IBM Spectrum Protect for Virtual Environments
Version 8.1.0

Data Protection for VMware - Guía de instalación

IBM Spectrum Protect for Virtual Environments
Version 8.1.0

Data Protection for VMware - Guía de instalación

Nota:
Antes de utilizar esta información y el producto al que da soporte, lea la información del apartado “Avisos” en la página 121.

Esta edición se aplica a la versión 8, release 1, modificación 0 de IBM Spectrum Protect for Virtual Environments (número de producto 5725-X00) y a todos los releases y las modificaciones subsiguientes hasta que se indique lo contrario en nuevas ediciones.

Contenido

Acerca de esta publicación v
A quién va dirigida esta publicación v
Publicaciones v

Novedades de la versión 8.1 vii

Capítulo 1. Instalación y actualización de Data Protection for VMware 1
Componentes instalables 1
Interfaz gráfica de usuario de Data Protection for VMware vSphere 3
Agente de recuperación de IBM Spectrum Protect 6
Extensión de IBM Spectrum Protect. 7
Interfaz de línea de mandatos de Data Protection for VMware 7
Interfaz de restauración de archivos de IBM Spectrum Protect 8
Característica de transportador de datos 8
Planificación de la instalación de Data Protection for VMware 9
Esquema de instalación. 9
Escenarios de instalación 10
Requisitos del sistema 11
Instalación de los componentes de Data Protection for VMware 19
Obtención del paquete de instalación de Data Protection for VMware 20
Instalación de los componentes de Data Protection for VMware utilizando el asistente de instalación. 21
Instalación de los componentes de Data Protection for VMware en modalidad silenciosa . 24
Primeros pasos después de instalar Data Protection for VMware 31
Actualización de Data Protection for VMware . . . 32
Actualización de Data Protection for VMware . . 33
Actualización de Data Protection for VMware en un sistema Windows de 64 bits en modo silencioso 34
Actualización de Data Protection for VMware en un sistema Linux en modo silencioso. 35
Desinstalación de Data Protection for VMware . . 36
Desinstalación de Data Protection for VMware en Windows 36
Desinstalación de Data Protection for VMware for Windows en modalidad silenciosa 38
Desinstalación de Data Protection for VMware en un sistema Linux 39

Capítulo 2. Configuración de Data Protection for VMware 41
Configuración de una nueva instalación con el asistente 41
Utilizando el cuaderno para editar una instalación existente 42
Habilitación del entorno para operaciones de restauración de archivos 43
Configuración de operaciones de restauración de archivos en Linux 44
Modificación de opciones para las operaciones de restauración de archivos 45
Opciones de restauración de archivos. 46
Configuración de la actividad de registro para operaciones de restauración de archivos 47
Opciones de actividad del registro de restauración de archivos 48
Configuración de un nodo de transportador de datos para soporte de descodificación 49
Configuración del entorno para las operaciones de restauración instantánea de máquinas virtuales completas 51
1. Configuración del software de iSCSI en el host de ESXi. 52
2. Instalación y configuración de aplicaciones en transportador de datos 53
3. Configuración de la conexión del agente de recuperación 53
4. Configuración de una red iSCSI dedicada para el host de ESXi y el transportador de datos. . . 54
Configuración de la comunicación con Seguridad de la capa de transporte 55
Uso de un certificado de tercero 56
Habilitación de comunicación segura con el servidor IBM Spectrum Protect 60
Requisitos de privilegios de usuario del servidor de VMware vCenter 62
Roles de usuario de Interfaz gráfica de usuario de Data Protection for VMware vSphere 65
Claves de registro de la GUI de Data Protection for VMware 68
Configuración de la interfaz gráfica de usuario agente de recuperación 69
Habilitación de la comunicación segura de agente de recuperación al servidor de IBM Spectrum Protect 74
Valores de entorno local 78
Actividad del archivo de registro 79
Inicio y ejecución de los servicios de Data Protection for VMware 81

Apéndice A. Tareas de configuración avanzadas 83
Configuración de los nodos de IBM Spectrum Protect en un entorno de vSphere 84
Configuración de los nodos transportadores de datos en un entorno de vSphere 85

Configuración de la Interfaz de línea de mandatos de Data Protection for VMware en un entorno de vSphere 91
Lista de comprobación de configuración de interfaz de línea de mandatos de entorno de vSphere . . . 93
Directrices de configuración de cintas. 96
Configuración manual de un dispositivo iSCSI en un sistema Linux 98
Configuración manual de un dispositivo iSCSI en un sistema Windows 101
Configuración manual de los nodos de proxy de montaje en un sistema Linux 103
Configuración manual de los nodos de proxy de montaje en un sistema Windows remoto 106
Configuración manual de varios servicios aceptadores de cliente en un sistema Linux . . . 108
Modificación del archivo de configuración de VMCLI 110

Apéndice B. Migración a una estrategia de copia de seguridad incremental constante 113

Apéndice C. Funciones de accesibilidad para la familia de productos IBM Spectrum Protect . . . 119

Avisos 121

Glosario 125

Índice. 127

Acerca de esta publicación

IBM Spectrum Protect for Virtual Environments ofrece copia de seguridad incremental de bloques fuera de host y recuperación de archivos y restauración instantánea a partir de una copia de seguridad de VM completa para máquinas de invitado Windows y Linux. Están disponibles copias de seguridad incrementales de nivel de bloque cuando se utiliza IBM Spectrum Protect for Virtual Environments con el transportador de datos de IBM Spectrum Protect.

A quién va dirigida esta publicación

Esta publicación está destinada a los administradores y los usuarios que desean instalar y configurar IBM Spectrum Protect for Virtual Environments.

La información general, las tareas de usuario, los escenarios de copia de seguridad y restauración, la referencia de mandatos y los mensajes de error se documentan en *IBM Spectrum Protect for Virtual Environments: Guía del usuario de Data Protection for VMware*.

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 del producto IBM, consulte IBM Knowledge Center.

Novedades de la versión 8.1

Data Protection for VMware Versión 8.1 presenta nuevas características y actualizaciones.

Si desea una lista de nuevas características y actualizaciones en este release, consulte Actualizaciones de Data Protection for VMware.

Capítulo 1. Instalación y actualización de Data Protection for VMware

La instalación de Data Protection for VMware incluye la planificación, instalación y configuración inicial.

Componentes instalables

Data Protection for VMware incluye varios componentes que puede instalar para proteger el entorno virtual.

En función del entorno de sistema operativo, están disponibles para instalarse las siguientes características de Data Protection for VMware:

Restricción: Cada paquete de instalación se le presenta con un archivo de licencia de usuario (EULA). Si no acepta el archivo, se detiene el proceso de instalación.

Tabla 1. Características de Data Protection for VMware disponibles por sistema operativo

Componente	Linux	Windows
El agente de recuperación de IBM Spectrum Protect Este componente proporciona capacidades de restauración instantánea y montaje virtual.		√
Interfaz de línea de mandatos de agente de recuperación La interfaz de línea de mandatos que se utiliza para operaciones de montaje.		√
Documentos Los documentos incluyen los archivos léame y avisos.	√	√
Archivo de habilitación de Data Protection for VMware Este componente habilita IBM Spectrum Protect para ejecutar los siguientes tipos de copia de seguridad: • Copia de seguridad incremental constante • Copia de seguridad completa incremental constante Este componente es necesario para la protección de aplicaciones. Si descarga cargas de trabajo de copia de seguridad, este archivo debe estar instalado en el servidor de seguridad vStorage.	√	√

Tabla 1. Características de Data Protection for VMware disponibles por sistema operativo (continuación)

