** Si una tarea de mantenimiento está en ejecución demasiado tiempo, cambie la hora de inicio o el tiempo de ejecución máximo. Realice los pasos siguientes: 1. En la página Descripción general de Centro de operaciones, pase el ratón sobre el icono de configuración y pulse **Creador de mandatos**. 2. Para cambiar la hora de inicio o el tiempo de ejecución máximo de una tarea, emita el mandato **`UPDATE SCHEDULE`**. Para obtener instrucciones, consulte UPDATE SCHEDULE (Actualizar una planificación de cliente).

Referencia relacionada:

- QUERY ACTLOG (Consultar las anotaciones de actividades)
- UPDATE STGPOOL (Actualizar una agrupación de almacenamiento)
- QUERY EXTENTUPDATES (Consultar extensiones de datos actualizadas)

Capítulo 13. Verificación de la conformidad de licencia

Verifique que la solución de IBM Spectrum Protect cumple con las provisiones del acuerdo de licencia. Verificando la conformidad regularmente, puede realizar seguimiento a las tendencias en el crecimiento de datos o el uso de value unit de procesador (PVU). Utilice esta información para planificar una compra de licencia futura.

Acerca de esta tarea

El método para verificar la conformidad de licencia varía dependiendo de las provisiones del acuerdo de licencia de IBM Spectrum Protect:

Licencia de capacidad frontal
El modelo frontal determina los requisitos de licencia basados en la cantidad de datos primarios de los que se informa que los clientes están haciendo copia de seguridad. Los clientes incluyen aplicaciones, máquinas virtuales y sistemas.

Licencia de capacidad de programa de fondo
El modelo de programa de fondo determina los requisitos de licencia basándose en los terabytes de datos que se almacenan en las agrupaciones de almacenamiento primarias y los repositorios.

Sugerencias:

- Para garantizar la precisión de las estimaciones de capacidad frontal y de programa de fondo, instale la última versión del software de cliente en cada nodo de cliente.
- La información sobre la capacidad frontal y de fondo en el Centro de operaciones es para fines de planificación y estimación.

Licencia de PVU
El modelo de PVU se basa en el uso de PVU por parte de los dispositivos de servidor.

Importante: Los cálculos de PVU que proporciona IBM Spectrum Protect se consideran estimaciones y no son jurídicamente vinculantes. La información de licencias de PVU proporcionada por IBM Spectrum Protect no se considera un sustituto aceptable de IBM License Metric Tool.

Para ver la última información sobre los modelos de licencia , consulte la información sobre cómo comparar paquetes en Sitio web de la familia de productos IBM Spectrum Protect. Si tiene preguntas o dudas sobre los requisitos de licencia, póngase en contacto con el proveedor de software de IBM Spectrum Protect.

Procedimiento

Para supervisar la conformidad de licencia, complete los pasos que corresponden a las provisiones del acuerdo de licencia.

Consejo: El Centro de operaciones proporciona un informe de correo electrónico que resume el uso de capacidad frontal y de fondo. Pueden enviarse informes

automáticamente a uno o más destinatarios de forma regular. Para configurar y gestionar informes de correo electrónico, pulse **Informes** en la barra de menús del Centro de operaciones.

Opción	Descripción
Modelo frontal	1. En la barra de menús de Centro de operaciones, pase el ratón sobre el icono de configuración y pulse **Licencias**. La estimación de capacidad frontal se visualiza en la página Uso frontal. 2. Si se visualiza un valor en la columna Sin informes, pulse el número para identificar clientes que no han informado del uso de capacidad. 3. Para calcular la capacidad para clientes que no han informado del uso de capacidad, vaya al siguiente sitio FTP, que proporciona instrucciones y herramientas de medidas: ftp://public.dhe.ibm.com/storage/tivoli-storage-management/front_end_capacity_measurement_tools Siga las instrucciones de la última guía de licencia disponible para medir la capacidad frontal mediante un script. 4. Añada la estimación de Centro de operaciones y las estimaciones obtenidas utilizando un script. 5. Verifique que la capacidad estimada cumple con el acuerdo de licencia.
Modelo suplementario	**Restricción:** No puede utilizar el Centro de operaciones para supervisar el uso de capacidad de fondo de los clientes replicados si los servidores de réplica de origen y destino no utilizan los mismos valores de política. Para obtener información sobre cómo estimar el uso de capacidad de estos clientes, consulte nota técnica 1656476. 1. En la barra de menús de Centro de operaciones, pase el ratón sobre el icono de configuración y pulse **Licencias**. 2. Pulse la pestaña **Suplementario**. 3. Verifique que la cantidad de datos estimada cumple con el acuerdo de licencia.
Modelo de PVU	Siga las instrucciones en Evaluación de la conformidad con el modelo de licencias de PVU.

Capítulo 14. Seguimiento del estado del sistema mediante informes de correo electrónico

Configure el Centro de operaciones para generar informes de correo electrónico que resuman el estado del sistema. Puede configurar una conexión con el servidor de correo, cambiar valores de informe y, opcionalmente, crear informes SQL personalizados.

Antes de empezar

Antes de configurar los informes de correo electrónico, asegúrese de que se cumplen los siguientes requisitos:

- Un servidor de host del protocolo simple de transferencia de correo (SMTP) está disponible para enviar y recibir informes por correo electrónico. El servidor de SMTP debe configurarse como un relé de correo abierto. También debe asegurarse de que el servidor IBM Spectrum Protect que envía mensajes de correo electrónico tiene acceso al servidor SMTP. Si el Centro de operaciones está instalado en un sistema independiente, el sistema no requiere acceso al servidor SMTP.
- Para configurar los informes de correo electrónico, debe tener el privilegio de sistema para el servidor.
- Para especificar los destinatarios, puede entrar una o más direcciones de correo electrónico o ID de administrador. Si planea entrar un ID de administrador, el ID debe estar registrado en el servidor hub y debe tener una dirección de correo electrónico asociada con él. Para especificar una dirección de correo electrónico para un administrador, utilice el parámetro **EMAILADDRESS** del mandato **UPDATE ADMIN**.

Acerca de esta tarea

Puede configurar el Centro de operaciones para enviar un informe de operaciones general, un informe de verificación de licencia y uno o más informes personalizados, todos los cuales utilizarán sentencia SELECT SQL para consultar servidores gestionados.

Consejo: El informe de operaciones general incluye un archivo adjunto. Para obtener información más detallada, expanda las secciones del archivo adjunto.

Procedimiento

Para configurar y gestionar los informes de correo electrónico, complete los pasos siguientes:

1. En la barra de menús del Centro de operaciones, pulse **Informes**.
2. Si aún no se ha configurado ninguna conexión con el servidor de correo electrónico, pulse **Configurar servidor de correo** y complete los campos. Después de configurar el servidor de correo, se habilitan el informe de operaciones general y el informe de verificación de licencia.
3. Para cambiar los valores de un informe, seleccione dicho informe, pulse **Detalles** y actualice el formulario.
4. Opcional: Para añadir un informe SQL personalizado, pulse **+ Informe** y complete los campos.

Consejo: Para ejecutar un informe y enviarlo de inmediato, seleccione el informe y pulse **Enviar**.

Resultados

Se envían los informes habilitados, de acuerdo con los valores especificados.

Si no puede ver la imagen de un informe, puede que esté utilizando un cliente de correo electrónico que convierte HTML a otro formato. Para obtener información sobre las restricciones, consulte la ayuda en línea Centro de operaciones.

Referencia relacionada:

UPDATE ADMIN (Actualizar un administrador)

Parte 4. Gestión de operaciones

Utilice esta información para gestionar operaciones para una solución de disco de sitio único con IBM Spectrum Protect que incluya un servidor y utilice la eliminación de datos duplicados para una única ubicación.

Capítulo 15. Gestión del Centro de operaciones

El Centro de operaciones ofrece acceso web y a móvil a la información de estado sobre el entorno de IBM Spectrum Protect. Puede utilizar Centro de operaciones para supervisar varios servidores y para completar algunas tareas administrativas. Centro de operaciones también proporciona acceso web a la línea de mandatos de IBM Spectrum Protect.

Adición y eliminación de servidores spoke

En un entorno de varios servidores, puede conectarse a los demás servidores, llamados *servidores spoke*, al servidor hub.

Acerca de esta tarea

Los servidores spoke envían alertas e información de estado al servidor hub. El Centro de operaciones le muestra una vista consolidada de alertas e información de estado para el servidor hub y los servidores spoke.

Adición de un servidor de radio

Después de configurar el servidor concentrador para Centro de operaciones, puede añadir uno o más servidores de radio al servidor concentrador.

Antes de empezar

Cuando se instala el servidor de IBM Spectrum Protect, la configuración predeterminada requiere la comunicación segura utilizando el protocolo Secure Sockets Layer (SSL) o Transport Layer Security (TLS). A menos que este requisito se haya inhabilitado para los servidores de concentrador y de radio, debe añadir el certificado del servidor de radio al archivo de almacén de confianza del servidor concentrador.

Procedimiento

1. En la barra de menús de Centro de operaciones, pulse **Servidores**. Se abre la página Servidores.

   En la tabla de la página Servidores, un servidor puede tener un estado de "No supervisado." Este estado significa que aunque un administrador haya definido este servidor al servidor concentrador utilizando el mandato **DEFINE SERVER**, el servidor todavía no está configurado como un servidor de radio.
2. Realice uno de los siguientes pasos:
   - Seleccione el servidor para resaltarlo, y en la tabla de la barra del menú, pulse **Supervisar radio**.
   - Si el servidor que desea añadir no se muestra en la tabla, y no es necesaria la comunicación segura SSL/TLS, pulse **+ Servidor de radio** en la barra de menús de la tabla.
3. Proporcione la información necesaria y complete los pasos del asistente de configuración del servidor de radio.

   Consejo: Si el periodo de retención del registro de sucesos del servidor es inferior a 14 días, el periodo se restablece automáticamente a 14 días, si configura el servidor como un servidor de radio.

Eliminación de un servidor spoke

Puede eliminar un servidor spoke del Centro de operaciones.

Acerca de esta tarea

Tal vez sea conveniente eliminar un servidor de radio en las situaciones siguientes, por ejemplo:

- Desea mover el servidor spoke de un servidor concentrador a otro servidor concentrador.
- Desea que el servidor spoke quede fuera de servicio.

Procedimiento

Para eliminar el servidor spoke del grupo de servidores que gestiona el servidor concentrador, realice los pasos siguientes:

1. Desde la línea de mandatos de IBM Spectrum Protect, emita el mandato siguiente en el servidor concentrador:

   ```
   QUERY MONITORSETTINGS
   ```

2. En la salida del mandato, copie el nombre incluido en el campo **Grupo supervisado**.
3. Emita el mandato siguiente en el servidor concentrador, donde *nombre_grupo* representa el nombre del grupo supervisado y *nombre_miembro* representa el nombre del servidor spoke:

   ```
   DELETE GRPMEMBER nombre_grupo nombre_miembro
   ```

4. Opcional: Si desea mover el servidor de radio de un servidor concentrador a otro servidor concentrador, **no** lleve a cabo este paso. De lo contrario, puede inhabilitar las alertas y la supervisión en el servidor spoke emitiendo los mandatos siguientes en el servidor spoke:

   ```
   SET STATUSMONITOR OFF
   SET ALERTMONITOR OFF
   ```

5. Opcional: Si la definición del servidor de radio se utiliza para otros fines, como por ejemplo, la configuración empresarial, el direccionamiento de mandatos, el almacenamiento de volúmenes virtuales o la gestión de bibliotecas, **no** lleve a cabo este paso. De lo contrario, puede suprimir la definición del servidor spoke en el servidor concentrador emitiendo el mandato siguiente en el servidor concentrador:

   ```
   DELETE SERVER nombre_servidor_spoke
   ```

Inicio y detención del servidor web

El servidor web de Centro de operaciones se ejecuta como un servicio y se inicia automáticamente. Es posible que tenga que detener e iniciar el servidor web, por ejemplo, para realizar cambios de configuración.

Procedimiento

1. Detener el servidor web.
   - AIX Desde el directorio */installation_dir*/ui/utils, donde *installation_dir* representa el directorio donde está instalado Centro de operaciones, emita los siguientes mandatos:

     ```
     ./stopserver.sh
     ```

   - Linux Emita el mandato siguiente:

     ```
     service opscenter.rc stop
     ```

- Windows En la ventana Servicios, detenga el servicio de **IBM Spectrum Protect Operations Center**.

2. Inicie el servidor web.
   - AIX Desde el directorio `/installation_dir/ui/utils`, donde *installation_dir* representa el directorio donde está instalado Centro de operaciones, emita los siguientes mandatos:

     ```
     ./startserver.sh
     ```

   - Linux Emita los comandos siguientes:

     Inicie el servidor:

     ```
     service opscenter.rc start
     ```

     Reinicie el servidor:

     ```
     service opscenter.rc restart
     ```

     Determine si el servidor se está ejecutando:

     ```
     service opscenter.rc status
     ```

   - Windows En la ventana Servicios, inicie el servicio **IBM Spectrum Protect Operations Center**.

Reinicio del asistente de configuración inicial

Es posible que tenga que reiniciar el asistente de configuración inicial de Centro de operaciones, por ejemplo, para hacer cambios de configuración.

Antes de empezar

Para cambiar los siguientes valores, utilice la página Valores de Centro de operaciones en lugar de reiniciar el asistente de configuración inicial:

- La frecuencia de actualización de los datos de estado
- El tiempo de duración que las alertas permanecen activas, inactivas o cerradas
- Las condiciones que indican que los clientes están en riesgo

La ayuda de Centro de operaciones incluye más información acerca de cómo cambiar estos valores.

Acerca de esta tarea

Para reiniciar el asistente de configuración inicial, debe suprimir un archivo de propiedades que incluye información acerca de la conexión del servidor concentrador. Sin embargo, no se eliminarán los valores de alerta, supervisión, en riesgo o multiservidor que se hayan configurado para el servidor concentrador. Estos valores se utilizan como valores predeterminados en el asistente de configuración cuando se reinicia el asistente.

Procedimiento

1. Detenga el servidor web de Centro de operaciones.
2. En el sistema donde está instalado Centro de operaciones, vaya al siguiente directorio, donde *installation_dir* representa el directorio en el que está instalado Centro de operaciones:
   - AIX Linux *dir_instalación*`/ui/Liberty/usr/servers/guiServer`
   - Windows *dir_instalación*`\ui\Liberty\usr\servers\guiServer`

   Por ejemplo:

- AIX Linux `/opt/tivoli/tsm/ui/Liberty/usr/servers/guiServer`
- Windows `c:\Archivos de programa\Tivoli\TSM\ui\Liberty\usr\servers\guiServer`

3. En el directorio `guiServer`, elimine el archivo `serverConnection.properties`.
4. Inicie el servidor web Centro de operaciones.
5. Abra el Centro de operaciones.
6. Utilice el asistente de configuración para volver a configurar el Centro de operaciones. Especifique una contraseña nueva para el ID de administración de supervisión.
7. En cualquier servidor spoke que estuviera conectado anteriormente al servidor concentrador, actualice la contraseña para el ID de administrador de supervisión emitiendo el mandato siguiente desde la interfaz de línea de mandatos de IBM Spectrum Protect:

   ```
   UPDATE ADMIN IBM-OC-hub_server_name new_password
   ```

   Restricción: No cambie ningún valor para el ID de administrador. Después de especificar la contraseña inicial, Centro de operaciones la gestiona automáticamente.

Cambio del servidor concentrador

Puede utilizar el Centro de operaciones para eliminar el servidor concentrador de IBM Spectrum Protect y configurar otro servidor concentrador.

Procedimiento

1. Reinicie el asistente de configuración inicial del Centro de operaciones. Como parte de este procedimiento, suprima la conexión del servidor concentrador existente.
2. Utilice el asistente para configurar el Centro de operaciones para conectarse al nuevo servidor concentrador.

Tareas relacionadas:

"Reinicio del asistente de configuración inicial" en la página 97

Restauración de la configuración a un estado de preconfiguración

Si se producen determinados problemas, es posible que desee restaurar la configuración de Centro de operaciones al estado preconfigurado donde los servidores de IBM Spectrum Protect no están definidos como servidores de concentrador o spoke.