Componente	Linux	Windows
Interfaz gráfica de usuario de Data Protection for VMware vSphere Este componente es la interfaz gráfica de usuario (GUI) que accede a los datos de la máquina virtual en el servidor de VMware vCenter. El contenido de la GUI está disponible en tres visualizaciones: • Una vista de navegador web. Se accede a esta vista en un navegador web soportado utilizando el URL para el host del servidor web de GUI. Por ejemplo: `https://guihost.mycompany.com:9081/TsmVMwareUI/` • La vista de Extensión de IBM Spectrum Protect del cliente web de VMware vSphere. Los paneles de esta vista están exclusivamente diseñados para integrarse dentro del cliente web, pero los datos y mandatos para esta vista se obtienen del mismo servidor web de la GUI que las otras vistas. Extensión de IBM Spectrum Protect proporciona un subconjunto de las funciones que están disponibles en la vista del navegador web y algunas funciones adicionales. Las funciones de configuración y elaboración avanzada de informes no se ofrecen en esta vista. Puede especificar una o más vistas durante la instalación.	√	√
GUI de restauración de archivos Este componente es una GUI basada en web que le permite restaurar archivos a partir de una copia de seguridad de máquina virtual VMware sin ayuda del administrador. La GUI se instala automáticamente cuando se instala la GUI de Data Protection for VMware. Se habilita a través del asistente de configuración.	[1]	√
Transportador de datos El transportador de datos de IBM Spectrum Protect mueve datos para Data Protection for VMware. Esta funcionalidad se conoce como el transportador de datos. El transportador de datos mueve los datos del entorno virtual al servidor de IBM Spectrum Protect. Cuando instale el transportador de datos en un servidor, el servidor se puede utilizar como un servidor de seguridad de vStorage. Puede instalar el transportador de datos en el mismo sistema que Data Protection for VMware o en otro servidor.	√	√

1. Aunque deba instalarse el componente de interfaz de restauración de archivos y habilitarse en un sistema Windows, puede utilizar esta interfaz para restaurar archivos en máquinas virtuales de invitado tanto Windows como Linux.

Data Protection for VMware descarga la carga de trabajo de copia de seguridad de las máquinas virtuales en un servidor de seguridad de vStorage. Para llevar a cabo esta tarea, el transportador de datos V8.1.0 debe estar instalado en el Servidor de seguridad vStorage.

Interfaz gráfica de usuario de Data Protection for VMware vSphere

El componente de Interfaz gráfica de usuario de Data Protection for VMware vSphere (GUI de vSphere) es una interfaz gráfica de usuario que accede a datos de máquina virtual en el servidor de VMware vCenter.

Visión general

La Interfaz gráfica de usuario de Data Protection for VMware vSphere es la interfaz primaria desde la que se deben completar las siguientes tareas:

- Iniciar o planificar copias de seguridad de las máquinas virtuales en un servidor de IBM Spectrum Protect.
- Inicie una recuperación completa de las máquinas virtuales desde un servidor de IBM Spectrum Protect.
- Emitir los informes sobre el progreso de las tareas, los sucesos más recientes que se han completado,el estado de copia de seguridad y el uso de espacio. Esta información puede ayudarle a resolver los errores que se produjeron en el proceso de copia de seguridad.

Consejo: La información sobre cómo realizar tareas con la GUI de vSphere se proporciona en la ayuda en línea que se instala con la GUI. Pulse en **Learn More** (Más información) en cualquiera de la ventanas de la interfaz gráfica de usuario para abrir la ayuda en línea y obtener asistencia.

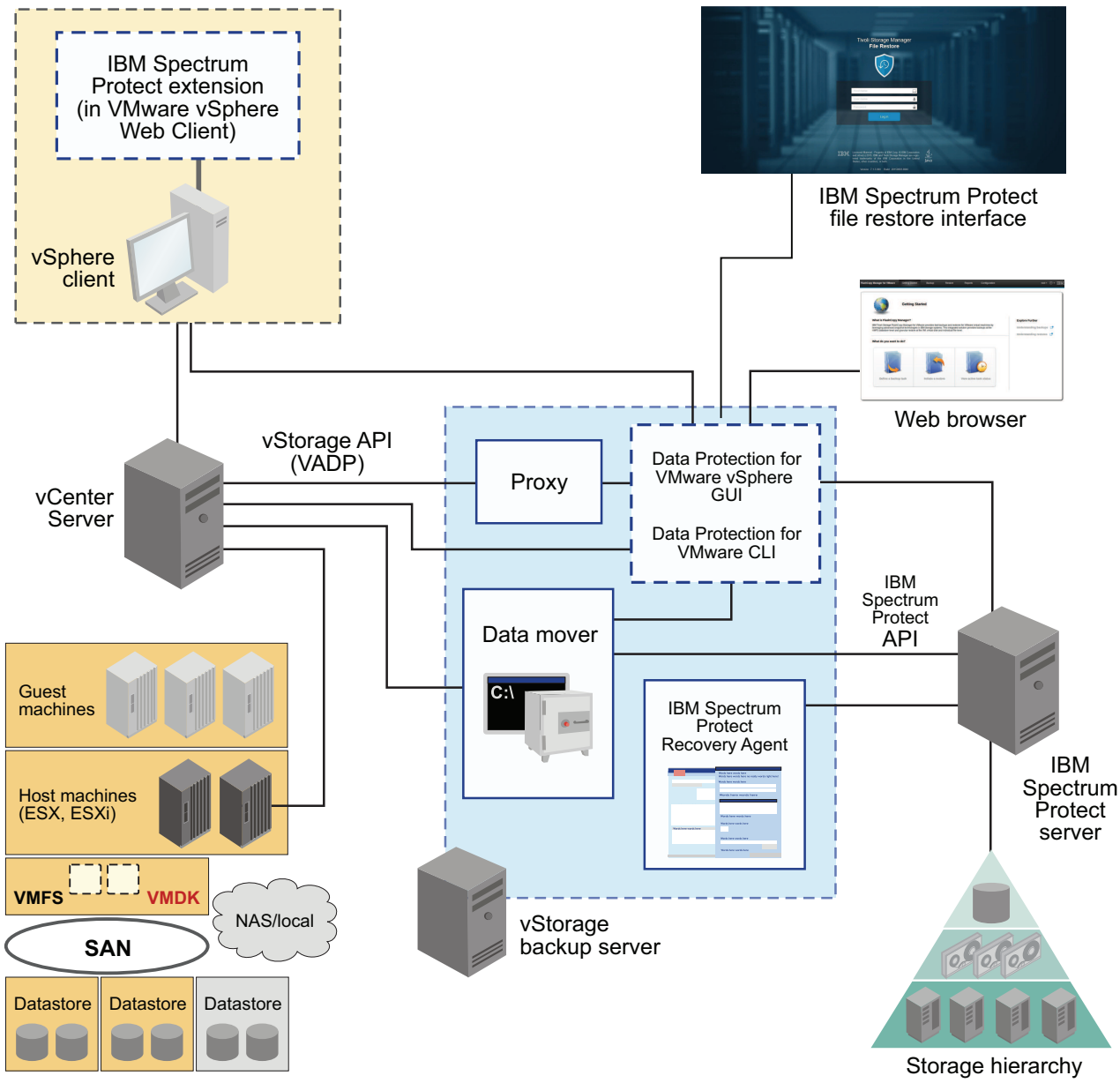

Figura 1. Componentes de sistema de Data Protection for VMware en un entorno de usuario de VMware vSphere

Requisitos

Interfaz gráfica de usuario de Data Protection for VMware vSphere se puede instalar en cualquier sistema que cumpla los requisitos previos de sistema operativo. Los requisitos de recursos de GUI de vSphere son mínimos ya que no se procesan transferencias de datos de E/S.

Consejo: La instalación de la GUI de vSphere en el servidor de seguridad de vStorage es la configuración más común.

La GUI de vSphere debe tener conectividad de red para los siguientes sistemas:

- Servidor de seguridad vStorage
- Servidor de IBM Spectrum Protect
- Servidor vCenter

Además, los puertos para la base de datos Derby (valor predeterminado 1527a) y el servidor web de GUI (valor predeterminado 9081) deben estar disponibles.