Procedimiento

Para restaurar la configuración, complete los pasos siguientes:

1. Detenga el servidor web de Centro de operaciones.
2. Para desconfigurar el servidor concentrador, lleve a cabo los siguientes pasos:
   a. En el servidor concentrador, emita los mandatos siguientes:

   ```
   SET MONITORINGADMIN ""
   SET MONITOREDSERVERGROUP ""
   SET STATUSMONITOR OFF
   SET ALERTMONITOR OFF
   REMOVE ADMIN IBM-OC-hub_server_name
   ```

Consejo: IBM-OC-*nombre_servidor_concentrador* representa el ID de administrador de supervisión que se creó automáticamente al configurar inicialmente el servidor concentrador.

b. Restablezca la contraseña para el servidor concentrador emitiendo el siguiente mandato en el servidor concentrador:

```
SET SERVERPASSWORD ""
```

Atención: No complete este paso si el servidor concentrador está configurado con otros servidores para otros fines como, por ejemplo, para la compartición de bibliotecas, exportación e importación de datos o la réplica de nodos.

3. Desconfigure los servidores spoke completando los pasos siguientes:

a. En el servidor concentrador para determinar si algún servidor spoke permanece como miembro del grupo de servidores, emita el siguiente mandato:

```
QUERY SERVERGROUP IBM-OC-nombre_servidor_concentrador
```

Consejo: IBM-OC-*nombre_servidor_concentrador* representa el nombre del grupo de servidores supervisados que se han creado automáticamente al configurar el primer servidor spoke. Este nombre de grupo de servidores también es el mismo que el ID de administrador de supervisión que se creó automáticamente al configurar inicialmente el servidor concentrador.

b. En el servidor concentrador, para suprimir servidores spoke del grupo de servidores, emita el siguiente mandato para cada servidor spoke:

```
DELETE GRPMEMBER IBM-OC-nombre_servidor_concentrador nombre_servidor_spoke
```

c. Después de que todos los servidores spoke se ha suprimido del grupo de servidores, emita los mandatos siguientes en el servidor concentrador:

```
DELETE SERVERGROUP IBM-OC-nombre_servidor_concentrador
SET MONITOREDSERVERGROUP ""
```

d. En cada servidor spoke, emita los siguientes mandatos:

```
REMOVE ADMIN IBM-OC-hub_server_name
SETOPT PUSHSTATUS NO
SET ALERTMONITOR OFF
SET STATUSMONITOR OFF
```

e. En cada servidor spoke, elimine la definición del servidor concentrador emitiendo el siguiente mandato:

```
DELETE SERVER nombre_servidor_concentrador
```

Atención: No complete este paso si la definición se utiliza para otros fines, como, por ejemplo, para la compartición de bibliotecas, exportación e importación de datos o la réplica de nodos.

f. En el servidor concentrador, suprima la definición de cada servidor spoke emitiendo el mandato siguiente:

```
DELETE SERVER nombre_servidor_spoke
```

Atención: No complete este paso si la definición de servidor se utiliza para otros fines, como, por ejemplo, para la compartición de bibliotecas, exportación e importación de datos o la réplica de nodos.

4. Restaure los valores predeterminados en cada uno de los servidores emitiendo los mandatos siguientes:

```
SET STATUSREFRESHINTERVAL 5
SET ALERTUPDATEINTERVAL 10
SET ALERTACTIVEDURATION 480
SET ALERTINACTIVEDURATION 480
```

```
SET ALERTCLOSEDDURATION 60
SET STATUSATRISKINTERVAL TYPE=AP INTERVAL=24
SET STATUSATRISKINTERVAL TYPE=VM INTERVAL=24
SET STATUSATRISKINTERVAL TYPE=SY INTERVAL=24
SET STATUSSKIPASFAILURE YES TYPE=ALL
```

5. Reinicie el asistente de configuración inicial del Centro de operaciones.

Tareas relacionadas:

"Reinicio del asistente de configuración inicial" en la página 97

"Inicio y detención del servidor web" en la página 96

Capítulo 16. Protección de aplicaciones, máquinas virtuales y sistemas

El servidor protege los datos para los clientes, que pueden incluir aplicaciones, máquinas virtuales y sistemas. Para iniciar la protección de datos de cliente, registre el nodo cliente con el servidor y seleccione una planificación de copia de seguridad para proteger los datos de cliente.

Adición de clientes

Después de implementar una solución de protección de datos con IBM Spectrum Protect, puede expandir la solución añadiendo clientes.

Acerca de esta tarea

El procedimiento describe los pasos básicos para añadir un cliente. Para obtener instrucciones más detalladas sobre la configuración de clientes, consulte la documentación del producto que haya instalado en el nodo cliente. Puede tener los siguientes tipos de nodos de cliente:

Nodos de cliente de aplicaciones
Los nodos de cliente de aplicaciones incluyen servidores de correo electrónico, bases de datos y otras aplicaciones. Por ejemplo, cualquiera de las siguientes aplicaciones puede ser un nodo cliente de aplicaciones:

- IBM Spectrum Protect Snapshot
- IBM Spectrum Protect for Databases
- IBM Spectrum Protect for Enterprise Resource Planning
- IBM Spectrum Protect for Mail
- IBM Spectrum Protect for Virtual Environments

Nodos de cliente de sistemas
Los nodos de cliente de sistemas incluyen estaciones de trabajo, servidores de archivos de almacenamiento adjunto a red (NAS) y clientes de API.

Nodos de cliente de máquina virtual
Los nodos de cliente de máquina virtual constan de un host invitado individual dentro de un hipervisor. Cada máquina virtual se representa como un espacio de archivos.

Procedimiento

Para añadir un cliente, complete los pasos siguientes:

1. Seleccione el software a instalar en el nodo de cliente y planifique la instalación. Siga las instrucciones de “Selección del software de cliente y planificación de la instalación” en la página 102.
2. Especifique cómo hacer copia de seguridad y archivado de los datos de cliente. Siga las instrucciones de “Especificación de reglas para hacer copia de seguridad y archivado de los datos de cliente” en la página 104.
3. Especifique cuándo hacer copia de seguridad y archivado de los datos de cliente. Siga las instrucciones de “Planificación de copia de seguridad y operaciones de archivado” en la página 107.

4. Para permitir que el cliente se conecte al servidor, registre el cliente. Siga las instrucciones de “Registro de clientes” en la página 108.
5. Para iniciar la protección de un nodo de cliente, instale y configure el software seleccionado en el nodo de cliente. Siga las instrucciones de “Instalación y configuración de clientes” en la página 109.

Selección del software de cliente y planificación de la instalación

Diferentes tipos de datos requieren diferentes tipos de protección. Identifique el tipo de datos que debe proteger y seleccione el software apropiado.

Acerca de esta tarea

La práctica preferida es instalar el cliente de archivado y copia de seguridad en todos los nodos de cliente para poder configurar e iniciar el aceptador de cliente en el nodo de cliente. El aceptador de cliente se ha diseñado para ejecutar de forma eficaz operaciones planificadas.

El aceptador de cliente ejecuta planificaciones para los productos siguientes: el cliente de archivado y copia de seguridad, IBM Spectrum Protect for Databases, IBM Spectrum Protect for Enterprise Resource Planning, IBM Spectrum Protect for Mail y IBM Spectrum Protect for Virtual Environments. Si instala un producto para el cual el aceptador de cliente no ejecuta planificaciones, debe seguir las instrucciones de configuración en la documentación de producto para asegurarse de que se puede producir las operaciones planificadas.

Procedimiento

En función de su objetivo, seleccione los productos para instalar y revise las instrucciones de instalación.

Consejo: Si instala el software de cliente ahora, también debe completar las tareas de configuración de cliente que se describen en “Instalación y configuración de clientes” en la página 109 antes de poder utilizar el cliente.

Objetivo	Producto y descripción	Instrucciones de instalación
Proteger un servidor de archivos o una estación de trabajo	El cliente de archivado y copia de seguridad realiza la copia de seguridad y el archivado de archivos y directorios de los servidores de archivos y las estaciones de trabajo en el almacenamiento. También puede restaurar y recuperar versiones de copias de seguridad y copias archivadas de archivos.	• Requisitos del cliente de archivado y copia de seguridad • Instalación de los clientes de archivado y copia de seguridad de UNIX y Linux • Instalación del cliente de archivado y copia de seguridad de Windows
Proteger aplicaciones con prestaciones de restauración y copia de seguridad de instantáneas	IBM Spectrum Protect Snapshot protege los datos con prestaciones de restauración y copia de seguridad de instantánea conocidas por la aplicación e integradas. Puede proteger datos almacenados por aplicaciones de IBM software de base de datos DB2 y SAP, Oracle, Microsoft Exchange y Microsoft SQL Server.	• Instalación y actualización de IBM Spectrum Protect Snapshot para UNIX y Linux • Instalación y actualización de IBM Spectrum Protect Snapshot for VMware • Instalación y actualización de IBM Spectrum Protect Snapshot for Windows

Objetivo	Producto y descripción	Instrucciones de instalación
Proteja una aplicación de correo electrónico en un servidor IBM Domino	IBM Spectrum Protect for Mail: Data Protection for IBM Domino automatiza la protección de datos, de forma que las copias de seguridad se han completado sin concluir servidores IBM Domino.	• Instalación de Data Protection for IBM Domino en un sistema UNIX, AIX o Linux (V7.1.0) • Instalación de Data Protection for IBM Domino en un sistema Windows (V7.1.0)
Proteja una aplicación de correo electrónico en un servidor Microsoft Exchange	IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server automatiza la protección de datos de forma que las copias de seguridad se han completado sin concluir servidores Microsoft Exchange.	Instalación, actualización y migración de IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server
Proteja una base de datos IBM DB2	La interfaz de programación de aplicaciones (API) del cliente de archivado y copia de seguridad puede utilizarse para hacer una copia de seguridad de los datos de DB2 en el servidor de IBM Spectrum Protect.	Instalación de clientes de archivado y copia de seguridad de IBM Spectrum Protect (UNIX, Linux y Windows)
Proteja una base de datos IBM Informix	La API del cliente de archivado y copia de seguridad puede utilizarse para hacer una copia de seguridad de los datos de Informix en el servidor de IBM Spectrum Protect.	Instalación de clientes de archivado y copia de seguridad de IBM Spectrum Protect (UNIX, Linux y Windows)
Proteja una base de datos de Microsoft SQL.	IBM Spectrum Protect for Databases: Data Protection for Microsoft SQL Server protege datos de Microsoft SQL.	Instalación de Data Protection for SQL Server en Windows Server Core
Proteger una base de datos Oracle	IBM Spectrum Protect for Databases: Data Protection for Oracle protege los datos de Oracle.	Instalación de Data Protection for Oracle
Proteger un entorno SAP	IBM Spectrum Protect for Enterprise Resource Planning: La protección de datos para SAP proporciona protección personalizada para entornos SAP. El producto está diseñado para mejorar la disponibilidad de servidores de bases de datos SAP y reducir la carga de trabajo de administración.	• Instalación de IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP for DB2 • Instalación de IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP for Oracle
Proteger una máquina virtual	IBM Spectrum Protect for Virtual Environments proporciona protección que se ha adaptado para los entornos virtuales Microsoft Hyper-V y VMware. Puede utilizar IBM Spectrum Protect for Virtual Environments para crear copias de seguridad siempre incrementales almacenadas en un servidor centralizado, crear políticas de copia de seguridad y restaurar máquinas virtuales o archivos individuales. De forma alternativa, utilice el cliente de archivado y copia de seguridad para hacer la copia de seguridad y restauración de una máquina virtual de VMware o Microsoft Hyper-V completa. También puede hacer copia de seguridad y restaurar archivos y directorios desde una máquina virtual VMware.	• Instalación de Data Protection for Microsoft Hyper-V • Instalación y actualización de Data Protection for VMware • Instalación de clientes de archivado y copia de seguridad de IBM Spectrum Protect (UNIX, Linux y Windows)

Consejo: Para utilizar el cliente para gestionar el espacio, puede instalar IBM Spectrum Protect for Space Management o IBM Spectrum Protect HSM for Windows.

Especificación de reglas para hacer copia de seguridad y archivado de los datos de cliente

Antes de añadir un cliente, asegúrese de que se han especificado las reglas correctas de copia de seguridad y archivado de los datos de cliente. Durante el proceso de registro de cliente, asigne el nodo de cliente a un dominio de políticas, que tenga las reglas que controlan cómo y cuándo se almacenan los datos de cliente.

Antes de empezar

Determine cómo debe procederse:

- Si está familiarizado con las políticas que están configuradas para la solución y sabe que no requieren cambios, continúe con "Planificación de copia de seguridad y operaciones de archivado" en la página 107.
- Si no está familiarizado con las políticas, siga los pasos de este procedimiento.

Acerca de esta tarea

Las políticas afectan a la cantidad de datos que se almacenan a lo largo del tiempo y el periodo de tiempo durante el cual los datos se retienen y están disponibles para que los clientes los restauren. Para cumplir los objetivos de protección de datos, puede actualizar la política predeterminada y crear sus propias políticas. Una política incluye las siguientes reglas:

- Cómo y cuándo se hace una copia de seguridad de los archivos y se archivan en el almacenamiento del servidor.
- El número de copias de un archivo y el período de tiempo que se mantienen las copias en el almacenamiento del servidor.

Durante el proceso de registro de cliente, se asigna un cliente a un *dominio de políticas*. La política para un cliente específico la determinan las reglas del dominio de políticas al que está asignado el cliente. En el dominio de políticas, las reglas que están en vigor se encuentran en el *conjunto de políticas activas* activo.

Cuando un cliente realiza la copia de seguridad o el archivado de un archivo, el archivo se vincula a una clase de gestión del conjunto de políticas activas activo del dominio de políticas. Una *clase de gestión* es el conjunto de claves de reglas para gestionar los datos de cliente. Las operaciones de copia de seguridad y archivado en el cliente utilizan los valores de la clase de gestión predeterminada del dominio de políticas a menos que se personalice adicionalmente la política. Una política puede personalizarse definiendo más clases de gestión y asignando su uso a través de las opciones de cliente.

Las opciones de cliente se pueden especificar en un archivo local editable del sistema cliente y en un conjunto de opciones de cliente en el servidor. Las opciones del conjunto de opciones de cliente en el servidor pueden alterar temporalmente las opciones del archivo de opciones del cliente local o añadirse a dichas opciones.

Procedimiento

1. Revise las políticas configuradas para su solución siguiendo las instrucciones incluidas en "Visualización de políticas" en la página 105.

2. Si necesita realizar cambios poco importantes para adaptarse a los requisitos de retención de datos, siga las instrucciones incluidas en "Edición de políticas".
3. Opcional: Si necesita crear dominios de políticas o realizar cambios extensos en las políticas para satisfacer los requisitos de retención de datos, consulte Personalización de políticas.

Visualización de políticas

Vea las políticas para determinar si se deben editar para satisfacer los requisitos.

Procedimiento

1. Para ver el conjunto de políticas activas para un dominio de políticas, complete los pasos siguientes:
   a. En la página Servicios del Centro de operaciones, seleccione un dominio de políticas y pulse **Detalles**.
   b. En la página Resumen del dominio de políticas, pulse el separador **Conjuntos de políticas**.
2. Para ver los conjuntos de políticas inactivas para un dominio de políticas, complete los pasos siguientes:
   a. En la página Conjuntos de políticas, pulse el conmutador **Configurar**. Ahora puede ver y editar los conjuntos de políticas que están inactivos.
   b. Desplácese a través de conjuntos de políticas inactivas utilizando las flechas hacia adelante y atrás. Al visualizar un conjunto de políticas inactivas, los valores que diferencian el conjunto de políticas inactivas del conjunto de políticas activas se resaltan.
   c. Pulse el conmutador **Configurar**. Los conjuntos de políticas ya no se pueden editar.

Edición de políticas

Para cambiar las reglas que se aplican a un dominio de políticas, edite el conjunto de políticas activas para el dominio de políticas. También puede activar un conjunto de políticas diferente para un dominio.