Configuración

Puede registrar varias GUI de vSphere en un único servidor de vCenter. Este escenario reduce el número de centros de datos (y las copias de seguridad de invitado de máquina virtual) gestionados por una única GUI de VMware vSphere. Un servidor de vCenter puede después gestionar un subconjunto del total de centros de datos definidos en el servidor de vCenter.

Para actualizar los centros de datos gestionados, vaya a **Configuración** > **Editar configuración**.

Al registrar varias GUI de vSphere en un único servidor de vCenter, se aplican las siguientes directrices:

- Cada centro de datos puede estar gestionado únicamente por una GUI de vSphere instalada.
- Se requiere un nombre de nodo de VMCLI exclusivo para cada GUI de vSphere instalada.
- La utilización de nombres de nodo de transportador de datos exclusivos para cada GUI de vSphere instalada simplifica la gestión de los nodos.

Acceso a la GUI de vSphere

Se accede a la GUI de vSphere mediante los métodos siguientes:

- Una GUI de navegador web autónoma. Se accede a esta GUI a través de un marcador de URL al servidor web de GUI, por ejemplo:

  `https://nombre_host:puerto/TsmVMwareUI/`

  donde:
  - *nombre_host* es el nombre del sistema donde está instalada la Interfaz gráfica de usuario de Data Protection for VMware vSphere
  - *puerto* es el número de puerto a través del cual la GUI de vSphere es accesible. El número de puerto predeterminado es 9081.
- Una extensión de cliente web de vSphere que se conecta a un servidor web de GUI para acceder a las máquinas virtuales en el almacenamiento de IBM (conocido como extensión de protección de datos). El contenido es un subconjunto de lo que se proporciona en la GUI del explorador web.

Puede especificar uno o más métodos de acceso durante la instalación.

Windows El directorio de instalación predeterminado es `C:\IBM\tivoli\tsm\tdpvmware\webserver`.

Linux El directorio de instalación predeterminado es `/opt/tivoli/tsm/tdpvmware/common/webserver`.

Agente de recuperación de IBM Spectrum Protect

Utilice el servicio de agente de recuperación para montar cualquier volumen de instantánea desde el servidor de IBM Spectrum Protect.

Visión general

Puede ver las instantáneas localmente, con acceso de sólo lectura, en el sistema cliente, o utilice un protocolo iSCSI para acceder a una instantánea desde un sistema remoto.

Además, el agente de recuperación proporciona la función de restauración instantánea y la protección para aplicaciones invitadas. La restauración instantánea permite al volumen que está en uso, permanecer disponible mientras la operación de restauración sigue en segundo plano. La protección de aplicación permite a las aplicaciones que están instaladas en un sistema virtual invitado, como Microsoft Exchange Server y Microsoft SQL Server, estar disponibles para la protección de restauración y copia de seguridad.

Importante: Cuando se instala el agente de recuperación para la función de restauración instantánea, también debe seleccionar el controlador de dispositivo para su instalación. De forma predeterminada no está seleccionado.

El controlador de dispositivo no es necesario para la protección de aplicaciones.

El agente de recuperación puede realizar las siguientes tareas desde un sistema remoto:

- Recopilar información sobre los datos que se pueden restaurar, por ejemplo:
  - Realizar copias de seguridad de máquinas virtuales.
  - Instantáneas disponibles para una máquina virtual de copia de seguridad.
  - Particiones disponibles en una instantánea específica.
- Montar una instantánea como dispositivo virtual.
- Proporcione una lista de dispositivos virtuales.
- Eliminar un dispositivo virtual.

Para obtener información detallada sobre los mandatos, parámetros y códigos de retorno, consulte la sección de referencia de mandatos de la *IBM Spectrum Protect for Virtual Environments: Data Protection for VMware - Guía del usuario*.

Requisitos

Windows En sistemas Windows, puede instalar la GUI de agente de recuperación, la interfaz de línea de mandatos y el controlador de dispositivo.

Acceso al agente de recuperación

Windows Puede acceder el agente de recuperación desde el menú **Inicio**: **Inicio** > **IBM Spectrum Protect** > **IBM Spectrum Protect for Virtual Environments** > **IBM Spectrum Protect agente de recuperación**

Windows De forma alternativa, puede acceder a la GUI y la interfaz de línea de mandatos desde un indicador de mandatos:

```
dir_instalación\TSM\recoveryagent\mount\RecoveryAgent.exe -notservice
dir_instalación\TSM\recoveryagent\shell\RecoveryAgentShell.exe
```

donde *dir_instalación* es el directorio de instalación. El valor predeterminado es `C:\Archivos de programa\Tivoli`. En sistemas Windows, utilice `Archivos de programa (x86)`.

Extensión de IBM Spectrum Protect

La Extensión de IBM Spectrum Protect es una extensión del cliente web de VMware vSphere que proporciona una visión de la Interfaz gráfica de usuario de Data Protection para VMware vSphere.

Visión general

Extensión de IBM Spectrum Protect proporciona un subconjunto de las funciones que están disponibles en la vista del navegador para la Interfaz gráfica de usuario de Data Protection para VMware vSphere y algunas funciones adicionales.

Requisito

Para instalar la Extensión de IBM Spectrum Protect, debe seleccionar las opciones siguientes al ejecutar el asistente de instalación de IBM Spectrum Protect for Virtual Environments.

- En la página Protección del entorno del asistente de instalación, pulse **Protección de vSphere**.
- En la Información de GUI para la página de protección de vSphere, seleccione **Habilitar el acceso a la GUI mediante un navegador web** y **Registrar como una extensión en el cliente web de vSphere**.

Acceso a la extensión de protección de datos

Puede acceder a la extensión del cliente web de vSphere.

Interfaz de línea de mandatos de Data Protection for VMware

La CLI de Data Protection for VMware es una interfaz de línea de mandatos de funciones completas que se instala con la Interfaz gráfica de usuario de Data Protection for VMware vSphere.

Visión general

Puede utilizar la CLI de Data Protection for VMware para realizar las siguientes tareas:

- Iniciar o planificar copias de seguridad de las máquinas virtuales en un servidor de IBM Spectrum Protect.
- Iniciar una recuperación completa de las máquinas virtuales, los archivos de máquinas virtuales o los discos de máquinas virtuales (VMDK) desde un servidor de IBM Spectrum Protect.
- Visualice información de configuración sobre el entorno y la base de datos de copia de seguridad.

Aunque el Interfaz gráfica de usuario de Data Protection for VMware vSphere es la interfaz primaria de tareas, la CLI de Data Protection for VMware proporciona una útil interfaz secundaria.

Por ejemplo, se puede utilizar la CLI de Data Protection for VMware para implementar un mecanismo de planificación que sea diferente del implementado por la Interfaz gráfica de usuario de Data Protection for VMware vSphere.

También, la CLI de Data Protection for VMware es útil cuando se evalúan los resultados de automatización con los scripts.

Acceso a la Interfaz de línea de mandatos de Data Protection for VMware

Puede acceder a la CLI de Data Protection for VMware desde una línea de mandatos.

Para obtener información detallada sobre los mandatos disponibles, consulte la sección de referencia de mandatos de la *IBM Spectrum Protect for Virtual Environments: Data Protection for VMware - Guía de usuario*

Interfaz de restauración de archivos de IBM Spectrum Protect

Puede restaurar archivos individuales desde una copia de seguridad de máquina virtual de VMware.

Visión general

La interfaz de restauración de archivo es una interfaz basada en web donde puede restaurar archivos individuales desde una copia de seguridad de máquina virtual. La ventaja de esta interfaz es que los propietarios de archivo, software y plataforma pueden restaurar sus propios archivos sin conocimiento previo de las operaciones de copia de seguridad y restauración de IBM Spectrum Protect.

La función de interfaz de restauración de archivos se instala al seleccionar la opción para proteger los datos en un entorno de vSphere. En el asistente de configuración de Data Protection for VMware, debe habilitar la característica de restauración de archivos para que la interfaz esté disponible.

Acceso a la interfaz de restauración de archivos de IBM Spectrum Protect

Para acceder a la interfaz de restauración de archivos, abra un navegador web y escriba el URL proporcionado por el administrador. Por ejemplo:

`https://nombre_host:9081/FileRestoreUI`

donde *nombre_host* es el nombre de host del sistema en el que está instalado Interfaz gráfica de usuario de Data Protection for VMware vSphere.

Característica de transportador de datos

El transportador de datos es un nodo de cliente específico que "mueve" datos de un sistema a otro.

Visión general

En el entorno VMware normal, el nodo de transportador de datos se utiliza para guardar las copias de seguridad de máquina virtual en un nodo de centro de datos.

Para obtener más información sobre el transportador de datos, incluida la información sobre entornos con varios transportadores de datos, consulte Cómo se utilizan los nodos de IBM Spectrum Protect en un entorno virtual.

Acceso a los archivos de configuración de transportador de datos

Puede configurar el transportador de datos desde la GUI de vSphere de Data Protection for VMware.

Windows El directorio de instalación predeterminado es `C:\Archivos de programa\Tivoli\TSM\baclient`.

Linux El directorio de instalación predeterminado es `/opt/tivoli/tsm/client/ba/bin`.

Planificación de la instalación de Data Protection for VMware

Data Protection for VMware elimina el impacto de la ejecución de copias de seguridad en una VM descargando las cargas de trabajo de copia de seguridad de un host VMware basado en ESX o ESXi en un servidor de copia de seguridad vStorage.

Data Protection for VMware funciona con el transportador de datos (instalado en el servidor de seguridad de vStorage) para completar las copias de seguridad completas constantes e incrementales constantes de las MV. El nodo de cliente que está instalado en el servidor de seguridad de vStorage se denomina nodo de transportador de datos. Este nodo "mueve" los datos al servidor de IBM Spectrum Protect para el almacenamiento, y para la restauración de nivel de imagen de la máquina virtual en un futuro. La restauración instantánea está disponible a nivel de volumen del disco y a nivel de la máquina virtual completa.

Consejo: El transportador de datos es un componente con licencia independiente que contiene sus propias interfaces de usuario y documentación. Para integrar de forma adecuada un plan global para proteger las máquinas virtuales con Data Protection for VMware, es necesario estar familiarizado con este producto y su documentación. Data Protection for VMware para Windows de 64 bits incluye la característica de transportador de datos.

Esquema de instalación

La siguiente tabla identifica los pasos para completar un proceso de instalación correcto.

Tabla 2. Tareas de instalación para clientes de Data Protection for VMware nuevos o existentes

Paso	Tarea	Comience aquí
1	Comprobar requisitos de sistema.	Asegúrese de que el sistema en el queData Protection for VMware se va a instalar cumple con los requisitos del sistema.
2	Comprobar requisitos de permisos de usuario.	Evite los errores de instalación potenciales o los retrasos utilizando los niveles de permiso de usuario necesarios.

Tabla 2. Tareas de instalación para clientes de Data Protection for VMware nuevos o existentes (continuación)

Paso	Tarea	Comience aquí
3	Comprobar la disponibilidad de los puertos de comunicación necesarios.	Evite el error de instalación o los retrasos abriendo los puertos de comunicación necesarios antes de intentar instalarData Protection for VMware.
4	Instalar Data Protection for VMware: • Instalación de Data Protection for VMware utilizando el asistente de instalación • "Instalación de los componentes de Data Protection for VMware en modalidad silenciosa" en la página 24 Actualizar Data Protection for VMware: Actualización de Data Protection for VMware	Cada paquete de instalación se le presenta con un archivo de licencia de usuario (EULA). Si no acepta este archivo, la instalación finalizará.
5	"Configuración de una nueva instalación con el asistente" en la página 41 Si está planificando actualizar Data Protection for VMware, en función de los componentes que se instalen, es posible que sea necesario realizar más tareas de configuración. Consulte los temas de configuración de *IBM Spectrum Protect for Virtual Environments: Data Protection for VMware - Guía del usuario* para obtener más detalles.	Utilice el asistente de configuración para una configuración inicial. Dependiendo de las funciones que estén instaladas, se necesitan más tareas de configuración como las que se describen en esta sección.

Consejo: Para ayudarle a planificar la cantidad de hosts proxy que son necesarios para el entorno de copia de seguridad de Data Protection for VMware específico, está disponible la siguiente documentación la wiki de IBM Spectrum Protect:
Guía paso a paso a vStorage Backup Server (Proxy) Sizing
Esta publicación está disponible en la sección de productos de IBM Spectrum Protect for Virtual Environments.

Escenarios de instalación

Antes de instalar Data Protection for VMware, elija el escenario que mejor se adapte a las necesidades de la empresa.

Puede instalar Data Protection for VMware y el transportador de datos utilizando la GUI o en modalidad silenciosa:

- "Instalación de los componentes de Data Protection for VMware utilizando el asistente de instalación" en la página 21
- "Instalación de los componentes de Data Protection for VMware en modalidad silenciosa" en la página 24

Para obtener una lista de características y componentes que están disponibles por plataforma, consulte "Componentes instalables" en la página 1.

Tabla 3. Escenarios de instalación

Número de escenario	Descripción	Tareas que debe completar
1	Utilice este escenario para una instalación nueva donde desea instalar Data Protection for VMware y el transportador de datos en el mismo sistema.	Windows Puede utilizar el instalador de suite en la GUI o en modalidad silenciosa. Linux Puede utilizar InstallAnywhere en la GUI o en modalidad silenciosa.
2	Utilice este escenario para una instalación nueva en la que desea instalar solo Data Protection for VMware.	Windows Puede completar una instalación personalizada utilizando el instalador de suite para instalar Data Protection for VMware en la GUI o en modalidad silenciosa. Linux Puede completar una instalación personalizada utilizando InstallAnywhere para instalar Data Protection for VMware en la GUI o en modalidad silenciosa.
3	Utilice este escenario cuando desee instalar sólo el transportador de datos en un sistema.	Windows Puede completar una instalación personalizada utilizando el instalador de suite. Linux La característica del transportador de datos ahora está instalada con Data Protection for VMware.

Requisitos del sistema

Para implementar los componentes de Data Protection for VMware, el sistema debe cumplir con los requisitos de sistema adecuados.

requisitos de software

Tabla 4. Requisitos de software para Data Protection for VMware.

Componente	Requisito mínimo	Preferido
Sistema operativo	**Importante:** Los detalles sobre requisitos de software y sistema operativo pueden cambiar con el tiempo. Para obtener los requisitos de software actuales, consulte la Nota técnica 1505139.	
Protocolo de comunicaciones		
Controladores de dispositivo		
Otro software		

Requisitos de hardware

Los requisitos de hardware varían y dependen de los siguientes elementos:

- Número de servidores protegidos
- Número de volúmenes protegidos
- Tamaños del conjunto de datos

- Conectividad de LAN y SAN

  Nota: El componente agente de recuperación no da soporte a operaciones en un entorno sin LAN.

La tabla siguiente describe los requisitos de hardware que se necesitan para instalar Data Protection for VMware.

Tabla 5. Requisitos de hardware para Data Protection for VMware.

Componente	Requisito mínimo	Preferido
Sistema	Procesador IntelPentium D 3 GHz Dual Core o compatible	No aplicable
Memoria	2 GB RAM, espacio de dirección virtual de 2 GB	No aplicable
Disco duro disponible	200 MB para la carpeta 'Documents and Settings'	2 GB
Tarjeta NIC	1 NIC - 100 Mbps	1 NIC - 1 Gbps

Se necesita un host proxyWindows para agente de recuperación en Linux. Este host proxyWindows debe tener agente de recuperación instalado.