Antes de empezar

Los cambios en la política pueden afectar a la retención de datos. Asegúrese de que continúa haciendo copia de seguridad de los datos que son esenciales para su organización para que pueda restaurar esos datos si se produce un desastre. Además, asegúrese de que el sistema tiene suficiente espacio de almacenamiento para operaciones de copia de seguridad planificadas.

Acerca de esta tarea

Edite un conjunto de políticas cambiando una o más clases de gestión dentro de un conjunto de políticas. Si edita un conjunto de políticas activas, los cambios no están disponibles para los clientes a menos que reactive el conjunto de políticas. Para hacer que el conjunto de políticas editado esté disponible para los clientes, active el conjunto de políticas.

Aunque puede definir varios conjuntos de políticas para un dominio de políticas, sólo un conjunto de políticas puede estar activo. Cuando activa un conjunto de políticas diferente, sustituye al conjunto de políticas activo actualmente.

Para obtener información acerca de las prácticas preferidas para definir las políticas, consulte Personalización de políticas.

Procedimiento

1. En la página Servicios del Centro de operaciones, seleccione un dominio de políticas y pulse **Detalles**.
2. En la página Resumen del dominio de políticas, pulse el separador **Conjuntos de políticas**.

   La página Conjuntos de políticas indica el nombre del conjunto de políticas activo y lista todas las clases de gestión pare ese conjunto de políticas.
3. Pulse el conmutador **Configurar**. El conjunto de políticas es editable.
4. Opcional: Para editar un conjunto de políticas que no está activo, pulse las flechas hacia adelante y hacia atrás para ubicar el conjunto de políticas.
5. Edite el conjunto de políticas completando cualquiera de las siguientes acciones:

Opción	Descripción
Añadir una clase de gestión	1. En la tabla Conjuntos de políticas, pulse **+Clase de gestión**. 2. Para especificar las reglas para los datos de copia de seguridad y archivado, complete los campos de la ventana Añadir clase de gestión. 3. Para hacer que la clase de gestión sea la clase de gestión predeterminada, seleccione la casilla de verificación **Establecer como predeterminada**. 4. Pulse **Añadir**.
Suprimir una clase de gestión	En la columna Clase de gestión, pulse **-**. **Consejo:** Para suprimir la clase de gestión predeterminada, primero debe asignar una clase de gestión diferente como predeterminada.
Establecer una clase de gestión como clase de gestión predeterminada	En la columna Predeterminada para la clase de gestión, pulse el botón de selección. **Consejo:** La clase de gestión predeterminada gestiona los archivos de cliente cuando no hay asignada otra clase de gestión a, o cuando es adecuada para gestionar un archivo. Para asegurarse de que los clientes siempre pueden hacer copia de seguridad y archivar archivos, elija una clase de gestión que contenga reglas para la copia de seguridad y archivado de archivos.
Modificar una clase de gestión	Para cambiar las propiedades de una clase de gestión, actualice los campos en la tabla.

6. Pulse **Guardar**.

   Atención: Cuando activa un conjunto de políticas nuevo, es posible que se pierdan datos. Los datos protegidos bajo un conjunto de políticas es posible que no estén protegidos bajo otro conjunto de políticas. Por lo tanto, antes de activar un conjunto de políticas, asegúrese de que las diferencias entre el conjunto de políticas anterior y el nuevo conjunto de políticas no provocan una pérdida de datos.
7. Pulse **Activar**. Se visualiza un resumen de las diferencias entre el conjunto de políticas activas y el nuevo conjunto de políticas. Asegúrese de que los cambios en el nuevo conjunto de políticas son coherentes con los requisitos de retención de datos completando los pasos siguientes:
   a. Revise las diferencias entre las clases de gestión correspondientes en los dos conjuntos de políticas y tenga en cuenta las consecuencias para los archivos cliente. Los archivos cliente que están enlazados a clases de gestión en el conjunto de políticas activas se enlazarán a las clases de gestión con los mismos nombres en el conjunto de políticas nuevo.

b. Identifique las clases de gestión en el conjunto de políticas activas que no tienen contrapartidas en el conjunto de políticas nuevo y tenga en cuenta las consecuencias para los archivos cliente. Los archivos cliente que están enlazados a estas clases de gestión estarán gestionados por la clase de gestión predeterminada en el conjunto de políticas nuevo.

c. Si los cambios que va a implementar el conjunto de políticas son aceptables, seleccione la casilla de verificación **Entiendo que estas actualizaciones pueden provocar pérdida de datos** y pulse **Activar**.

Planificación de copia de seguridad y operaciones de archivado

Antes de registrar un nuevo cliente en el servidor, asegúrese de que existe una planificación disponible para especificar cuándo tendrán lugar las operaciones de archivado y copia de seguridad. Durante el proceso de registro, asigne una planificación al cliente.

Antes de empezar

Determine cómo debe procederse:

- Si está familiarizado con las planificaciones que se han configurado para la solución y sabe que no necesitan modificación, continúe con "Registro de clientes" en la página 108.
- Si no está familiarizado con las planificaciones o las planificaciones necesitan modificación, siga los pasos de este procedimiento.

Acerca de esta tarea

Normalmente, las operaciones de seguridad para todos los clientes deben completarse diariamente. Planifique detenidamente las cargas de trabajo de cliente y servidor para lograr el mejor rendimiento para el entorno de almacenamiento. Para evitar el solapamiento de las operaciones de cliente y servidor, planifique las operaciones de archivado y copia de seguridad de cliente para que se ejecuten por la noche. Si las operaciones de cliente y servidor se solapan o no se les da el tiempo y recursos suficientes para procesarse, es posible que experimente una disminución del rendimiento del sistema, operaciones con errores u otros problemas.

Procedimiento

1. Revise las planificaciones disponibles pasando el cursor sobre **Clientes** en la barra de menús Centro de operaciones. Pulse **Planificaciones**.
2. Opcional: Modifique o cree una planificación completando los pasos siguientes:

Opción	Descripción
Modificar una planificación	1. En la vista Planificaciones, seleccione la planificación y pulse **Detalles**. 2. En la página Detalles de planificación, vea detalles pulsando las flechas azules al principio de las filas. 3. Modifique los valores de la planificación y pulse **Guardar**.
Crear una planificación	En la vista Planificaciones, pulse **+Planificar** y complete los pasos para crear una planificación.

3. Opcional: Para configurar valores de planificación que no están visibles en el Centro de operaciones, utilice un mandato de servidor. Por ejemplo, puede que desee planificar una operación de cliente que realice la copia de seguridad de un directorio específico y lo asigne a una clase de gestión distinta de la predeterminada.
   a. En la página Visión general del Centro de operaciones, pase el ratón por encima del icono de configuración  y pulse **Creador de mandatos**.
   b. Emita el mandato **DEFINE SCHEDULE** para crear una planificación o el mandato **UPDATE SCHEDULE** para modificar una planificación. Para obtener detalles sobre los mandatos, consulte DEFINE SCHEDULE (Definir una planificación de cliente) o UPDATE SCHEDULE (Actualizar una planificación de cliente).

Tareas relacionadas:

Ajuste de la planificación para las operaciones diarias

Registro de clientes

Registrar un cliente para garantizar que el cliente pueda conectarse con el servidor y el servidor pueda proteger los datos de cliente.

Antes de empezar

Determine si el cliente requiere un ID de usuario administrativo con autorización de propietario de cliente en el nodo de cliente. Para determinar qué clientes requieren un ID de usuario administrativo, consulte nota técnica 7048963.

Restricción: Para algunos tipos de clientes, el nombre de nodo de cliente y el ID de usuario administrativo deben coincidir. No se pueden autenticar los clientes utilizando el método de autenticación Lightweight Directory Access Protocol que se ha introducido en V7.1.7. Para obtener detalles sobre este método de autenticación, lo que a veces se denomina modalidad integrada, consulte Autenticación de los usuarios mediante una base de datos Active Directory.

Procedimiento

Para registrar un cliente, realice una de las siguientes acciones.

- Si el cliente necesita un ID de usuario administrativo, registre el cliente mediante el mandato **REGISTER NODE** y especifique el parámetro **USERID**:

  ```
  register node nombre_nodo contraseña userid=nombre_nodo
  ```

  donde *nombre_nodo* especifica el nombre de nodo y *contraseña* especifica la contraseña del nodo. Si desea obtener más información al respecto, consulte el apartado Registrar un nodo.
- Si el cliente no requiere un ID de usuario administrativo, registre el cliente mediante el asistente Agregar cliente de Centro de operaciones. Realice los pasos siguientes:
  1. En la barra de menús de Centro de operaciones, pulse **Clientes**.
  2. En la tabla Clientes, pulse **+ Cliente**.
  3. Complete los pasos en el asistente Añadir cliente:
     a. Especifique que los datos redundantes se puedan eliminar en el cliente y en el servidor. En el área de eliminación de duplicados de datos del lado del cliente, active la casilla de verificación **Habilitar**.

b. En la ventana Configuración, copie los valores de opción **TCPSERVERADDRESS**, **TCPPORT**, **NODENAME** y **DEDUPLICATION**.

   Consejo: Anote los valores de opción y guárdelos en un lugar seguro. Después de completar el registro de cliente e instalar el software en el nodo de cliente, utilice los valores para configurar el cliente.

c. Siga las instrucciones del asistente para especificar el dominio de políticas y un conjunto de opciones.

d. Defina cómo se mostrarán los riesgos para el cliente especificando el valor de en riesgo.

e. Pulse **Añadir cliente**.

Referencia relacionada:

- Opción Tcpserveraddress
- Opción Tcpport
- Opción Nodename
- Opción Deduplication

Instalación y configuración de clientes

Para empezar a proteger un nodo cliente, debe instalar y configurar el software seleccionado.

Procedimiento

Si ya ha instalado el software, comience en el paso 2 en la página 110.

1. Realice una de las siguientes acciones:
   - Para instalar software en una aplicación de nodo cliente, siga las instrucciones.

Software	Enlace a instrucciones
Cliente de copia de seguridad/archivado de IBM Spectrum Protect	• Instalación de los clientes de archivado y copia de seguridad de UNIX y Linux • Instalación del cliente de archivado y copia de seguridad de Windows
IBM Spectrum Protect for Databases	• Instalación de Data Protection for Oracle • Instalación de Data Protection for SQL Server en Windows Server Core
IBM Spectrum Protect for Mail	• Instalación de Data Protection for IBM Domino en un sistema UNIX, AIX o Linux (V7.1.0) • Instalación de Data Protection for IBM Domino en un sistema Windows (V7.1.0) • Instalación, actualización y migración de IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server
IBM Spectrum Protect Snapshot	• Instalación y actualización de IBM Spectrum Protect Snapshot para UNIX y Linux • Instalación y actualización de IBM Spectrum Protect Snapshot for VMware • Instalación y actualización de IBM Spectrum Protect Snapshot for Windows

Software	Enlace a instrucciones
IBM Spectrum Protect for Enterprise Resource Planning	• Instalación de IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP for DB2 • Instalación de IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP for Oracle

- Para instalar software en un nodo cliente de máquina virtual, siga las instrucciones para el tipo de copia de seguridad seleccionada.

Tipo de copia de seguridad	Enlace a instrucciones
Si planea crear copias de seguridad de VMware completas de máquinas virtuales, instale y configure el cliente de archivado y copia de seguridad de IBM Spectrum Protect.	• Instalación de los clientes de archivado y copia de seguridad de UNIX y Linux • Instalación del cliente de archivado y copia de seguridad de Windows
Si planea crear copias de seguridad incrementales siempre completas de máquinas virtuales, instale y configure IBM Spectrum Protect for Virtual Environments y el cliente de archivado y copia de seguridad en el mismo nodo de cliente o en nodos de cliente diferentes.	• Documentación del producto en línea de IBM Spectrum Protect for Virtual Environments **Consejo:** Puede obtener el software para IBM Spectrum Protect for Virtual Environments y el cliente de archivado y copia de seguridad en el paquete de instalación de IBM Spectrum Protect for Virtual Environments.

2. Para permitir que el cliente se conecte al servidor, añada o actualice los valores para las opciones **TCPSERVERADDRESS**, **TCPPORT** y **NODENAME** en el archivo de opciones del cliente. Utilice los valores que ha anotado cuando ha registrado el cliente (“Registro de clientes” en la página 108).
   - Para los clientes que están instalados en un sistema operativo AIX, Linux o Mac OS X, añada los valores al archivo de opciones de sistema de cliente, `dsm.sys`.
   - Para los clientes que se han instalado en un sistema operativo Windows, añada los valores al archivo `dsm.opt`.

   De forma predeterminada, los archivos de opciones están en el directorio de instalación.
3. Si ha instalado un cliente de archivado y copia de seguridad en un sistema operativo Linux o Windows, instale el servicio de gestión de clientes en el cliente. Siga las instrucciones de “Instalación del servicio de gestión de cliente” en la página 66.
4. Configure el cliente para ejecutar las operaciones planificadas. Siga las instrucciones de “Configuración del cliente para ejecutar las operaciones planificadas” en la página 111.
5. Opcional: Configure las comunicaciones a través de un cortafuegos. Siga las instrucciones de “Configuración de las comunicaciones entre cliente y servidor a través de un cortafuegos” en la página 113.
6. Ejecute una copia de seguridad de prueba para verificar que los datos están protegidos según lo planificado. Por ejemplo, para un cliente de archivado y copia de seguridad, complete los pasos siguientes:

a. En la página Clientes del Centro de operaciones, seleccione el cliente del que desea realizar la copia de seguridad y pulse **Copia de seguridad**.
b. Verifique que la copia de seguridad finalice correctamente y que no hay mensajes de error o de aviso.

7. Supervise los resultados de las operaciones planificadas para el cliente en el Centro de operaciones.

Qué hacer a continuación

Si necesita cambiar los elementos de los que se está haciendo copia de seguridad del cliente, siga las instrucciones de "Modificación del ámbito de una copia de seguridad de cliente" en la página 118.

Configuración del cliente para ejecutar las operaciones planificadas

Debe configurar e iniciar un planificador de cliente en el nodo cliente. El planificador de cliente habilita la comunicación entre el cliente y el servidor para que se puedan realizar las operaciones planificadas. Por ejemplo, las operaciones planificadas normalmente incluyen la copia de seguridad de archivos desde un cliente.

Acerca de esta tarea

El método preferido es instalar el cliente de archivado y copia de seguridad en todos los nodos de cliente de forma que pueda configurar e iniciar el aceptador de cliente en el nodo de cliente. El aceptador de cliente se ha diseñado para ejecutar de forma eficaz operaciones planificadas. El aceptador de cliente gestiona el planificador de cliente para que el planificador de cliente solo se ejecute cuando sea necesario:

- Cuando es el momento de consultar al servidor sobre la siguiente operación planificada
- Cuando es el momento de iniciar la siguiente operación planificada

Utilizando el aceptador de cliente, puede reducir el número de procesos de fondo en el cliente y ayudar a evitar problemas de retención de memoria.

El aceptador de cliente ejecuta planificaciones para los productos siguientes: el cliente de archivado y copia de seguridad, IBM Spectrum Protect for Databases, IBM Spectrum Protect for Enterprise Resource Planning, IBM Spectrum Protect for Mail y IBM Spectrum Protect for Virtual Environments. Si ha instalado un producto para el cual el aceptador de cliente no ejecuta planificaciones, siga las instrucciones de configuración en la documentación de producto para garantizar que las operaciones planificadas se pueden producir.

Si la empresa utiliza una herramienta de planificación de terceros como práctica estándar, puede utilizar dicha herramienta de planificación como alternativa al aceptador de cliente. Normalmente, las herramientas de planificación de terceros inician los programas cliente directamente utilizando mandatos de sistema operativo. Para configurar una herramienta de planificación de terceros, consulte la documentación del producto.

Procedimiento

Para configurar e iniciar el planificador de cliente utilizando el aceptador de cliente, siga las instrucciones para el sistema operativo que está instalado en el nodo cliente.