Restricción: Las siguientes restricciones se aplican a los VMDK de VMware que participan en una operación de copia de seguridad:

- En la modalidad de copia de seguridad incremental constante, cada VMDK implicado en una operación de copia de seguridad no puede superar los 8 TB. Si un VMDK tiene más de 8 TB, la operación de copia de seguridad falla. Si desea aumentar el tamaño de VMDK para que supere el valor predeterminado de 2 TB, especifique el tamaño máximo con la opción `vmmaxvirtualdisks`. Para obtener más información, consulte Vmmaxvirtualdisks.
- En la modalidad de copia de seguridad completa incremental constante, cada VMDK implicado en una operación de copia de seguridad no puede superar los 2 TB. Si un VMDK tiene más de 2 TB, la operación de copia de seguridad falla.

Para evitar una anomalía durante la modalidad de copia de seguridad, puede saltarse el proceso de VMDK especificando `vmskipmaxvirtualdisks yes` en el archivo de opciones del transportador de datos. Para obtener más información, consulte Vmskipmaxvirtualdisks .

Permisos de instalación necesarios

Antes de empezar la instalación, asegúrese de que el ID de usuario contiene el nivel de permiso necesario.

Acerca de esta tarea

Tabla 6. Permisos de usuario necesarios para instalar y configurar Data Protection for VMware

Sistema	Permiso necesario
Windows	Administrador
Linux	Root

Tabla 6. Permisos de usuario necesarios para instalar y configurar Data Protection for VMware (continuación)

Sistema	Permiso necesario
Servidor vCenter	Privilegios de administrador El rol de servidor vCenter requiere los privilegios siguientes: **Extensión** > **Registrar extensión, Anular registro de extensión, Actualizar extensión** Este nuevo rol se debe aplicar al objeto de vCenter en la jerarquía de servidor vCenter de VMware para el ID de usuario que se ha especificado durante la instalación.
Servidor de IBM Spectrum Protect **Restricción:** El servidor se debe iniciar.	Acceso administrativo (Privilegio de **Sistema** o **Dominio de políticas sin restricciones**)

Puertos de comunicación necesarios

Vea una lista de puertos de comunicación que son necesarios para abrirse en el cortafuegos al instalar Data Protection for VMware.

Los puertos identificados en la tabla reflejan una instalación típica. Una instalación típica consiste en los siguientes componentes en el mismo sistema Windows:

- Servidor Data Protection for VMware GUI
- Servidor de seguridad de vStorage (transportador de datos)
- Proxy de montaje de Windows
- Interfaz de restauración de archivos de IBM Spectrum Protect

Si se utiliza una instalación no típica, pueden ser necesarios más puertos.

Restricción: El proxy de montaje de Windows y el proxy de montaje de Linux deben estar en la misma subred.

Tabla 7. Puertos de comunicación necesarios. Esta tabla identifica los puertos a los que accede Data Protection for VMware.

Puerto TCP	Iniciador: de salida (de host)	Destino: De entrada (a host)
443	Servidor de seguridad vStorage	Servidor vCenter (HTTP seguro)
443	Servidor de Interfaz gráfica de usuario de Data Protection for VMware vSphere	Servidor vCenter
443 Este valor solo es necesario cuando el transportador de datos es un sistema Linux.	Proxy de montaje de Windows	Servidor vCenter
902 443	Servidor vCenter	Hosts ESXi
902 443	Servidor de seguridad vStorage (proxy)	Hosts ESXi (todos los hosts protegidos)

Tabla 7. Puertos de comunicación necesarios (continuación). Esta tabla identifica los puertos a los que accede Data Protection for VMware.

Puerto TCP	Iniciador: de salida (de host)	Destino: De entrada (a host)
1500 (**tcpport**)	Servidor de seguridad vStorage (proxy)	Servidor de IBM Spectrum Protect
1500 (**tcpadminport**)	Servidor de Interfaz gráfica de usuario de Data Protection for VMware vSphere • 1500 (**tcpadminport**) es comunicación no SSL • Para la comunicación SSL, **tcpadminport** es el único puerto que soporta la comunicación SSL con el servidor de IBM Spectrum Protect. El número de puerto correcto a utilizar para el protocolo SSL es normalmente el valor especificado por la opción **ssltcpadminport** en el archivos dsmserv.opt del servidor de IBM Spectrum Protect. Sin embargo, si se especifica **adminonclient no** en el archivo dsmserv.opt, el número de puerto correcto a utilizar para el protocolo SSL es el valor especificado por la opción **ssltcpadminport**. La opción **ssltcpadminport** no tiene un valor predeterminado. Por lo tanto, el valor debe ser especificado por el usuario.	Servidor de IBM Spectrum Protect
1527 Base de datos Derby interna		
1501 1581 (**httpport**)	Servidor de IBM Spectrum Protect	Servidor de seguridad vStorage • Planificador del transportador de datos • Cliente Web • Daemon de aceptador de cliente
1581 (**httpport**) 1582, 1583 (**webports**)	Servidor de Interfaz gráfica de usuario de Data Protection for VMware vSphere	Servidor de seguridad vStorage
9081 Servidor web de GUI (protocolo HTTPS)	Cliente de vSphere	Servidor de Interfaz gráfica de usuario de Data Protection for VMware vSphere (puerto HTTPS seguro para acceder a vCenter a través de navegador web)

Tabla 7. Puertos de comunicación necesarios (continuación). Esta tabla identifica los puertos a los que accede Data Protection for VMware.

Puerto TCP	Iniciador: de salida (de host)	Destino: De entrada (a host)
22 Puerto predeterminado de SSH para el agente de recuperación	Agente de recuperación	Host de "montaje" de Data Protection for VMware de Windows • Agente de recuperación SSH para Linux
3260	Restauración de archivos Linux de Data Protection for VMware	Host de "montaje" de Data Protection for VMware de Windows • iSCSI
3260 Puerto predeterminado iSCSI para agente de recuperación	Destino de Windows con disco dinámico para restauración de archivos	Host de "montaje" de Data Protection for VMware de Windows • iSCSI
5985	Operaciones de la GUI de restauración de archivos	Windows Remote Management
135	Proxy de montaje de Windows	Máquina virtual de VMware que contiene los archivos que se van a restaurar con la interfaz de restauración de archivos de IBM Spectrum Protect

Requisitos de privilegios de usuario del servidor de VMware vCenter

Son necesarios ciertos privilegios del servidor de VMware vCenter para ejecutar operaciones de Data Protection for VMware.

Privilegios del servidor vCenter necesarios para proteger los centros de datos de VMware con la vista del explorador web para la Interfaz gráfica de usuario de Data Protection for VMware vSphere

El ID de usuario del servidor de vCenter que inicia sesión en la vista de navegador para la Interfaz gráfica de usuario de Data Protection for VMware vSphere

debe tener suficientes privilegios de VMware para ver el contenido del centro de datos gestionado mediante la GUI.

Por ejemplo, un entorno de VMware vSphere contiene cinco centros de datos. Un usuario, “jenn”, tiene privilegios suficientes únicamente para dos de estos centros de datos. Como resultado, únicamente estos dos centros de datos donde existen privilegios suficientes son visibles para “jenn” en las vistas. Los otros tres centros de datos (donde “jenn” no tiene privilegios) no son visibles para el usuario “jenn”.

El servidor de VMware vCenter define un conjunto de privilegios de forma colectiva como rol. Un rol se aplica a un objeto para usuario o grupo especificado para crear un privilegio. Desde el cliente web de VMware vSphere, debe crear un rol con un conjunto de privilegios. Para crear un rol del servidor de vCenter para operaciones de copia de seguridad y restauración, utilice la función **Añadir un rol**

del cliente de VMware vSphere. Debe asignar este rol a un ID de usuario para un vCenter Server o centro de datos especificados. Si quiere propagar los privilegios a todos los centros de datos del vCenter, especifique el servidor vCenter y seleccione la casilla de verificación `propagar a hijos`. También puede limitar los permisos si asigna el rol solo a los centros de datos necesarios con la casilla de verificación `propagar a hijos` seleccionada. La implementación para la del navegador se encuentra en el nivel del centro de datos.

El ejemplo siguiente muestra cómo controlar el acceso a los centros de datos para dos grupos de usuarios de VMware. En primer lugar, cree un rol que contenga todos los privilegios definidos en nota técnica 7047438. El conjunto de privilegios de este ejemplo se identifica mediante el rol denominado "TDPVMwareManage". El grupo 1 necesita acceso para gestionar máquinas virtuales en los centros de datos `Primary1_DC` y `Primary2_DC`. El grupo 2 necesita acceso para gestionar máquinas virtuales en los centros de datos `Secondary1_DC` y `Secondary2_DC`.

Para el grupo 1, asigne el rol "TDPVMwareManage" a los centros de datos `Primary1_DC` y `Primary2_DC`. Para el grupo 2, asigne el rol "TDPVMwareManage" a los centros de datos `Secondary1_DC` y `Secondary2_DC`.

Los usuarios de cada grupo de usuarios de VMware pueden utilizar la GUI Data Protection for VMware para gestionar máquinas virtuales únicamente en sus respectivos centros de datos.

Consejo: Cuando cree un rol, plantéese añadir privilegios adicionales al rol que pueda necesitar más adelante para completar otras tareas en los objetos.

Privilegios del servidor de vCenter para utilizar el transportador de datos

El transportador de datos de IBM Spectrum Protect instalado en el Servidor de seguridad vStorage (el nodo de transportador de datos) necesita las opciones `VMCUser` y `VMCPw`. La opción `VMCUser` especifica el ID de usuario del vCenter o servidor ESX que quiere consultar, restaurar o del que quiere hacer una copia de seguridad. Los privilegios asignados a este ID de usuario (`VMCUser`) garantizan que el cliente puede ejecutar operaciones en la máquina virtual y en el entorno VMware. Este ID de usuario debe tener los privilegios de VMware descritos en nota técnica 7047438.

Para crear un rol del servidor de vCenter para operaciones de copia de seguridad y restauración, utilice la función **Añadir un rol** del cliente de VMware vSphere. Tiene que seleccionar la opción `propagar a hijos` al añadir privilegios para este ID de usuario (`VMCUser`). Considere además si quiere añadir otros privilegios a este rol para desempeñar tareas distintas a la copia de seguridad y restauración. Para la opción `VMCUser`, la implementación se produce en el objeto de más alto nivel.

Privilegios del servidor vCenter necesarios para proteger los centros de datos de VMware con la vista de la Extensión de IBM Spectrum Protect para la Interfaz gráfica de usuario de Data Protection for VMware vSphere

La Extensión de IBM Spectrum Protect necesita un conjunto de privilegios independientes de los privilegios necesarios para iniciar sesión en la GUI.

Durante la instalación, se crean los privilegios personalizados siguientes para la Extensión de IBM Spectrum Protect:

- **Centro de datos** > **IBM Data Protection**
- **Global** > **IBM Data Protection**

Los privilegios personalizados necesarios para la Extensión de IBM Spectrum Protect se registran como una extensión independiente. La clave de extensión de privilegios es `com.ibm.tsm.tdpvmware.IBMDataProtection.privileges`.

Estos privilegios permiten que el administrador de VMware pueda habilitar e inhabilitar el acceso al contenido de la Extensión de IBM Spectrum Protect. Únicamente los usuarios que tengan estos privilegios personalizados en el objeto de VMware necesario podrán acceder al contenido de la Extensión de IBM Spectrum Protect. Se registra una Extensión de IBM Spectrum Protect para cada servidor de vCenter, y se comparte entre todos los hosts de la GUI configurados para dar soporte al servidor de vCenter.

Desde el cliente web de VMware vSphere, debe crear un rol para los usuarios que puedan completar funciones de protección de datos para máquinas virtuales utilizando la Extensión de IBM Spectrum Protect. Para este rol, además de los privilegios de rol de administrador de máquina virtual estándares necesarios para el cliente web, debe especificar el privilegio **Centro de datos** > **IBM Data Protection**. Para cada centro de datos, asigne este rol para cada usuario o grupo de usuarios donde desee otorgar permiso para que el usuario pueda gestionar máquinas virtuales.

El privilegio **Global** > **IBM Data Protection** es necesario para el usuario a nivel vCenter. Este privilegio permite al usuario gestionar, editar o eliminar la conexión entre el servidor vCenter y el servidor web de Interfaz gráfica de usuario de Data Protection para VMware vSphere. Asigne este privilegio a los administradores que estén familiarizados con la Interfaz gráfica de usuario de Data Protection para VMware vSphere que protege sus respectivos servidores vCenter. Gestione sus conexiones de Extensión de IBM Spectrum Protect en la página Conexiones de la extensión.

El siguiente ejemplo muestra cómo controlar el acceso a los centros de datos para dos grupos de usuarios. El grupo 1 necesita acceso para gestionar máquinas virtuales para los centros de datos `NewYork _DC` y `Boston_DC`. El grupo 2 necesita acceso para gestionar máquinas virtuales para los centros de datos `LosAngeles_DC` y `SanFrancisco_DC`.

Desde el cliente de VMware vSphere, cree por ejemplo el rol "IBMDataProtectManage", asigne los privilegios de rol de administrador de máquina virtual y también el privilegio **Centro de datos** > **IBM Data Protection**.

Para el grupo 1, asigne el rol "IBMDataProtectManage" a los centros de datos `NewYork_DC` y `Boston_DC`. Para el grupo 2, asigne el rol "IBMDataProtectManage" a los centros de datos `LosAngeles_DC` y `SanFranciso_DC`.

Los usuarios de cada grupo pueden utilizar la Extensión de IBM Spectrum Protect en el cliente web de vSphere para gestionar máquinas virtuales sólo en sus respectivos centros de datos.

Problemas relacionados con permisos insuficientes

Cuando el usuario del explorador web no tiene permisos suficientes para cualquier centro de datos, se bloquea el acceso a la vista. En su lugar, se emite el mensaje de error GVM2013E para indicar que el usuario no está autorizado a acceder a ningún

centro de datos gestionado debido a que no tiene los permisos suficientes. También hay disponibles otros mensajes nuevos que informan al usuario de problemas derivados de no tener suficientes permisos. Para solucionar cualquier problema relacionado con permisos, asegúrese de que el rol de usuario esté configurado tal y como se describe en las secciones anteriores. El rol de usuario tiene que tener todos los privilegios identificados en la tabla Privilegios necesarios para el ID de usuario del servidor de vCenter y para el transportador de datos, y estos privilegios tienen que aplicarse a nivel de centro de datos con la casilla de verificación `propagar a hijos`.

Cuando el usuario de Extensión de IBM Spectrum Protect no tiene los permisos suficientes para un centro de datos, las funciones de protección de datos para dicho centro de datos y su contenido se convierten en no disponibles en la extensión.

Cuando el ID de usuario IBM Spectrum Protect (especificado por la opción `VMCUser`) contiene permisos insuficientes para una operación de copia de seguridad y restauración, se muestra el siguiente mensaje:

```
ANS9365E Error de la API de VMware vStorage.
"El permiso para realizar esta operación se ha denegado".
```

Cuando el ID de usuario de IBM Spectrum Protect no contiene permisos suficientes para ver una máquina, se muestran los mensajes siguientes:

```
Se ha iniciado el mandato de copia de seguridad de la máquina virtual.  Número total de máquinas vir
ANS4155E No se ha podido encontrar la máquina virtual 'tango' en el servidor
de VMware.
ANS4148E La copia de seguridad de máquina virtual completa de la máquina virtual
'foxtrot' ha fallado con RC 4390
```

Para recuperar la información de registro a través del servidor del centro virtual VMware para ver problemas de permisos, realice estos pasos:

1. En Valores del servidor de vCenter, seleccione **Opciones de registro** y establezca **Registro de vCenter** en **Trivia (Trivialidad)**.
2. Vuelva a crear el error de permisos.
3. Restablezca el **Registro de vCenter** a su valor anterior para evitar el registro de una cantidad excesiva de información de registro.
4. En Registros del sistema, busque el registro del servidor de vCenter más actual (`vpxd-`*`wxyz`*`.log`) y busque la serie `NoPermission`. Por ejemplo:

   ```
   [2011-04-27 15:15:35.955 03756 verbose 'App'] [VpxVmomi] Invoke error:
   vim.VirtualMachine.createSnapshot session: 92324BE3-CD53-4B5A-B7F5-96C5FAB3F0EE
   Throw: vim.fault.NoPermission
   ```

   Este mensaje de registro indica que el ID de usuario no contenía permisos suficientes para crear una instantánea (`createSnapshot`).