AIX y Oracle Solaris

1. Desde la GUI del cliente de archivado y copia de seguridad, pulse **Editar** > **Preferencias de cliente**.
2. Pulse la pestaña **Cliente web**.
3. En el campo **Opciones de servicios gestionados**, pulse **Planificar**. Si también desea que el aceptador de cliente gestione el cliente web, pulse la opción **Ambas**.
4. Para asegurarse de que el planificador puede iniciarse sin supervisión, en el archivo `dsm.sys`, establezca la opción **`passwordaccess`** en `generate`.
5. Para almacenar la contraseña del nodo de cliente, emita el siguiente mandato y entre la contraseña del nodo de cliente cuando se le solicite:

   ```
   dsmc query sess
   ```
6. Inicie el aceptador de cliente emitiendo el mandato siguiente en la línea de mandatos:

   ```
   /usr/bin/dsmcad
   ```
7. Para permitir que el aceptador de cliente se inicie automáticamente después del reinicio de un sistema, añada la entrada siguiente al archivo de arranque del sistema (normalmente, `/etc/inittab`):

   ```
   tsm::once:/usr/bin/dsmcad > /dev/null 2>&1 # Daemon de aceptación de clientes
   ```

Linux

1. Desde la GUI del cliente de archivado y copia de seguridad, pulse **Editar** > **Preferencias de cliente**.
2. Pulse la pestaña **Cliente web**.
3. En el campo **Opciones de servicios gestionados**, pulse **Planificar**. Si también desea que el aceptador de cliente gestione el cliente web, pulse la opción **Ambas**.
4. Para asegurarse de que el planificador puede iniciarse sin supervisión, en el archivo `dsm.sys`, establezca la opción **`passwordaccess`** en `generate`.
5. Para almacenar la contraseña del nodo de cliente, emita el siguiente mandato y entre la contraseña del nodo de cliente cuando se le solicite:

   ```
   dsmc query sess
   ```
6. Inicie el aceptador de cliente iniciando sesión con el ID de usuario root y emitiendo el mandato siguiente:

   ```
   service dsmcad start
   ```
7. Para permitir que el aceptador de cliente pueda iniciarse automáticamente después del reinicio de un sistema, añada el servicio emitiendo el mandato siguiente en el indicador de shell:

   ```
   # chkconfig --add dsmcad
   ```

MAC OS X

1. En la GUI del cliente de archivado y copia de seguridad, pulse **Editar** > **Preferencias de cliente**.
2. Para asegurarse de que el planificador puede iniciarse sin supervisión, pulse **Autorización**, seleccione **Generar contraseña** y pulse **Aplicar**.
3. Para especificar cómo se gestionan los servicios, pulse **Cliente web**, seleccione **Planificar**, pulse **Aplicar**, y pulse **Aceptar**.
4. Para asegurarse de que la contraseña generada se guarda, reinicie el cliente de archivado y copia de seguridad.
5. Utilice la aplicación de herramientas IBM Spectrum Protect para administradores para iniciar el aceptador de cliente.

Windows

1. En la GUI del cliente de archivado y copia de seguridad, pulse **Programas de utilidad** > **Asistente de configuración** > **Obtener ayuda para configurar Planificador cliente**. Pulse **Siguiente**.
2. Consulte la información en la página Asistente del planificador y pulse **Siguiente**.
3. En la página Tarea de planificador, seleccione **Instalar un planificador nuevo o adicional** y pulse **Siguiente**.
4. En la página Nombre y ubicación del planificador, especifique un nombre para el planificador de cliente que está añadiendo. A continuación, seleccione **Utilizar el daemon de aceptador de cliente (CAD)** para gestionar el planificador y pulse **Siguiente**.
5. Especifique el nombre que desea asignar a este aceptador de cliente. El nombre predeterminado es Aceptación de clientes. Pulse **Siguiente**.
6. Complete la configuración paso a paso a través del asistente.
7. Actualice el archivo de opciones de cliente, `dsm.opt`, y configure la opción **`passwordaccess`** como `generate`.
8. Para almacenar la contraseña de nodo de cliente, emita el siguiente mandato en el indicador de mandatos:

   ```
   dsmc query sess
   ```

   Entre la contraseña de nodo de cliente cuando se le solicite.
9. Inicie el servicio aceptador de cliente desde la página Control de servicios. Por ejemplo, si ha utilizado el nombre predeterminado, inicie el servicio Aceptador de cliente. No inicie el servicio de planificador que ha especificado en la página Nombre y ubicación del planificador. El servicio de planificador se ha iniciado y detenido automáticamente mediante el servicio aceptador de cliente, según sea necesario.

Configuración de las comunicaciones entre cliente y servidor a través de un cortafuegos

Si un cliente debe comunicarse con un servidor a través de un cortafuegos, deberá habilitar las comunicaciones entre cliente y servidor a través del cortafuegos.

Antes de empezar

Si ha utilizado el asistente Añadir cliente para registrar un cliente, busque los valores de opción en el archivo de opciones de cliente que ha obtenido durante ese proceso. Puede utilizar los valores para especificar puertos.

Acerca de esta tarea

Atención: No configure un cortafuegos de forma que pueda provocar la finalización de sesiones que está utilizando un agente de almacenamiento o servidor. La finalización de una sesión válida puede provocar resultados imprevisibles. Es posible que los procesos y sesiones parece que se detienen debido a errores de entrada y de salida. Para ayudar a excluir sesiones de las restricciones de tiempo de espera, configure puertos conocidos para los componentes de IBM Spectrum Protect. Asegúrese de que la opción de servidor **`KEEPALIVE`** permanece establecida en el valor predeterminado de `YES`. De esta forma, puede asegurarse de que la comunicación entre cliente y servidor no se interrumpe. Para obtener instrucciones sobre la configuración de la opción de servidor **`KEEPALIVE`**, consulte KEEPALIVE.

Procedimiento

Abra los siguientes puertos para permitir el acceso a través del cortafuegos:

Puerto TCP/IP para el cliente de copia de seguridad y archivado, el cliente administrativo de línea de mandatos y el planificador de cliente

Especifique el puerto utilizando la opción **tcpport** en el archivo de opciones de cliente:

- Si no está utilizando el protocolo de capa de sockets seguros (SSL) para asegurar las comunicaciones, la opción **tcpport** del archivo de opciones de cliente debe coincidir con la opción **TCPPORT** en el archivo de opciones de servidor. El valor predeterminado es 1500. Si decide utilizar un valor que no sea el valor predeterminado, especifique un número en el rango 1024 - 32767.
- Si utiliza el protocolo SSL para las comunicaciones seguras, la opción de cliente **tcpport** debe coincidir con el valor de la opción de servidor **SSLTCPPORT**.

Puerto HTTP para habilitar la comunicación entre el cliente web y estaciones de trabajo remotas

Especifique el puerto para la estación de trabajo remota estableciendo la opción **httpport** en el archivo de opciones de cliente de la estación de trabajo remota. El valor predeterminado es 1581.

Puertos TCP/IP para la estación de trabajo remota

El valor predeterminado de 0 (cero) hace que los dos números de puerto libres se asignen aleatoriamente a la estación de trabajo remota. Si no desea que los números de puerto se asignen aleatoriamente, especifique valores estableciendo la opción **webports** en el archivos de opciones de cliente de la estación de trabajo remota.

Puerto TCP/IP para sesiones de administración

Especifique el puerto en el que el servidor espera las solicitudes para sesiones de cliente de administración:

- Si no está utilizando el protocolo SSL para proteger las comunicaciones, el valor de la opción **tcpadminport** de cliente debe coincidir con el valor de la opción de servidor **TCPADMINPORT**. De esta forma, puede asegurar las sesiones administrativas dentro de una red privada.
- Si está utilizando el protocolo SSL para proteger las comunicaciones, el valor de la opción **tcpadminport** de cliente debe coincidir con el valor de la opción **SSLTCPADMINPORT** de servidor.

Gestión de operaciones de cliente

Puede evaluar y resolver errores relacionados con un cliente de archivado y copia de seguridad utilizando Centro de operaciones, que proporciona sugerencias para resolver errores. Para errores en otros tipos de clientes, debe examinar los registros de errores en el cliente y revisar la documentación del producto.

Acerca de esta tarea

En algunos casos, puede resolver errores de cliente deteniendo e iniciando el aceptador de cliente. Si se han bloqueado los nodos cliente o los ID de administrador, puede solucionar el problema desbloqueando el nodo cliente o el ID de administrador y restableciendo después la contraseña.

Para obtener instrucciones detalladas sobre la identificación y resolución de errores de cliente, consulte Resolución de problemas relacionados con el cliente de IBM Spectrum Protect.

Evaluación de errores en registros de errores de cliente

Puede solucionar errores de cliente obteniendo sugerencias de Centro de operaciones o revisando los registros de errores en el cliente.

Antes de empezar

Para solucionar los errores de un cliente de archivado y copia de seguridad de un sistema operativo Linux o Windows, asegúrese de que servicio de gestión de clientes se haya instalado e iniciado. Para obtener instrucciones de instalación, consulte la publicación "Instalación del servicio de gestión de cliente" en la página 66. Para obtener instrucciones sobre cómo verificar la instalación, consulte "Verificación de que el servicio de gestión de clientes está instalado correctamente" en la página 67.

Procedimiento

Para diagnosticar y resolver errores de cliente, realice una de las siguientes acciones:

- Si servicio de gestión de clientes se ha instalado en el nodo cliente, lleve a cabo los siguientes pasos:
  1. En la página Descripción general de Centro de operaciones, pulse **Clientes** y seleccione el cliente.
  2. Pulse **Detalles**.
  3. En la página Resumen de cliente, pulse la pestaña **Diagnóstico**.
  4. Revise los mensajes de registro recuperados.

     Sugerencias:

     – Para mostrar u ocultar el panel Registros de clientes, efectúe una doble pulsación en la barra Registros de clientes.
     – Para cambiar el panel Registros de clientes, pulse y arrastre la barra Registros de clientes.

     Si se muestran sugerencias en la página Diagnóstico, seleccione una sugerencia. En el panel Registros de clientes, los mensajes de registro de clientes con los que se relaciona la sugerencia se resaltan.
  5. Utilice las sugerencias cuando resuelva los problemas indicados por los mensajes de error.

     Consejo: Solo se proporcionan sugerencias para un subconjunto de mensajes de cliente.
- Si servicio de gestión de clientes no se ha instalado en el nodo cliente, revise los registros de errores del cliente instalado.

Detención y reinicio del aceptador de cliente

Si cambia la configuración de la solución, debe reiniciar el aceptador de cliente en todos los nodos de cliente donde está instalado el cliente de archivado y copia de seguridad.

Acerca de esta tarea

En algunos casos, puede resolver los problemas de planificación de cliente deteniendo y reiniciando el aceptador de cliente. El aceptador de cliente debe estar en ejecución para asegurarse de que las operaciones planificadas se pueden producir en el cliente. Por ejemplo, si cambia la dirección IP o el nombre de dominio del servidor, debe reiniciar el aceptador de cliente.

Procedimiento

Siga las instrucciones del sistema operativo que esté instalado en el nodo cliente:

AIX y Oracle Solaris

- Para detener el aceptador de cliente, complete los pasos siguientes:
  1. Determine el ID de proceso para el aceptador de cliente emitiendo el mandato siguiente en la línea de mandatos:

     ```
     ps -ef | grep dsmcad
     ```

     Revise la salida. En la salida de ejemplo siguiente, 6764 es el ID de proceso para el aceptador de cliente:

     ```
     root  6764     1   0 16:26:35 ?           0:00 /usr/bin/dsmcad
     ```
  2. Emita el siguiente mandato en la línea de mandatos:

     ```
     kill -9 PID
     ```

     donde *PID* especifica el ID de proceso para el aceptador de cliente.
- Para iniciar el aceptador de cliente, emita el mandato siguiente en la línea de mandatos:

  ```
  /usr/bin/dsmcad
  ```

Linux

- Para detener el aceptador de cliente (y no reiniciarlo), emita el mandato siguiente:

  ```
  # service dsmcad stop
  ```
- Para detener y reiniciar el aceptador de cliente, emita el mandato siguiente:

  ```
  # service dsmcad restart
  ```

MAC OS X

Pulse **Aplicaciones** > **Programas de utilidad** > **Terminal**.

- Para detener el aceptador de cliente, emita el mandato siguiente:

  ```
  /bin/launchctl unload -w com.ibm.tivoli.dsmcad
  ```
- Para iniciar el aceptador de cliente, emita el mandato siguiente:

  ```
  /bin/launchctl load -w com.ibm.tivoli.dsmcad
  ```

Windows

- Para detener el servicio aceptador de cliente, complete los pasos siguientes:
  1. Pulse **Inicio** > **Herramientas administrativas** > **Servicios**.

2. Efectúe doble pulsación en el servicio aceptador de cliente.
3. Pulse **Detener** y **Aceptar**.

- Para reiniciar el servicio aceptador de cliente, complete los pasos siguientes:
  1. Pulse **Inicio** > **Herramientas administrativas** > **Servicios**.
  2. Efectúe doble pulsación en el servicio aceptador de cliente.
  3. Pulse **Iniciar** y **Aceptar**.

Referencia relacionada:

Resolución de problemas de planificación del cliente

Restablecimiento de contraseñas

Si se pierde la contraseña de un nodo cliente o un ID de administrador, podrá restablecerla. Varios intentos de acceso al sistema con una contraseña incorrecta pueden ocasionar el bloqueo del nodo cliente o del ID de administrador. Puede tomar medidas para resolver el problema.

Procedimiento

Para resolver problemas de contraseña, realice una de las siguientes acciones:

- Si se ha instalado un cliente de archivado y copia de seguridad en un nodo cliente, y se pierde la contraseña o se olvida, realice los siguientes pasos:
  1. Genere una nueva contraseña ejecutando el mandato **UPDATE NODE**:
     ```
     update node nombre_nodo nueva_contraseña forcepwreset=yes
     ```
     donde *nombre_nodo* especifica el nodo cliente y *nueva_contraseña* especifica la contraseña que asigne.
  2. Informe al propietario del nodo cliente sobre la contraseña modificada. Cuando el propietario del nodo cliente inicie sesión con la contraseña especificado, se generará automáticamente una contraseña nueva. Esta contraseña es desconocida para los usuarios a fin de mejorar la seguridad.

     Consejo: La contraseña se genera automáticamente si ha definido previamente la opción **passwordaccess** como `generar` en el archivo de opciones del cliente.
- Si se bloquea a un administrador por problemas con la contraseña, realice lo siguiente:
  1. Para proporcionar acceso al administrador al servidor, ejecute el mandato **UNLOCK ADMIN**. Para obtener instrucciones, consulte UNLOCK ADMIN (Desbloquear un administrador).
  2. Configure una contraseña nueva utilizando el mandato **UPDATE ADMIN**:
     ```
     update admin nombre_admin nueva_contraseña forcepwreset=yes
     ```
     donde *admin* especifica el nombre del administrador y *nueva_contraseña* especifica la contraseña que asigne.
- Si se bloquea un nodo cliente, lleve a cabo los siguientes pasos:
  1. Determine la causa del bloqueo y si es necesario desbloquearlo. Por ejemplo, si el nodo cliente está fuera de servicio, se elimina del entorno de producción. No se puede revertir la operación de fuera de servicio y el nodo cliente permanece bloqueado. También se puede bloquear un nodo cliente si los datos del cliente están sujetos a una investigación judicial.

2. Si necesita desbloquear un nodo cliente, utilice el mandato **UNLOCK NODE**. Para obtener instrucciones, consulte UNLOCK NODE (Desbloquear un nodo de cliente).
3. Genere una nueva contraseña ejecutando el mandato **UPDATE NODE**:

   ```
   update node nombre_nodo nueva_contraseña forcepwreset=yes
   ```

   donde *nombre_nodo* especifica el nombre del nodo y *nueva_contraseña* especifica la contraseña que asigne.
4. Informe al propietario del nodo cliente sobre la contraseña modificada. Cuando el propietario del nodo cliente inicie sesión con la contraseña especificado, se generará automáticamente una contraseña nueva. Esta contraseña es desconocida para los usuarios a fin de mejorar la seguridad.

   Consejo: La contraseña se genera automáticamente si ha definido previamente la opción **passwordaccess** como `generar` en el archivo de opciones del cliente.

Modificación del ámbito de una copia de seguridad de cliente

Al configurar operaciones de copia de seguridad de cliente, se recomienda que excluya los objetos que no necesite. Por ejemplo, normalmente deseará excluir archivos temporales de una operación de copia de seguridad.

Acerca de esta tarea

Al excluir objetos innecesarios de las operaciones de copia de seguridad, puede obtener mejor control de la cantidad de espacio de almacenamiento que se necesita para las operaciones de copia de seguridad y el coste de almacenamiento. En función de su paquete de licencia, también podrá reducir los costes de licencia.

Procedimiento

Cómo modificar el ámbito de las operaciones de copia de seguridad depende del producto que está instalado en el nodo de cliente:

- Para un cliente de archivado y copia de seguridad, puede crear una lista de inclusión-exclusión para incluir o excluir un archivo, grupos de archivos o directorios de las operaciones de copia de seguridad. Para crear una lista de inclusión-exclusión, siga las instrucciones en Creación de una lista de inclusión-exclusión.

  Para asegurar la coherencia de uso de una lista de inclusión/exclusión de todos los clientes de un tipo, puede crear un conjunto de opciones de cliente en el servidor que contiene las opciones necesarias. A continuación, asigne el conjunto de opciones de cliente a cada uno de los clientes del mismo tipo. Si desea obtener más información al respecto, consulte el apartado Control de las operaciones de cliente mediante conjuntos de opciones de cliente.
- Para un cliente de archivado y copia de seguridad, puede especificar los objetos que desea incluir en una operación de copia de seguridad incremental utilizando la opción **dominio**. Siga las instrucciones de Opción de cliente Domain.
- Para otros productos, para definir qué objetos se incluyen y se excluyen en las operaciones de copia de seguridad, sigas las instrucciones de la documentación del producto.

Gestión de actualizaciones del cliente

Cuando hay disponible un fixpack o arreglo temporal, puede actualizar el servidor para sacar provecho de las mejoras del producto. Los servidores y clientes se pueden actualizar en momentos diferentes y pueden estar a distintos niveles con algunas restricciones.

Antes de empezar

1. Revise los requisitos de compatibilidad cliente/servidor en nota técnica 1053218. Si la solución incluye servidores o clientes en un nivel anterior a V7.1, revise las directrices para asegurarse de que las operaciones de archivado y copia de seguridad de cliente no se vean afectadas.
2. Verifique los requisitos del sistema para el cliente en Sistemas operativos admitidos para IBM Spectrum Protect.
3. Si la solución incluye agentes de almacenamiento o clientes de biblioteca, revise la información sobre la compatibilidad de agente de almacenamiento y cliente de biblioteca con los servidores que se configuran como gestores de biblioteca. Consulte el apartado nota técnica 1302789.

   Si tiene pensado actualizar un gestor de biblioteca y un cliente de biblioteca, debe actualizar el gestor de biblioteca primero.

Procedimiento

Para actualizar el software, siga las instrucciones que se muestran en la tabla siguiente.

Software	Enlace a instrucciones
Cliente de copia de seguridad/archivado de IBM Spectrum Protect	• Actualización del cliente de archivado y copia de seguridad
IBM Spectrum Protect Snapshot	• Instalación y actualización de IBM Spectrum Protect Snapshot para UNIX y Linux • Instalación y actualización de IBM Spectrum Protect Snapshot for VMware • Instalación y actualización de IBM Spectrum Protect Snapshot for Windows
IBM Spectrum Protect for Databases	• Actualización de Data Protection for SQL Server • Instalación de Data Protection for Oracle • Instalación, actualización y migración de IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server
IBM Spectrum Protect for Enterprise Resource Planning	• Actualización de IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP for DB2 • Actualización de IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP for Oracle
IBM Spectrum Protect for Mail	• Instalación de Data Protection for IBM Domino en un sistema UNIX, AIX o Linux (V7.1.0) • Instalación de Data Protection for IBM Domino en un sistema Windows (V7.1.0) • Instalación, actualización y migración de IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server
IBM Spectrum Protect for Virtual Environments	• Instalación y actualización de Data Protection for VMware • Instalación de Data Protection for Microsoft Hyper-V

Poner fuera de servicio un nodo cliente

Si ya no se necesita un nodo cliente, puede iniciar un proceso para eliminarlo del entorno de producción. Por ejemplo, si una estación de trabajo estaba haciendo una copia de seguridad de datos en el servidor de IBM Spectrum Protect, pero la estación de trabajo ya no se utiliza, puede ponerla fuera de servicio.

Acerca de esta tarea

Cuando inicia el proceso para poner el servidor fuera de servicio, éste bloquea el nodo cliente para impedir que acceda al servidor. Los archivos que pertenecen al nodo cliente se suprimen gradualmente y, a continuación, el nodo cliente se suprime. Puede poner fuera de servicio los siguientes tipos de nodo cliente:

Nodos de cliente de aplicaciones
Los nodos de cliente de aplicaciones incluyen servidores de correo electrónico, bases de datos y otras aplicaciones. Por ejemplo, cualquiera de las siguientes aplicaciones puede ser un nodo cliente de aplicaciones:

- IBM Spectrum Protect Snapshot
- IBM Spectrum Protect for Databases
- IBM Spectrum Protect for Enterprise Resource Planning
- IBM Spectrum Protect for Mail
- IBM Spectrum Protect for Virtual Environments

Nodos de cliente de sistemas
Los nodos de cliente de sistemas incluyen estaciones de trabajo, servidores de archivos de almacenamiento adjunto a red (NAS) y clientes de API.

Nodos de cliente de máquina virtual
Los nodos de cliente de máquina virtual constan de un host invitado individual dentro de un hipervisor. Cada máquina virtual se representa como un espacio de archivos.

El método más sencillo para poner fuera de servicio un nodo cliente es utilizar Centro de operaciones. El procese de poner fuera de servicio se ejecuta en segundo plano. Si el cliente está configurado para replicar datos de cliente, Centro de operaciones elimina automáticamente el cliente de la réplica en los servidores de réplica de origen y de destino antes de que ponga fuera de servicio al cliente.

Consejo: De forma alternativa, puede poner fuera de servicio un nodo cliente emitiendo el mandato **DECOMMISSION NODE** o **DECOMMISSION VM**. Es posible que desee utilizar este método en los casos siguientes:

- Para planificar el proceso de poner fuera de servicio en un futuro o para ejecutar una serie de mandatos utilizando un script, especifique el proceso de poner fuera de servicio para ejecutarlo en segundo plano.
- Para supervisar el proceso de poner fuera de servicio para fines de depuración, especifique el proceso de poner fuera de servicio para ejecutarlo en primer plano. Si ejecuta el proceso en primer plano, debe esperar a que se complete el proceso antes de continuar con otras tareas.

Procedimiento

Realice una de las siguientes acciones:

- Para poner fuera de servicio un cliente en segundo plano utilizando Centro de operaciones, complete los pasos siguientes:

1. En la página de Centro de operaciones Visión general, pulse **Clientes** y seleccione el cliente.
2. Pulse **Más** > **Poner fuera de servicio**.

- Para que un nodo cliente quede fuera de servicio utilizando un mandato administrativo, realice una de las siguientes acciones:
  - Para poner fuera de servicio un nodo cliente del sistema o de la aplicación, emita el mandato **DECOMMISSION NODE**. Por ejemplo, si el nodo cliente se denomina AUSTIN, emita el siguiente mandato:

    ```
    decommission node austin
    ```

  - Para poner fuera de servicio un nodo cliente del sistema o de la aplicación en primer plano, emita el mandato **DECOMMISSION NODE** y especifique el parámetro `wait=yes`. Por ejemplo, si el nodo cliente se denomina AUSTIN, emita el siguiente mandato:

    ```
    decommission node austin wait=yes
    ```

  - Para poner fuera de servicio una máquina virtual en segundo plano, emita el mandato **DECOMMISSION VM**. Por ejemplo, si la máquina virtual se denomina AUSTIN, el espacio de archivos es 7 y el nombre de espacio de archivos se especifica por el ID de espacio de archivos, emita el siguiente mandato:

    ```
    decommission vm austin 7 nametype=fsid
    ```

    Si el nombre de la máquina virtual incluye uno o más espacios, especifique el nombre entre comillas dobles. Por ejemplo:

    ```
    decommission vm "austin 2" 7 nametype=fsid
    ```

  - Para poner fuera de servicio una máquina virtual en primer plano, emita el mandato **DECOMMISSION VM** y especifique el parámetro `wait=yes`. Por ejemplo, emita el siguiente comando:

    ```
    decommission vm austin 7 nametype=fsid wait=yes
    ```

    Si el nombre de la máquina virtual incluye uno o más espacios, especifique el nombre entre comillas dobles. Por ejemplo:

    ```
    decommission vm "austin 2" 7 nametype=fsid wait=yes
    ```

Qué hacer a continuación

Tenga en cuenta los mensajes de error, que se pueden mostrar en la interfaz de usuario o en la salida de mandatos, inmediatamente después de ejecutar el proceso.

Puede verificar que el nodo de cliente esté fuera de servicio:

1. En la página de Centro de operaciones Visión general, pulse **Clientes**.
2. En la tabla Clientes, en la columna En riesgo, revise el estado:
   - Un estado DECOMMISSIONED especifica que el nodo está fuera de servicio.
   - Un valor null especifica que el nodo no está fuera de servicio.
   - Un estado PENDING especifica que el nodo se está dejando fuera de servicio, o que el proceso de dejar fuera de servicio ha fallado.

   Consejo: Si desea determinar el estado de un proceso de invalidación pendiente, emita el mandato siguiente:

   ```
   proceso de consulta
   ```

3. Revise la salida del mandato:
   - Si se proporciona el estado para el proceso de invalidación, el proceso estará en curso. Por ejemplo:

```
proceso de consulta

 Proceso     Descripción proceso           Estado proceso
  proceso
--------     --------------------     ------------------------------------------

3            DECOMMISSION NODE        Número de objetos de copia de seguridad
                                      desactivados para el nodo NODE1: 8
                                      objetos desactivados.
```

- Si no se proporciona ningún estado para el proceso de invalidación, y si no ha recibido ningún mensaje de error, el proceso estará incompleto. Un proceso puede estar incompleto si los archivos asociados con el nodo no están aún desactivados. Una vez que se desactiven los archivos, ejecute el proceso de invalidación de nuevo.
- Si no se proporciona ningún estado para el proceso de invalidación, y si recibe un mensaje de error, el proceso fallará. Ejecute el proceso de invalidación de nuevo.

Referencia relacionada:

DECOMMISSION NODE (Poner fuera de servicio un nodo de cliente)

DECOMMISSION VM (Poner fuera de servicio una máquina virtual)

Desactivación de datos para liberar espacio de almacenamiento

En algunos casos, puede desactivar los datos que se almacenan en el servidor de IBM Spectrum Protect. Cuando ejecuta el proceso de desactivación, los datos de seguridad almacenados antes de la fecha y hora especificadas se desactivan y se suprimirán cuando caduca. De este modo, puede liberar espacio en el servidor.

Acerca de esta tarea

Algunos clientes de aplicaciones siempre guardan datos en el servidor como datos de copia de seguridad activos. Puesto que los datos de copia de seguridad activos no están gestionados por las políticas de caducidad de inventario, los datos no se suprimen automáticamente y utilizan el espacio de almacenamiento del servidor de forna indefinida. Para liberar el espacio de almacenamiento utilizado por datos obsoletos, puede desactivar los datos.

Cuando ejecute el proceso de desactivación, todos los datos de copia de seguridad activos almacenados antes de la fecha especificada pasan a inactivos. Los datos se suprimen cuando caducan y no se pueden restaurar. La característica de desactivación se aplica solo a clientes de aplicación que protegen bases de datos de Oracle.

Procedimiento

1. En la página Descripción general de Centro de operaciones, pulse **Clientes**.
2. En la tabla Clientes, seleccione uno o más clientes y pulse **Más** > **Borrar**.

Método de línea de mandatos: Desactive los datos utilizando el mandato **DEACTIVATE DATA**.

Referencia relacionada:

DEACTIVATE DATA (Desactivar datos para un nodo de cliente)

Capítulo 17. Gestión del almacenamiento de datos

Gestione los datos para la eficiencia y añada dispositivos y soportes compatibles al servidor para almacenar datos de cliente.

Referencia relacionada:

Comparación de agrupaciones de almacenamiento

Auditoría de un contenedor de la agrupación de almacenamiento

Audite un contenedor de agrupación de almacenamiento para comprobar si hay incoherencias entre información de base de datos y un contenedor en una agrupación de almacenamiento.

Acerca de esta tarea

Audita un contenedor de la agrupación de almacenamiento en las siguientes situaciones:

- Cuando emite el mandato **QUERY DAMAGED** y se detecta un problema.
- Cuando el servidor muestra mensajes sobre extensiones de datos dañadas.
- El hardware informa de un problema y se visualizan mensajes de error asociados con el contenedor de la agrupación de almacenamiento.

Procedimiento

1. Para auditar un contenedor de la agrupación de almacenamiento, emita el mandato **AUDIT CONTAINER**. Por ejemplo, emita el siguiente mandato para auditar un contenedor, `000000000000076c.dcf`:

   ```
   audit container c:\tsm-storage\07\000000000000076c.dcf
   ```

2. Revise la salida del mensaje ANR4891I para obtener información sobre cualquier extensión de datos dañada.

Qué hacer a continuación

Si detecta problemas con el contenedor de la agrupación de almacenamiento, puede restaurar datos basándose en la configuración. Emita el mandato **AUDIT CONTAINER** y especifique el nombre del contenedor.

Referencia relacionada:

AUDIT CONTAINER (Verificar la coherencia de la información de base de datos para una agrupación de almacenamiento de contenedores de directorio)

QUERY DAMAGED (Consultar los datos dañados de una agrupación de almacenamiento de contenedores de directorios o de contenedores de nube)

Gestión de la capacidad de inventario

Gestione la capacidad de la base de datos, del registro activo y de los registros de archivado para asegurarse de que el inventario se dimensiona para las tareas, basándose en el estado de los registros.

Antes de empezar

Los registros activos y de archivado tienen las siguientes características:

- El registro activo puede tener un tamaño máximo de 512 GB. Para obtener más información sobre el dimensionamiento del registro activo para su sistema, consulte Planificación de matrices de almacenamiento.
- El tamaño del registro de archivado está limitado al tamaño del sistema de archivos en el que está instalado. El tamaño del registro de archivado no se mantiene a un tamaño predefinido como el registro activo. Los archivos de registro de archivado se suprimen automáticamente cuando ya no son necesarios.

Como práctica recomendada, puede crear opcionalmente un registro de migración tras error de archivado para almacenar archivos de registro de archivado cuando el directorio de registro de archivado está lleno.

Compruebe Centro de operaciones para determinar el componente del inventario que está lleno. Asegúrese de que detiene el servidor antes de aumentar el tamaño de uno de los componentes de inventario.

Procedimiento

- Para aumentar el tamaño de la base de datos, complete los pasos siguientes:
  - Cree uno o más directorios para la base de datos en unidades o sistemas de archivos individuales.
  - Emita el mandato **EXTEND DBSPACE** para agregar uno o varios directorios a la base de datos. Los directorios deben ser accesibles para el ID de usuario de instancia del gestor de bases de datos. De forma predeterminada, los datos se redistribuyen entre todos los directorios de bases de datos y se reclama el espacio.

    Sugerencias:

    - El tiempo necesario para completar la redistribución de datos y reclamar el espacio es variable, dependiendo del tamaño de la base de datos. Asegúrese de que lo ha planeado adecuadamente.
    - Asegúrese de que los directorios que especifique tienen el mismo tamaño que los directorios existentes para garantizar un grado coherente de paralelismo para las operaciones de la base de datos. Si uno o más directorios de la base de datos son más pequeños que los demás, reducen el potencial de precarga y distribución en paralelo optimizada de la base de datos.
  - Detenga y reinicie e servidor para utilizar completamente los nuevos directorios.
  - Reorganice la base de datos si es necesario. La reorganización de los índices y de las tabas de la base de datos del servidor puede contribuir a impedir que la base de datos aumente de forma inesperada o problemas de rendimiento. Para obtener más información sobre cómo reorganizar la base de datos, consulte nota técnica 1683633.