Claves de registro de la GUI de Data Protection for VMware

En función de las opciones que seleccione durante la instalación, puede acceder a la GUI de Data Protection for VMware utilizando distintos métodos. Se crean claves de registro para las GUI de Data Protection for VMware.

La frase "GUI de Data Protection for VMware" se aplica a las siguientes GUI:

- La Interfaz gráfica de usuario de Data Protection for VMware vSphere accedida en un navegador web
- La Extensión de IBM Spectrum Protect en la GUI de vSphere Web Client.

La clave de registro de la Extensión de IBM Spectrum Protect es `com.ibm.tsm.tdpvmware.IBMDataProtection`. Esta clave se registra cuando selecciona el recuadro de selección **Registrar la extensión vSphere Web Client** durante la instalación. Se registra una única instancia de Extensión de IBM Spectrum Protect por servidor de vCenter.

No se crea una clave de registro para la Interfaz gráfica de usuario de Data Protection for VMware vSphere a la que se accede en un navegador web.

Para ver las claves de registro, inicie una sesión en VMware Managed Object Browser (MOB). Después de iniciar una sesión en MOB, vaya a **Content→Extension Manager** para ver las claves de registro.

Instalación de los componentes de Data Protection for VMware

Puede instalar todos o algunos de los componentes que están disponibles en el paquete de Data Protection for VMware para el sistema operativo.

Acerca de esta tarea

Mediante el uso del instalador de Data Protection for VMware, puede instalar los siguientes componentes:

- Agente de recuperación de IBM Spectrum Protect
- Windows Interfaz de línea de mandatos de agente de recuperación
- Windows Documentación (archivo léame y avisos de noticias)
- Archivo de habilitación de Data Protection for VMware
- Interfaz gráfica de usuario de Data Protection for VMware vSphere
- Característica de transportador de datos, que incluye los siguientes elementos:
  - GUI de transportador de datos
  - Cliente web del transportador de datos
  - Archivos de tiempo de ejecución de API de cliente (64 bits)
  - Línea de comandos del cliente de administración
  - Archivos de tiempo de ejecución de VMware vStorage API

Consejo: Puede crear varios transportadores de datos en el mismo sistema que el software de Data Protection for VMware o puede crear transportadores de datos en sistemas remotos. Esta configuración aumenta los recursos disponibles para que los utilice Data Protection for VMware. Los sistemas con el transportador de datos instalado se denominan servidores de copia de seguridad vStorage.

Obtención del paquete de instalación de Data Protection for VMware

Puede obtener el paquete de instalación de Data Protection for VMware de un sitio de descarga de IBM, por ejemplo IBM Passport Advantage.

Linux

Antes de empezar

Si tiene la intención de descargar los archivos, establezca el límite de usuario del sistema para el tamaño máximo de archivo en ilimitado para garantizar que los archivos se pueden descargar correctamente:

1. Para consultar el valor de tamaño de archivo máximo, emita el mandato siguiente:

   ```
   ulimit -Hf
   ```

2. Si el límite de usuario de sistema para el tamaño máximo de archivo no está establecido en ilimitado, cámbielo a ilimitado, siguiendo las instrucciones de la documentación del sistema operativo.

Procedimiento

1. Descargue el archivo de paquete correspondiente de uno de los siguientes sitios web:
   - Para una primera instalación o un nuevo release vaya a Passport Advantage en: http://www.ibm.com/software/lotus/passportadvantage/. Passport Advantage es el único sitio del que puede descargar un archivo de paquete con licencia.
   - Para obtener la información más reciente, actualizaciones y arreglos de mantenimiento, vaya al sitio de soporte de IBM Spectrum Protect: http://www.ibm.com/support/entry/portal/Overview/Software/Tivoli/Tivoli_Storage_Manager.
2. Si ha descargado el paquete de un sitio de descarga de IBM, complete los pasos siguientes:
   a. Descargue el archivo de paquete en el directorio de su elección. La vía de acceso no debe contener más de 40 caracteres. Asegúrese de extraer los archivos de instalación en un directorio vacío. No extraiga en un directorio que contenga archivos extraídos anteriormente ni ningún otro archivo.
   b. Linux Asegúrese de que el permiso ejecutable está establecido para el paquete. Si es necesario, cambie los permisos de archivo emitiendo el mandato siguiente:

      ```
      chmod a+x nombre_paquete.bin
      ```

   c. Linux Extraiga el paquete emitiendo el mandato siguiente:

      ```
      ./nombre_paquete.bin
      ```

      donde *package_name* es el nombre del archivo descargado, por ejemplo, `8.1.0.000-TIV-TSM4VE-LinuxX64.bin`.
   d. Windows Extraiga el paquete realizando una doble pulsación en *nombre_paquete*, donde *nombre_paquete* es el nombre del archivo descargado, por ejemplo, `8.1.0.000-TIV-TSM4VE-Windows.exe`.

Instalación de los componentes de Data Protection for VMware utilizando el asistente de instalación

Puede instalar los componentes de Data Protection for VMware utilizando el asistente de instalación.

Acerca de esta tarea

Windows Puede utilizar el instalador de suite para instalar Data Protection for VMware y el transportador de datos.

Linux Puede utilizar el instalador autónomo para instalar Data Protection for VMware y el transportador de datos.

Instalación de los componentes de Data Protection for VMware en sistemas Windows

Instalar componentes y características de Data Protection for VMware utilizando el asistente de instalación.

Antes de empezar

Antes de instalar los componentes de Data Protection for VMware, asegúrese de que se cumplen los siguientes requisitos:

- Un ID de usuario con acceso de privilegios de administrador.
- Conectividad de red a un VMware vCenter Server 5.x (o posterior) con acceso de privilegios de administrador.
- Conectividad de red a un servidor de IBM Spectrum Protect con acceso de administrador (privilegio **Sistema** o **Dominio de políticas sin restricciones**). Este servidor debe estar disponible y en ejecución.
- Asegúrese de revisar los siguientes requisitos:
  - "Requisitos del sistema" en la página 11
  - "Permisos de instalación necesarios" en la página 12
  - "Puertos de comunicación necesarios" en la página 13

Antes de instalar Data Protection for VMware, debe ser consciente de las siguientes opciones:

Tipo de instalación

Instalación típica
Con las instalaciones típicas, se instalan todos los componentes y las características de Data Protection for VMware.

Instalación avanzada
Con las instalaciones avanzadas, puede seleccionar los componentes y las características que desea instalar.

Protección del entorno en un entorno de vSphere
Con la Interfaz gráfica de usuario de Data Protection for VMware vSphere, puede realizar copias de seguridad, restaurar y gestionar máquinas virtuales en un entorno VMware vCenter.

Acerca de esta tarea

Puede utilizar el Instalador de suite para instalar Data Protection for VMware. El archivo `spinstall.exe` para el Instalador de suite está ubicado en la raíz del paquete de instalación.

Para obtener una lista de componentes y características que puede instalar, consulte "Componentes instalables" en la página 1.

Procedimiento

Para instalar Data Protection for VMware, complete los siguientes pasos desde la ubicación del archivo `spinstall.exe` para el componente que ha elegido instalar:

1. Efectúe una doble pulsación en el archivo `spinstall.exe`.
2. Siga las instrucciones del asistente para instalar los componentes seleccionados. Al instalar el agente de recuperación para restauración instantánea, debe también seleccionar el controlador de dispositivo para la instalación. De forma predeterminada no está seleccionado.