- Para disminuir el tamaño de la base de datos para servidores V7.1 y posterior, emita los siguientes mandatos de DB2 desde el directorio de instancias de servidor:

  Restricción: Los mandatos pueden aumentar la actividad de E/S, y puede afectar al rendimiento del servidor. Para minimizar los problemas de rendimiento, espere hasta que se complete un mandato antes de emitir el siguiente. Los mandatos DB2 se pueden emitir cuando el servidor está en ejecución.

  ```
  db2 connect to tsmdb1
  db2 set schema tsmdb1
  db2 ALTER TABLESPACE USERSPACE1 REDUCE MAX
  db2 ALTER TABLESPACE IDXSPACE1 REDUCE MAX
  db2 ALTER TABLESPACE LARGEIDXSPACE1 REDUCE MAX
  db2 ALTER TABLESPACE LARGESPACE1 REDUCE MAX
  db2 ALTER TABLESPACE REPLTBLSPACE1 REDUCE MAX
  db2 ALTER TABLESPACE REPLIDXSPACE1 REDUCE MAX
  db2 ALTER TABLESPACE ARCHOBJDATASPACE REDUCE MAX
  db2 ALTER TABLESPACE ARCHOBJIDXSPACE REDUCE MAX
  db2 ALTER TABLESPACE BACKOBJDATASPACE REDUCE MAX
  db2 ALTER TABLESPACE BACKOBJIDXSPACE REDUCE MAX
  db2 ALTER TABLESPACE BFABFDATASPACE REDUCE MAX
  db2 ALTER TABLESPACE BFABFIDXSPACE REDUCE MAX
  db2 ALTER TABLESPACE BFBFEXTDATASPACE REDUCE MAX
  db2 ALTER TABLESPACE BFBFEXTIDXSPACE REDUCE MAX
  db2 ALTER TABLESPACE DEDUPTBLSPACE1 REDUCE MAX
  db2 ALTER TABLESPACE DEDUPIDXSPACE1 REDUCE MAX
  db2 ALTER TABLESPACE DEDUPTBLSPACE2 REDUCE MAX
  db2 ALTER TABLESPACE DEDUPIDXSPACE2 REDUCE MAX
  db2 ALTER TABLESPACE DEDUPTBLSPACE3 REDUCE MAX
  db2 ALTER TABLESPACE DEDUPIDXSPACE3 REDUCE MAX
  db2 ALTER TABLESPACE DEDUPTBLSPACE4 REDUCE MAX
  db2 ALTER TABLESPACE DEDUPIDXSPACE4 REDUCE MAX
  db2 ALTER TABLESPACE DEDUPTBLSPACE5 REDUCE MAX
  db2 ALTER TABLESPACE DEDUPIDXSPACE5 REDUCE MAX
  ```

- Para aumentar o disminuir el tamaño del registro activo, complete los pasos siguientes:
  1. Asegúrese de que la ubicación de las anotaciones activas tenga espacio suficiente para el tamaño de anotaciones mayor. Si existe una duplicación de anotaciones, su ubicación también debe tener espacio suficiente para el tamaño de anotaciones mayor.
  2. Detenga el servidor.
  3. En el archivo `dsmserv.opt`, actualice la opción **`ACTIVELOGSIZE`** para el nuevo tamaño del registro activo, en megabytes.

     El tamaño de un archivo de registro activo se basa en el valor de la opción `ACTIVELOGSIZE`. En la tabla siguiente se muestran las directrices de los requisitos de espacio:

Tabla 17. Cómo calcular el volumen y los requisitos de espacio de archivos

Valor de la opción `ACTIVELOGSize`	**Reserve esta cantidad de espacio libre en el directorio de registros activos, ademas del espacio de `ACTIVELOGSize`**
2 GB - 128 GB	5120 MB
129 GB - 256 GB	10240 MB
257 GB - 512 GB	20480 MB

     Para cambiar el registro activo a su tamaño máximo de 512 GB, entre la siguiente opción de servidor:

```
activelogsize 524288
```

4. Si piensa utilizar un nuevo directorio de registro activo, actualice el nombre de directorio especificado en la opción de servidor **ACTIVELOGDIRECTORY**. El nuevo directorio debe estar vacío y debe ser accesible para el ID de usuario del gestor de base de datos.
5. Reinicie el servidor.

- Comprima los registros de archivado para reducir la cantidad de espacio necesaria para el almacenamiento. Habilite la compresión dinámica del registro de archivado emitiendo el mandato siguiente:

  ```
  setopt archlogcompress yes
  ```

  Restricción: Preste atención cuando habilite la opción **ARCHLOGCOMPRESS** en sistemas con un alto volumen de utilización sostenido y mucha carga de trabajo. Si esta opción se habilita en este entorno del sistema pueden producirse retardos en el archivado de los archivos de registro de archivado desde el sistema de archivos de registro activos al sistema de archivos de registro de archivado. Este retardo puede provocar que el sistema de archivos de registro activos se quede sin espacio. Asegúrese de supervisar el espacio disponible en el sistema de archivos de registro activos después de habilitar la comprensión de archivos de registro. Si el uso sistema de archivos del directorio de registro activo está alcanzando condiciones de falta de espacio, se debe inhabilitar la opción del servidor **ARCHLOGCOMPRESS**. Puede utilizar el mandato **SETOPT** para inhabilitar la comprensión del registro de archivado de forma inmediata sin detener el servidor.

Referencia relacionada:

ACTIVELOGSIZE, opción de servidor

EXTEND DBSPACE (Incrementar el espacio para la base de datos)

SETOPT (Establecer una opción de servidor para actualización dinámica)

Gestión del uso de la memoria y del procesador

Asegúrese de que gestiona requisitos de memoria y el uso de procesador para garantizar que el servidor puede completar procesos de datos como, por ejemplo, la copia de datos y la deduplicación de datos. Tenga en cuenta el impacto sobre el rendimiento cuando complete determinados procesos.

Antes de empezar

- Asegúrese de que la configuración utiliza el hardware y el software necesarios. Para obtener más información, consulte Sistemas operativos admitidos para IBM Spectrum Protect.
- Para obtener más información acerca de la gestión de recursos como la base de datos y registro de recuperación, consulte Planificación de matrices de almacenamiento.
- Añada más memoria del sistema para determinar si hay una mejora de rendimiento. Supervise con regularidad el uso de la memoria para determinar si se necesita más.

Procedimiento

1. Libere memoria de la memoria caché de sistema de archivo donde sea posible.
2. Para gestionar la memoria del sistema utilizada para cada servidor en un sistema, utilice la opción de servidor DBMEMPERCENT. Limite el porcentaje de memoria del sistema que puede utilizar el gestor de bases de datos de cada

servidor. Si todos los servidores tienen igual importancia, utilice el mismo valor para cada servidor. Si un servidor es de producción y hay otros de prueba, establezca para el servidor de producción un valor más alto que para los de prueba.

3. Establezca el límite de datos de usuario y la memoria privada para la base de datos para asegurarse de que la memoria privada no se ha agotado. Agotar la memoria privada puede provocar errores e inestabilidad, en lugar de un rendimiento óptimo.

Ajuste de actividades planificadas

Planificar tareas de mantenimiento a diario para asegurarse de que su solución funciona correctamente. Ajustando la solución, se maximizan los recursos del servidor y se utilizan de forma eficaz distintas funciones disponibles en la solución.

Procedimiento

1. Supervise el rendimiento de sistema de forma periódica para asegurarse de que las tareas de copia de seguridad y mantenimiento se completan correctamente. Para obtener más información sobre supervisión, consulte Parte 3, “Supervisión de una solución de disco de sitio único”, en la página 73.
2. Si la información de supervisión muestra que la carga de trabajo del servidor ha aumentado, tal vez tenga que revisar la información de planificación. Revise si la capacidad del sistema es adecuada en los casos siguientes:
   - El número de clientes aumenta.
   - La cantidad de datos de los que se hace copia de seguridad aumenta.
   - La cantidad de tiempo necesaria disponible para realizar copias de seguridad cambia.
3. Determine si la solución tiene problemas de rendimiento. Revise las planificaciones de cliente para comprobar si las tareas se completan en el intervalo de tiempo planificado:
   a. En la página **Clientes** del Centro de operaciones, seleccione el cliente.
   b. Pulse **Detalles**.
   c. Desde la página de Resumen, revise la actividad de **Copiado** y **Replicado** para identificar los riesgos.

   Ajuste el tiempo y la frecuencia de las operaciones de copia de seguridad de cliente, si es necesario.
4. Planifique tiempo suficiente para que las siguientes tareas de mantenimiento se completen satisfactoriamente en un periodo de 24 horas:
   a. Copia de seguridad de la base de datos
   b. Ejecutar la caducidad para eliminar las copias de seguridad de cliente y las copias de archivo de archivado del almacenamiento de servidor.

Conceptos relacionados:

Rendimiento

Tareas relacionadas:

Deduplicación de datos (V7.1.1)

Capítulo 18. Protección del servidor IBM Spectrum Protect

Proteja el servidor IBM Spectrum Protect y los datos controlando el acceso a servidores y nodos de cliente, cifrando datos y manteniendo niveles de acceso seguros y contraseñas.

Conceptos sobre la seguridad

Puede proteger IBM Spectrum Protect de riesgos de seguridad utilizando protocolos de comunicación, contraseñas de seguridad y proporcionando diferentes niveles de acceso para administradores.

Seguridad de la capa de transporte

Puede utilizar el protocolo de Capa de sockets seguros (SSL) o de Seguridad de la capa de transporte (TLS) para proporcionar seguridad de la capa de transporte para una conexión segura entre servidores, clientes y agentes de almacenamiento. Si envía datos entre el servidor el cliente y el agente de almacenamiento, utilice SSL o TLS para cifrar los datos.

Consejo: Toda la documentación de IBM Spectrum Protect que indique "SSL" o "seleccionar SSL" se aplica a TLS.

SSL se proporciona mediante el Global Security Kit (GSKit) que se instala con el servidor de IBM Spectrum Protect que utilizan el servidor, el cliente y el agente de almacenamiento.

Restricción: No utilice los protocolos SSL o TLS para las comunicaciones con una instancia de base de datos de DB2 utilizada por los servidores de IBM Spectrum Protect.

Cada servidor, cliente o agente de almacenamiento que habilita SSL debe utilizar un certificado autofirmado de confianza u obtener un certificado exclusivo que esté firmado por una entidad emisora de certificados (CA). Puede utilizar sus propios certificados o adquirir certificados de una CA. Cada certificado debe instalarse y añadirse a la base de datos de claves en el servidor, cliente o agente de almacenamiento de IBM Spectrum Protect. El certificado se verifica por medio del servidor o cliente de SSL que solicita o inicia la comunicación SSL. Algunos certificados CA están preinstalados de forma predeterminada en las bases de datos de claves.

SSL se configura de forma independiente en el agente de almacenamiento, el cliente o en el servidor de IBM Spectrum Protect.

Niveles de autorización

Con cada servidor de IBM Spectrum Protect, hay diferentes niveles de autoridad administrativa disponibles que determinan las tareas que un administrador puede realizar.

Después de registrarse, el administrador debe tener autorización para que se le asignen uno o más niveles de autoridad administrativa. Un administrador con autoridad del sistema puede completar cualquier tarea con el servidor y asignar

niveles de autorización a otros administradores utilizando el mandato **GRANT AUTHORITY**. Los administradores con autoridad de política, almacenamiento u operador pueden completar subconjuntos de tareas.

Un administrador puede registrar otros ID de administrador, otorgarles niveles de autoridad, renombrarlos, eliminarlos y bloquearlos y desbloquearlos desde el servidor.

Un administrador puede controlar el acceso a nodos de cliente específicos para ID de usuario root e ID de usuario no root. De forma predeterminada, un ID de usuario no root no puede hacer copia de seguridad de los datos en el nodo. Utilice el mandato **UPDATE NODE** para cambiar los valores de nodo para habilitar la copia de seguridad.

Contraseñas

De forma predeterminada, el servidor utiliza automáticamente la autenticación de contraseña. Con la autenticación de contraseña, todos los usuarios deben especificar una contraseña al acceder al servidor.

Utilice Lightweight Directory Access Protocol (LDAP) para aplicar requisitos más estrictos para las contraseñas. Para obtener más información, consulte Gestión de contraseñas y procedimientos de inicio de sesión (V7.1.1).

Tabla 18. Características de la autenticación de contraseña

Característica	Más información
Distinción entre mayúsculas y minúsculas	No distingue entre mayúsculas y minúsculas.
Caducidad de la contraseña predeterminada	90 días. El período de caducidad se inicia cuando un ID de administrador o nodo cliente se inscribe por primera vez en el servidor. Si no se cambia la contraseña de usuario dentro de este período, el usuario deberá cambiar la contraseña la próxima vez que acceda al servidor.
Intentos de contraseña no válidos	Puede establecer un límite de intentos consecutivos no válidos de entrada de contraseña para todos los nodos cliente. Si se supera el límite, el servidor bloquea el nodo.
Longitud de la contraseña	El administrador puede especificar una longitud mínima de contraseña necesaria para las contraseñas.

Tareas relacionadas:

Protección de las comunicaciones

Gestión de administradores

Un administrador que tiene autorización del sistema puede completar cualquier tarea con el servidor de IBM Spectrum Protect, incluida la asignación de niveles de autorización a otros administradores. Para completar algunas tareas, se le debe otorgar autorización asignándole uno o más niveles de autorización.

Procedimiento

Complete las siguientes tareas para modificar los valores de administrador.

Tarea	Procedimiento

Añada un administrador.	Para añadir un administrador, ADMIN1, con autoridad del sistema y especificar una contraseña, lleve a cabo lo siguiente:
	1. Registre el administrador y especifique **Pa$#$twO** como contraseña ejecutando el siguiente mandato:
	`register admin admin1 Pa$#$twO`
	2. Ejecute el siguiente mandato para proporcionar autoridad del sistema al administrador:
	`grant authority admin1 classes=system`

Cambie los permisos del administrador.	Cambie el nivel de autorización de un administrador, ADMIN1.
	• Ejecute el siguiente mandato para proporcionar autoridad del sistema al administrador:
	`grant authority admin1 classes=system`
	• Emita el siguiente mandato para revocar la autoridad del sistema del administrador:
	`revoke authority admin1 classes=system`

Elimine administradores.	Ejecute el siguiente mandato para eliminar el acceso del administrador, ADMIN1, al servidor de IBM Spectrum Protect: `remove admin admin1`
Impida el acceso al servidor de forma temporal.	Utilice el mandato **LOCK ADMIN** o **UNLOCK ADMIN** para bloquear o desbloquear a un administrador.

Cambio de los requisitos de contraseña

Puede cambiar el límite mínimo de contraseña, la longitud de la contraseña, la caducidad de la contraseña y habilitar o inhabilitar la autenticación para IBM Spectrum Protect.

Acerca de esta tarea

Imponiendo la autenticación de contraseña y gestionando las restricciones de contraseña, protege los datos y los servidores de posibles riesgos de seguridad.

Procedimiento

Complete las siguientes tareas para cambiar los requisitos de contraseña para los servidores IBM Spectrum Protect.

Tabla 19. Tareas de autenticación para servidores IBM Spectrum Protect

Tarea	Procedimiento
Establecer un límite de intentos de contraseña no válidos.	1. En la página Servidores del Centro de operaciones, seleccione el servidor. 2. Pulse **Detalles** y, a continuación, haga clic en el separador **Propiedades**. 3. Establezca el número de intentos no válidos en el campo **Límite de intentos de inicio de sesión no válidos**. El valor predeterminado en la instalación es 0.
Establezca una longitud mínima para las contraseñas.	1. En la página Servidores del Centro de operaciones, seleccione el servidor. 2. Pulse **Detalles** y, a continuación, pulse el separador **Propiedades**. 3. Establezca el número de caracteres en el campo **Longitud de contraseña mínima**.
Establezca el periodo de caducidad para las contraseñas.	1. En la página Servidores del Centro de operaciones, seleccione el servidor. 2. Pulse **Detalles** y, a continuación, pulse el separador **Propiedades**. 3. Establecer el número de días en el campo **Caducidad común de la contraseña**.
Inhabilitar la autenticación de contraseña.	De forma predeterminada, el servidor utiliza automáticamente la autenticación de contraseña. Con la autenticación de contraseña, todos los usuarios deben especificar una contraseña para acceder al servidor. Puede inhabilitar la autenticación de contraseña sólo para las contraseñas que se autentican en el servidor (LOCAL). Al inhabilitar la autenticación de contraseña, se aumenta el riesgo de seguridad para el servidor.

Tabla 19. Tareas de autenticación para servidores IBM Spectrum Protect (continuación)

Tarea	Procedimiento

Establecer un método de autenticación predeterminado.	Emita el mandato **SET DEFAULTAUTHENTICATION**. Por ejemplo, para utilizar el servidor como el método de autenticación predeterminado, emita el siguiente mandato:
	`set defaultauthentication local`
	
	Para actualizar un nodo de cliente para autenticarse en el servidor, incluya `AUTHENTICATION=LOCAL` en el mandato **UPDATE NODE**:
	`update node authentication=local`

Conceptos relacionados:

Autenticación de usuarios de IBM Spectrum Protect utilizando un servidor LDAP

Gestión de contraseñas y procedimientos de inicio de sesión (V7.1.1)

Protección del servidor en el sistema

Proteja el sistema donde se ejecuta el servidor de IBM Spectrum Protect para evitar el acceso no autorizado.

Procedimiento

Asegúrese de que los usuarios no autorizados no puedan acceder a los directorios para la base de datos del servidor y la instancia de servidor. Mantenga los valores de acceso para estos directorios que ha configurado durante la implementación.

Restricción del acceso de usuario al servidor

Los niveles de autorización determinan qué puede hacer un administrador con el servidor de IBM Spectrum Protect. Un administrador con autoridad del sistema puede completar cualquier tarea con el servidor. Los administradores con autoridad de política, almacenamiento u operador pueden completar subconjuntos de tareas.

Procedimiento

1. Después de registrar un administrador utilizando el mandato **REGISTER ADMIN**, utilice el mandato **GRANT AUTHORITY** para establecer el nivel de autorización del administrador. Para obtener detalles sobre cómo establecer y cambiar la autorización, consulte "Gestión de administradores" en la página 131.
2. Para controlar la autoridad de un administrador para completar algunas tareas, utilice las dos opciones de servidor siguientes:
   a. Puede seleccionar el nivel de autorización que debe tener un administrador para emitir los mandatos **QUERY** y **SELECT** con la opción de servidor **QUERYAUTH**. De forma predeterminada, no se requiere ningún nivel de autorización. Puede cambiar el requisito para uno de los niveles de autorización, incluido el sistema.
   b. Puede especificar que se requiere autoridad del sistema para mandatos que hacen que el servidor se grabe en un archivo externo con la opción de

servidor **REQSYSAUTHOUTFILE**. El valor predeterminado establece que es necesaria la autorización del sistema para esos mandatos.

3. Puede restringir la copia de seguridad de datos en un nodo cliente a sólo los ID de usuario root o usuarios autorizados. Por ejemplo, para limitar copias de seguridad al ID de usuario root, emita el mandato **REGISTER NODE** o **UPDATE NODE** y especifique el parámetro **BACKUPINITIATION=root**:

```
update node backupinitiation=root
```

Limitación de acceso a través de restricciones de puerto

Limitar acceso al servidor aplicando restricciones de puerto.

Acerca de esta tarea

Es posible que tenga que restringir el acceso a servidores específicos, en base a los requisitos de seguridad. El servidor de IBM Spectrum Protect puede configurarse para escuchar en cuatro puertos TCP/IP: dos para los protocolos regulares y dos para los protocolos de seguridad de la capa de transporte (TLS).

Procedimiento

Puede establecer las opciones de servidor para especificar el puerto que necesita, tal como se enumera en Tabla 20.

Tabla 20. Opciones de servidor y acceso de puerto

Opción de servidor	Acceso de puerto
SSLTCPPORT	Especifica la dirección de puerto SSL TCP/IP para un servidor. Un valor de puerto predeterminado no está disponible. Si el cliente está configurado para la comunicación SSL, utiliza el puerto SSL para comunicarse con el servidor de destino durante la migración tras error.
SSLTCPADMINPORT	Especifica el número de puerto en el que el controlador de comunicaciones TCP/IP del servidor espera las solicitudes para las sesiones habilitadas para SSL. Un valor de puerto predeterminado no está disponible. Utilice esta opción para separar el tráfico de cliente administrativo del tráfico de cliente regular que utiliza las opciones **TCPPORT** y **SSLTCPPORT**.
TCPPORT	Especifica el número de puerto en el que el controlador de comunicaciones TCP/IP del servidor ha de estar a la espera de las solicitudes de sesiones de cliente. El valor predeterminado es 1500.
TCPADMINPORT	Especifica el número de puerto en el que el controlador de comunicaciones TCP/IP del servidor ha de estar a la espera de las peticiones de sesiones distintas de las sesiones de cliente. El valor predeterminado es el valor de **TCPPORT**. Utilice esta opción para separar el tráfico de cliente administrativo del tráfico de cliente regular que utiliza las opciones **TCPPORT** y **SSLTCPPORT**.

Referencia relacionada:

"Planificación del acceso de cortafuegos" en la página 27

Capítulo 19. Detención e inicio del servidor

Antes de completar las tareas de mantenimiento o reconfiguración, detenga el servidor. A continuación, inicie el servidor en modalidad de mantenimiento. Cuando haya terminado con las tareas de mantenimiento o reconfiguración, reinicie el servidor en modo de producción.

Antes de empezar

Debe tener el privilegio de operador o sistema para detener e iniciar el servidor de IBM Spectrum Protect.

Detención del servidor

Antes de detener el servidor, prepare el sistema asegurándose de que todas las operaciones de copia de seguridad de base de datos se han completado y que los demás procesos y sesiones han finalizado. De esta forma, puede concluir el servidor de forma segura y garantizar que los datos están protegidos.

Acerca de esta tarea

Cuando emite el mandato **HALT** para detener el servidor, se produce lo siguiente:

- Yodos los procesos y sesiones de nodo cliente se cancelan.
- Todas las transacciones actuales se detienen. (Las transacciones se retrotraerán cuando el servidor se reinicia.)

Procedimiento

Para preparar el sistema y detener el servidor, complete los pasos siguientes:

1. Impida que se inicien nuevas sesiones de nodo cliente emitiendo el mandato **DISABLE SESSIONS**:

   ```
   disable sessions all
   ```

2. Determine si los procesos o las sesiones de nodo de cliente están en curso completando los pasos siguientes:
   a. En la página Visión general del Centro de operaciones, vea el área Actividad para conocer el número total de procesos y sesiones que están activos actualmente. Si los números difieren de forma significativa de los números normales que se visualizan durante la rutina de gestión de almacenamiento diaria, vea otros indicadores de estado del Centro de operaciones para comprobar si hay un problema.
   b. Vea el gráfico en el área Actividad para comparar la cantidad de tráfico de red durante los periodos siguientes:
      - El periodo actual, es decir, el periodo de 24 horas más reciente
      - El periodo anterior, es decir, 24 horas antes del periodo actual

      Si el gráfico del periodo anterior representa la cantidad de tráfico esperada, las diferencias significativas en el gráfico del periodo actual pueden indicar que hay un problema.
   c. En la página Servidores, seleccione un servidor para el que desee ver los procesos y las sesiones y pulse **Detalles**. Si el servidor no está registrado como servidor concentrador o de radio en el Centro de operaciones, obtenga

información sobre los procesos utilizando mandatos administrativos. Emita el mandato **QUERY PROCESS** para consultar procesos y obtener información sobre sesiones emitiendo el mandato **QUERY SESSION**.

3. Espere hasta que las sesiones de nodo cliente se completen o cancélelas. Para cancelar los procesos y las sesiones, realice los pasos siguientes:
   - En la página Servidores, seleccione un servidor para el que desee ver los procesos y las sesiones y pulse **Detalles**.
   - Pulse el separador Tareas activas y seleccione uno o más procesos, sesiones o una combinación de ambos que desee cancelar.
   - Pulse **Cancelar**.
   - Si el servidor no está registrado como un servidor concentrador o de radio en el Centro de operaciones, cancele las sesiones utilizando mandatos administrativos. Emita el mandato **CANCEL SESSION** para cancelar una sesión y cancelar procesos utilizando el mandato **CANCEL PROCESS**.

     Consejo: Si un proceso que desea cancelar está esperando a que se monte un volumen de cinta, la solicitud de montaje se cancela. Por ejemplo, si emite un mandato **EXPORT**, **IMPORT** o **MOVE DATA**, el mandato puede iniciar un proceso que requiere que el volumen de cinta se monte. Sin embargo, si una biblioteca automatizada está montando un volumen de cinta, la operación de cancelación es posible que no entre en vigor hasta que se complete el proceso de montaje. Dependiendo del entorno del sistema, esto puede tardar varios minutos.
4. Detenga el servidor emitiendo el mandato **HALT**:

   ```
   halt
   ```

Inicio del servidor para tareas de mantenimiento o reconfiguración

Antes de comenzar con las tareas de mantenimiento o reconfiguración, inicie el servidor en modalidad de mantenimiento. Cuando inicia el servidor en modalidad de mantenimiento, inhabilita operaciones que pueden afectar a las tareas de mantenimiento o reconfiguración.

Acerca de esta tarea

Inicie el servidor en modalidad de mantenimiento ejecutando el programa de utilidad **DSMSERV** con el parámetro **MAINTENANCE**.

Las siguientes operaciones están inhabilitadas en la modalidad de mantenimiento:

- Planificaciones de comandos de administración
- Planificaciones de cliente
- Reclamación del espacio de almacenamiento en el servidor
- Caducidad de inventario
- Migración de agrupaciones de almacenamiento

Además, se impide a los clientes iniciar sesiones con el servidor.

Sugerencias:

- No tiene que editar el archivo de opciones de servidor, `dsmserv.opt`, para iniciar el servidor en modalidad de mantenimiento.
- Cuando el servidor se ejecuta en modalidad de mantenimiento, puede iniciar manualmente la reclamación de espacio de almacenamiento, la caducidad de inventario y los procesos de migración de la agrupación de almacenamiento.

Procedimiento

Para iniciar el servidor en modalidad de mantenimiento, emita el siguiente mandato:

```
dsmserv maintenance
```

Consejo: Para ver un vídeo sobre cómo iniciar el servidor en modalidad de mantenimiento, consulte Inicio de un servidor en modalidad de mantenimiento.

Qué hacer a continuación

Para reanudar las operaciones en modo de producción, complete los pasos siguientes:

1. Concluya el servidor emitiendo el mandato **HALT**:

   ```
   halt
   ```

2. Inicie el servidor utilizando el método que utiliza en el modo de producción. Siga las instrucciones para el sistema operativo:
   - AIX Inicio de la instancia de servidor
   - Linux Inicio de la instancia de servidor
   - Windows Inicio de la instancia de servidor

Las operaciones que se han inhabilitado durante la modalidad de mantenimiento se vuelven a habilitar.

Capítulo 20. Planificación para actualizar el servidor

Cuando un fixpack o arreglo temporal queda disponible, puede actualizar el servidor de IBM Spectrum Protect para sacar provecho de las mejoras del producto. Los servidores y los clientes se pueden actualizar en momentos diferentes. Asegúrese de que ha completado los pasos de planificación antes de actualizar el servidor.

Acerca de esta tarea

Siga estas directrices:

- El método preferido es actualizar el servidor utilizando el asistente de instalación. Después de iniciar el asistente, en la ventana IBM Installation Manager, pulse el icono **Actualizar**; no pulse el icono **Instalar** o **Modificar**.
- Si hay actualizaciones disponibles para el componente del servidor y el componente de Centro de operaciones, seleccione las casillas de verificación para actualizar ambos componentes.

Procedimiento

1. Revise la lista de fixpacks y arreglos temporales. Consulte el apartado nota técnica 1239415.
2. Revise las mejoras de producto, que se describen en los archivos léame.

   Consejo: Cuando obtiene el paquete de instalación de Sitio de soporte de IBM Spectrum Protect, también puede acceder al archivo léame.
3. Asegúrese de que la versión a la que actualiza el servidor es compatible con otros componentes como, por ejemplo, clientes y agentes de almacenamiento. Consulte el apartado nota técnica 1053218.
4. Si la solución incluye servidores o clientes en un nivel anterior a V7.1, revise las directrices para asegurarse de que las operaciones de archivado y copia de seguridad de cliente no se vean afectadas. Consulte el apartado nota técnica 1053218.
5. Revise las instrucciones de actualización. Asegúrese de que hace copia de seguridad de la base de datos del servidor, la información de configuración del dispositivo y el archivo de historial de volumen.

Qué hacer a continuación

Para instalar un fixpack o arreglo temporal, siga las instrucciones para su sistema operativo:

- AIX Instalación de un fixpack del servidor de IBM Spectrum Protect
- Linux Instalación de un fixpack del servidor de IBM Spectrum Protect
- Windows Instalación de un fixpack del servidor de IBM Spectrum Protect

Información relacionada:

Proceso de actualización y migración: preguntas más frecuentes

Capítulo 21. Implementación de un plan de recuperación ante siniestro

Implemente una estrategia de recuperación tras desastre para recuperar las aplicaciones si se produce un desastre y para garantizar una alta disponibilidad del servidor.

Acerca de esta tarea

Determine los requisitos que necesita para recuperación tras desastre identificando las prioridades empresariales respecto a la recuperación de nodo de cliente, los sistemas que utiliza para recuperar datos y si los nodos de cliente tienen conectividad con el servidor de recuperación. Utilice la réplica y la protección de agrupación de almacenamiento para proteger datos. También debe determinar la frecuencia con la que se protegen las agrupaciones de almacenamiento de contenedores de directorio.

Preparación para una parada o actualización de sistema

Prepare IBM Spectrum Protect para mantener el sistema en un estado coherente durante un corte eléctrico o una actualización del sistema.

Acerca de esta tarea

Asegúrese de planificar actividades regularmente para gestionar, proteger y mantener el servidor.

Procedimiento

1. Cancele los procesos y las sesiones que están en curso completando los pasos siguientes:
   a. En la página Servidores, seleccione un servidor para el que desee ver los procesos y las sesiones y pulse **Detalles**.
   b. Pulse el separador **Tareas activas** y seleccione uno o más procesos, sesiones o una combinación de ambos que desee cancelar.
   c. Pulse **Cancelar**.
2. Detenga el servidor emitiendo el mandato **HALT**:

   ```
   halt
   ```

Realización de la obtención de detalles de recuperación

Planifique las obtenciones de detalles de recuperación ante siniestro para prepararse para las auditorías que certifican la recuperabilidad del servidor de IBM Spectrum Protect y garantizar que los datos pueden restaurarse y las operaciones pueden reanudarse tras una parada. Las obtenciones de detalles le ayudan a garantizar que los datos se podrán restaurar y que se retomarán las operaciones antes de que se produzca una situación crítica.

Acerca de esta tarea

Restricciones: Las siguientes restricciones se aplican a soluciones de disco de sitio único:

- Sólo puede restaurar la base de datos.
- No puede utilizar la réplica porque no tiene un servidor de destino en un sitio de recuperación.
- No puede recuperarse de daños a agrupaciones de almacenamiento.

Procedimiento

Asegúrese de que se ha hecho copia de seguridad de la base de datos completando los pasos siguientes:

1. En la página Servidores de TSM de Centro de operaciones, seleccione el servidor de cuya base de datos desea hacer copia de seguridad.
2. Pulse **Copia de seguridad** y siga las instrucciones de la ventana Copia de seguridad de la base de datos del servidor.

Capítulo 22. Recuperación de paradas del sistema

Para soluciones de disco de sitio único de IBM Spectrum Protect, puede recuperar el inventario localmente únicamente y restaurar la base de datos para proteger los datos.

Procedimiento

Utilice uno de los métodos siguientes para recuperar el inventario para un sitio local, basado en el tipo de información del que se hace copia de seguridad.

Restricción: Puesto que las soluciones de disco de sitio único no tienen una segunda copia de la agrupación de almacenamiento, no puede restaurar las agrupaciones de almacenamiento. Para revisar la arquitectura de las soluciones de disco, consulte Selección de una solución de IBM Spectrum Protect.

Tabla 21. Escenarios para la recuperación tras un desastre

Escenario	Procedimiento
El sistema está inaccesible y desea restaurar localmente a una versión anterior utilizando las herramientas del sistema.	• Utilice IBM Spectrum Protect para hacer copia de seguridad del servidor a otro servidor. • Utilice las herramientas del sistema operativo para hacer copia de seguridad y restaurar el sistema a una versión anterior.
Se ha producido una parada o desastre y desea restaurar datos desde las versiones de copia de seguridad de los datos.	• Para hacer copia de seguridad de un cliente, en la página Clientes de TSM de Centro de operaciones, seleccione los clientes a los que desea hacer copia de seguridad y pulse **Hacer copia de seguridad**. • En la página Servidores de TSM de Centro de operaciones, seleccione el servidor de cuya base de datos desea hacer copia de seguridad. Pulse **Copia de seguridad** y siga las instrucciones de la ventana Copia de seguridad de la base de datos del servidor. Para restaurar una agrupación de almacenamiento de una versión de copia de seguridad de la agrupación de almacenamiento, debe restaurar la base de datos. Emita el mandato **DSMSERV RESTORE DB** para restaurar la base de datos y las agrupaciones de almacenamiento asociadas a una versión de copia de seguridad.

Referencia relacionada:

AUDIT CONTAINER (Verificar la coherencia de la información de base de datos para una agrupación de almacenamiento de contenedores de directorio)

DSMSERV RESTORE DB (Restaurar la base de datos)

Restauración de la base de datos

Es posible que tenga que restaurar la base de datos de IBM Spectrum Protect después de un siniestro. Puede restaurar la base de datos al estado más actual o a un punto específico en el tiempo. Debe tener volúmenes de copia de seguridad de base de datos de instantánea, completos o incrementales para restaurar la base de datos.

Antes de empezar

Si los directorios de la base de datos y el registro de recuperación se han perdido, vuelva a crearlos antes de emitir el programa de utilidad del servidor **DSMSERV RESTORE DB**. Por ejemplo, utilice los mandatos siguientes: AIX Linux

```
mkdir /tsmdb001
mkdir /tsmdb002
mkdir /tsmdb003
mkdir /activelog
mkdir /archlog
mkdir /archfaillog
```

Windows

```
mkdir e:\tsm\db001
mkdir f:\tsm\db001
mkdir g:\tsm\db001
mkdir h:\tsm\activelog
mkdir i:\tsm\archlog
mkdir j:\tsm\archfaillog
```

Restricciones:

- Para restaurar la base de datos a la versión más reciente, debe ubicar el directorio de registro de archivado. Si no puede ubicar el directorio, puede restaurar la base de datos sólo en un momento específico.
- No puede utilizar la capa de sockets seguros (SSL) para las operaciones de restauración de la base de datos.
- Si el nivel de release de la copia de seguridad de base de datos es diferente del nivel de release del servidor que se está restaurando, no puede restaurar la base de datos del servidor. Por ejemplo, si está utilizando un servidor de la Versión 8.1 e intenta restaurar una base de datos de la Versión 7.1, se produce un error.

Acerca de esta tarea

Las operaciones de restauración en un momento específico se utilizan generalmente para situaciones como la recuperación tras desastre o para eliminar los efectos de errores que pueden provocar incoherencias en la base de datos. Para recuperar la base de datos al instante en que se ha perdido la base de datos, recupérela a su estado actual.

Procedimiento

Utilice el programa de utilidad del servidor **DSMSERV RESTORE DB** para restaurar la base de datos. En función de la versión de la base de datos que desee restaurar, elija uno de los siguientes métodos:

- Restaure una base de datos a su versión más reciente. Por ejemplo, utilice este mandato:

  ```
  dsmserv restore db
  ```

- Restaure una base de datos a un momento específico. Por ejemplo, para restaurar la base de datos a una serie de copias de seguridad que se ha creado el 19 de abril de 2015, utilice el siguiente mandato:

  ```
  dsmserv restore db todate=04/19/2015
  ```

Qué hacer a continuación

Si ha restaurado la base de datos y existen agrupaciones de almacenamiento de contenedores de directorio en el servidor, debe identificar las incoherencias entre la base de datos y el sistema de archivos.

1. Si ha restaurado la base de datos a un punto en el tiempo y no ha retardado la reutilización de la agrupación de almacenamiento de contenedores de directorio, debe auditar todos los contenedores. Para auditar todos los contenedores, emita el siguiente mandato:

   ```
   audit container stgpool
   ```

2. Si el servidor no puede identificar contenedores en el sistema, complete los pasos siguientes para mostrar una lista de contenedores:
   a. Desde un cliente administrativo, emita el mandato siguiente:

      ```
      select container_name from containers
      ```

   b. Desde el sistema de archivos, emita el siguiente mandato para el directorio de la agrupación de almacenamiento en el servidor de origen:

      Consejo: El directorio de la agrupación de almacenamiento se visualiza en la salida del mandato:

      AIX Linux

      ```
      [root@source]$ ls -l
      ```

      Windows

      ```
      c:\source_stgpooldir\00>dir
      ```

   c. Compare los contenedores listados en el sistema de archivos y el servidor.
   d. Emita el mandato **AUDIT CONTAINER** y especifique el contenedor que falta de la salida del servidor. Especifique el parámetro **ACTION=REMOVEDAMAGED** para suprimir el contenedor.
   e. Para asegurarse de que los contenedores se suprimen en el sistema de archivos, revise los mensajes que se muestran.

Parte 5. Apéndices

Apéndice. Funciones de accesibilidad para la familia de productos IBM Spectrum Protect

Las funciones de accesibilidad ayudan a aquellos usuarios que tienen una discapacidad, como, por ejemplo, movilidad reducida o poca visión, a utilizar productos tecnológicos de información de forma satisfactoria.

Visión general

La familia de productos de IBM Spectrum Protect incluye las siguientes funciones de accesibilidad mayores:

- Funcionamiento utilizando sólo el teclado
- Operaciones que utilizan un lector de pantalla

La familia de productos de IBM Spectrum Protect utiliza el estándar W3C más reciente, WAI-ARIA 1.0 (www.w3.org/TR/wai-aria/), para asegurar la conformidad con US Section 508 (www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/section-508-standards) y Web Content Accessibility Guidelines (WCAG) 2.0 (www.w3.org/TR/WCAG20/). Para aprovechar las características de accesibilidad, utilice el release más reciente del lector de pantalla y el navegador web más reciente soportados por el producto.

La documentación del producto en IBM Knowledge Center está habilitada para la accesibilidad. Las funciones de accesibilidad del IBM Knowledge Center se describen en la Sección de accesibilidad de la ayuda del IBM Knowledge Center (www.ibm.com/support/knowledgecenter/about/releasenotes.html?view=kc#accessibility).

Navegación con el teclado

Este producto utiliza teclas estándar de navegación.

Información sobre interfaces

Las interfaces de usuario no tienen contenido que se actualiza de 2 a 55 veces por segundo.

Las interfaces de usuarios web se basan en las hojas de estilo en cascada para representar el contenido correctamente y para proporcionar una experiencia que se pueda utilizar. La aplicación proporciona un método equivalente para usuarios con problemas de poca visión para utilizar los parámetros de visualización del sistema, incluido el modo de alto contraste. Puede controlar el tamaño de fuente utilizando los parámetros del dispositivo o del navegador web.

Las interfaces de usuarios web incluyen puntos de referencia de navegación WAI-ARIA que puede utilizar para navegar rápidamente a áreas funcionales de la aplicación.

Fabricante de software

La familia de productos IBM Spectrum Protect incluye cierto software del proveedor que no está cubierto por 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 accesibilidad relacionada con sus productos.

Información de accesibilidad relacionada

Además del centro de atención al cliente de IBM y de los sitios web de soporte estándar, 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 América del Norte)

Para obtener más información acerca del compromiso que IBM tiene con la accesibilidad, consulte IBM Accessibility (www.ibm.com/able).

Avisos

Esta información se ha desarrollado para productos y servicios que se ofrecen en EE.UU. Es posible que este material esté disponible en otros idiomas en IBM. Sin embargo, es posible que tenga obligación de tener una copia del producto o de la versión del producto en dicho idioma para acceder a él.

Es posible que IBM no ofrezca los productos, servicios o funciones que se tratan en este documento en otros países. Consulte el representante local de IBM si desea más información sobre los productos y servicios disponibles actualmente en su zona. Cualquier referencia a un producto, programa o servicio de IBM no pretende afirmar ni implicar que solamente se pueda utilizar ese producto, programa o servicio de IBM. En su lugar, se puede utilizar cualquier producto, programa o servicio 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 la materia descrita en este documento. La posesión de este documento no le otorga ninguna licencia sobre dichas patentes. Puede enviar consultas sobre licencias a la siguiente dirección:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
EE.UU.

Para consultas de licencias referentes a información del juego de caracteres de doble byte (DBCS), póngase en contacto con el Departamento de propiedad intelectual de IBM de su país o envíe las consultas a la siguiente dirección:

Licencia de propiedad intelectual
Ley de propiedad intelectual y legal
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 EXPLÍCITA NI IMPLÍCITA, INCLUIDAS, PERO SIN LIMITARSE A, LAS GARANTÍAS O CONDICIONES IMPLÍCITAS DE NO VULNERACIÓN DE DERECHOS, COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN DETERMINADO. Algunos estados no autorizan la exclusión de garantías explícitas o implícitas en determinadas transacciones, por lo que es posible que este aviso no sea aplicable en su caso.

Esta información podría incluir imprecisiones técnicas o errores tipográficos. Se realizan cambios de forma periódica a la información contenida en el presente documento; estos cambios se incorporarán en nuevas ediciones de la publicación. IBM puede realizar mejoras y/o cambios en los productos y/o los programas descritos en esta publicación en cualquier momento sin previo aviso.

Las referencias contenidas en esta información a sitios web no IBM solo se proporcionan por comodidad y de ningún modo constituyen un aval de esos sitios web. Los materiales de estos sitios web no forman parte de los materiales para este producto IBM y el uso de estos sitios web es responsabilidad del usuario.

IBM puede utilizar o distribuir cualquier información que usted proporcione de la forma que considere apropiada sin incurrir en ninguna obligación con usted.

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 los términos y condiciones adecuados, incluyendo en algunos casos el pago de una tarifa.

El programa con licencia descrito en este documento y todo el material bajo licencia disponible para el mismo se proporciona por parte de IBM bajo los términos de los acuerdos IBM Customer Agreement, IBM International Program License Agreement o cualquier acuerdo equivalente entre las dos partes.

Los datos de rendimiento aquí mencionados se han obtenido en condiciones de funcionamiento específicas. Los resultados reales pueden variar.

La información relativa a productos que no son de IBM se ha obtenido de los proveedores de estos productos, sus anuncios publicados y otras fuentes públicamente disponibles. 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 relativas a las posibilidades de productos no IBM deben dirigirse a los suministradores de esos productos.

Esta información contiene ejemplos de datos e informes utilizados en operaciones empresariales diarias. Para que esta ilustración sea lo más completa posible, los ejemplos incluyen nombres de personas, empresas, marcas y productos. Todos estos nombres son ficticios y cualquier similitud con nombres y direcciones utilizados por una empresa real es mera coincidencia.

LICENCIA DE COPYRIGHT:

Esta información contiene programas de aplicación de muestra en el idioma de origen, que ilustra técnicas de programación en las diferentes plataformas operativas. Debe copiar, modificar y distribuir estos programas de muestra en cualquiera de las formas sin pago para IBM, para el desarrollo, utilización, marketing o distribución de los programas de aplicación conforme a la interfaz de programación de la aplicación para la plataforma operativa para la que están escritos los programas de muestra. Estos ejemplos no se han probado exhaustivamente bajo todas las condiciones. Por tanto, IBM, no puede garantizar ni implicar la fiabilidad, utilidad o función de estos programas. Los programas de

muestra se proporcionan como "AS IS", sin garantía de ninguna clase. IBM no será responsable de ningún daño que surja del uso de los programas de muestra.

Cada copia o fragmento de estos programas de ejemplo o cualquier trabajo derivado deben incluir un aviso de copyright como el siguiente: © (nombre de su empresa) (año). Partes de este código derivan de programas de ejemplo de IBM Corp. © Copyright IBM Corp. _escriba el año o años_.

Marcas registradas

IBM, el logotipo de IBM e ibm.com son marcas registradas o marcas comerciales registradas de International Business Machines Corp., registradas en muchas jurisdicciones internacionales. Otros nombres de productos y servicios pueden ser marcas registradas de IBM u otras compañías. Hay disponible una lista actual de marcas registradas de IBM en la web, en sección "Copyright and trademark information" de www.ibm.com/legal/copytrade.shtml.

Adobe es una marca registrada de Adobe Systems Incorporated en Estados Unidos y/o en otros países.

Linear Tape-Open, LTO y Ultrium son marcas registradas de HP, IBM Corp. y Quantum en EE.UU. y en otros países.

Intel y Itanium son marcas registradas de Intel Corporation o sus empresas filiales en Estados Unidos y otros países.

Linux es una marca registrada de Linus Torvalds en Estados Unidos y/o en otros países.

Microsoft, Windows y Windows NT son marcas comerciales de Microsoft Corporation en los Estados Unidos o en otros países.

Java™ y todas las marcas registradas y los logotipos basados en Java son marcas registradas de Oracle y/o sus filiales.

SoftLayer es una marca registrada de SoftLayer, Inc., una empresa de IBM.

UNIX es una marca registrada de The Open Group en Estados Unidos y en otros países.

Términos y condiciones para la documentación de producto

Los permisos para la utilización de estas publicaciones se otorgan sujetos a los siguientes términos y condiciones.

Aplicabilidad

Estos términos y condiciones se añaden a los términos de uso para el sitio web de IBM.

Uso personal

Puede reproducir estas publicaciones para su uso personal, no comercial, siempre que se conserven todos los avisos sobre derechos de propiedad. No podrá distribuir, visualizar ni crear trabajo derivado de estas publicaciones, o cualquier parte de éstas, sin el consentimiento expreso de IBM.

Uso comercial

Puede reproducir, distribuir y visualizar estas publicaciones únicamente en su empresa siempre que se conserven todos los avisos de propiedad. No puede realizar trabajos derivados de estas publicaciones, ni reproducir, distribuir ni visualizar estas publicaciones ni ninguna parte de las mismas fuera de la empresa, sin el consentimiento expreso de IBM.

Derechos

Con la excepción de lo explícitamente otorgado en este permiso, IBM no otorga ningún otro permiso, licencia o derecho, ya sea explícito o implícito, respecto a las publicaciones o cualquier información, datos, software u otra propiedad intelectual que se incluya en las mismas.

IBM se reserva el derecho de retirar los permisos otorgados aquí siempre que, a su discreción, considere que la utilización de las publicaciones actúa en detrimento de sus intereses o, según determine IBM, no se cumplan adecuadamente las instrucciones anteriores.

Queda prohibido descargar, exportar o reexportar esta información si no se cumplen íntegramente todas las leyes aplicables y regulaciones, incluyendo las leyes y regulaciones de exportación de los Estados Unidos.

IBM NO GARANTIZA EL CONTENIDO DE ESTAS PUBLICACIONES. LAS PUBLICACIONES SE SUMINISTRAN "TAL CUAL", SIN GARANTÍAS DE NINGÚN TIPO, NI EXPLÍCITAS NI IMPLÍCITAS, INCLUYENDO LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN PROPÓSITO DETERMINADO, SIN LIMITARSE A ELLAS.

Consideraciones sobre la política de privacidad

Los productos de IBM Software, incluidas las soluciones de software como servicio (“Ofertas de software”), pueden utilizar cookies u otras tecnologías para recopilar información de uso del producto, ayudar a mejorar la experiencia del usuario final, adaptar las interacciones con el usuario final u otros fines. En muchos casos, las ofertas de software no recopilan información de identificación personal. Algunas de las 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 ni otro tipo de tecnología 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 requisito 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 Declaración de privacidad en línea de IBM en http://www.ibm.com/privacy/details en la sección titulada “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 la publicación Glosario de IBM Spectrum Protect.

Para ver los glosarios de otros productos de IBM, consulte Terminología de IBM.

Índice

I

K

L

M

N

O

P

R

S

T

U

Número de Programa: 5725-W98
5725-W99
5725-X15

Impreso en España