Qué hacer a continuación

Para acceder a la Interfaz gráfica de usuario de Data Protection for VMware vSphere, consulte lo siguiente:

- "Acceso a la Interfaz gráfica de usuario de Data Protection for VMware vSphere" en la página 32

El asistente de configuración se muestra automáticamente la primera vez que se inicia la GUI.

Instalación de Data Protection for VMware en sistemas Linux

Instalar Data Protection for VMware en sistemas Linux utilizando la modalidad InstallAnywhere.

Antes de empezar

Antes de instalar Data Protection for VMware, asegúrese de que se cumplen los siguientes requisitos:

- Asegúrese de que el ID de usuario tiene el nivel de permiso necesario y que los puertos de comunicación necesarios están abiertos antes de continuar.
- El proceso de instalación crea el usuario `tdpvmware`. Debe emitir todos los mandatos de **`vmcli`** como usuario `tdpvmware` y con el ID de usuario root.
- X Window Server es necesario cuando se instala en modalidad de consola.
- Asegúrese de revisar los siguientes requisitos:
  - "Requisitos del sistema" en la página 11
  - "Permisos de instalación necesarios" en la página 12
  - "Puertos de comunicación necesarios" en la página 13

Procedimiento

Para instalar Data Protection for VMware, complete los pasos siguientes:

1. Desde la raíz de la carpeta de instalación, cambie al directorio `CD/Linux/DataProtectionForVMware`.
2. En una línea de mandatos, entre el mandato siguiente:

```
./install-Linux.bin
```

Resultados

Si recibe avisos o errores, consulte los archivos de registro para obtener más información. Consulte “Actividad del archivo de registro” en la página 79.

Si no puede instalar Data Protection for VMware debido a un error, consulte el procedimiento "Eliminación manual de Data Protection for VMware" en “Desinstalación de Data Protection for VMware en un sistema Linux” en la página 39.

Realización de una instalación limpia de Data Protection for VMware en Linux

Si se interrumpe una instalación en Linux, normalmente puede reiniciarla. Sin embargo, si la instalación no se puede reiniciar, se necesita una instalación limpia.

Acerca de esta tarea

Antes de iniciar una instalación limpia, asegúrese de que el producto se ha eliminado. Siga estos pasos para garantizar un entorno limpio:

Procedimiento

1. Si se ha instalado la Interfaz gráfica de usuario de Data Protection for VMware vSphere, realice estas tareas:
   a. Detenga la Interfaz de línea de mandatos de Data Protection for VMware emitiendo este mandato:
   `/etc/init.d/vmcli stop`
   b. Detenga el servidor web de GUI de Data Protection for VMware emitiendo este mandato:
   `/etc/init.d/webserver stop`
   c. Elimine el paquete `.rpm` emitiendo este comando:
   `rpm -e TIVsm-TDPVMwarePlugin`
2. Elimine las entradas del producto de Motor de despliegue:
   a. Emita el siguiente comando para mostrar todas las entradas de Motor de despliegue:
   `/usr/ibm/common/acsi/bin/de_lsrootiu.sh`
   b. Emita el siguiente comando para eliminar todas las entradas de Motor de despliegue:
   `/usr/ibm/common/acsi/bin/deleteRootIU.sh <UUID> <discriminant>`
   c. Elimine el directorio `/var/ibm/common`.
   d. Elimine el directorio `/usr/ibm/common`.
   e. Limpie el directorio de `/tmp` eliminando el archivo `acu_de.log`, si existe.
   f. Elimine el directorio `/tmp` que contiene el ID del usuario que ha instalado el motor de despliegue
   g. Elimine todas las entradas del motor de despliegue del archivo del sistema `/etc/inittab`. Las entradas están delimitadas por `#Begin AC Solution Install block` y `#End AC Solution Install block`. Elimine todo el texto entre esos delimitadores y elimine el propio texto del delimitador.
   h. Elimine todas las referencias del motor de despliegue del archivo del sistema `/etc/services`.
3. Elimine todos los archivos de Data Protection for VMware de la instalación errónea:

a. Elimine los archivos de <*USER_INSTALL_DIR*>, que es la ruta en la que se llevó a cabo la instalación errónea. Por ejemplo: `/opt/tivoli/tsm/TDPVMware/`
b. Elimine todos los accesos directos del escritorio.

4. Realice una copia de seguridad del archivo de registro global (`/var/.com.zerog.registry.xml`). Tras realizar una copia de seguridad de este archivo, elimine todas las etiquetas que hagan referencia a Data Protection for VMware.
5. Elimine los archivos de registro de la raíz que contengan la serie `TDPVMware`. Por ejemplo:
`IA-TDPVMware-00.log` o `IA-TDPVMware_Uninstall-00.log`.
6. Elimine el usuario que haya ejecutado el Interfaz de línea de mandatos de Data Protection for VMware.
   a. Emita el mandato siguiente:
   ```
   userdel -r tdpvmware
   ```
   b. Emita el mandato siguiente:
   ```
   groupdel tdpvmware
   ```

   Consejo: En algunas versiones de Linux, el mandato **`userdel`** también elimina el grupo cuando no existe ningún otro usuario asociado. Como resultado, omita cualquier mensaje de error relacionado con mandatos.

Resultados

Tras completar estos pasos, inicie la instalación limpia.

Instalación de los componentes de Data Protection for VMware en modalidad silenciosa

Puede instalar Data Protection for VMware en segundo plano. Durante esta instalación silenciosa, no se muestran mensajes.

Acerca de esta tarea

Windows Puede utilizar el instalador de suite para instalar Data Protection for VMware y el transportador de datos.

Linux Puede utilizar el instalador autónomo para instalar Data Protection for VMware y el transportador de datos.

Instación de Data Protection for VMware en sistemas Windows en modalidad silenciosa

Instalar todos los componentes de Data Protection for VMware y la característica de transportador de datos utilizando el Instalador de suite en modalidad silenciosa.

Antes de empezar

Antes de instalar Data Protection for VMware y la característica de transportador de datos, asegúrese de que el sistema cumple con los requisitos en las siguientes secciones:

- “Requisitos del sistema” en la página 11
- “Permisos de instalación necesarios” en la página 12

- "Puertos de comunicación necesarios" en la página 13

Utilice los siguientes parámetros de Data Protection for VMware con las características de instalación silenciosa:

Tabla 8. Parámetros de instalación silenciosa de Data Protection for VMware

Parámetro	Descripción	Valor predeterminado
ISFeatureInstall	Especifique una o las dos opciones siguientes: **TSM4VE** Instalar todas las características de Protección de datos para VMware salvo el controlador de dispositivo del agente de recuperación. **Cliente** Instalar todas las características del transportador de datos.	`TSM4VE,Client`
ComponentsToInstallVe	Especificar las características de Protección de datos para VMware a instalar. Usar las características descritas en Tabla 9 en la página 26	Ninguna.
ComponentsToInstallBa	Especifique las características de movimiento de datos a instalar. Use las características descritas en Tabla 10 en la página 27	Ninguna.
GUI_MODE	Para proteger los datos en un entorno de vSphere, especifique **GUI_MODE=vcenter**. Este parámetro instala la Interfaz gráfica de usuario de Data Protection for VMware vSphere. Esta GUI integra el producto con el cliente de VMware vSphere para hacer copia de seguridad, restaurar y gestionar las VM en un entorno de VMware vCenter. Incluye la Interfaz de línea de mandatos de Data Protection for VMware. Sólo puede instalar una Interfaz gráfica de usuario de Data Protection for VMware vSphere en una máquina. Como consecuencia, no se permiten varias GUI de Data Protection for VMware vSphere en la misma máquina. `vcenter` es el valor predeterminado cuando se especifica **GUI_MODE**.	`vcenter`
VCENTER_HOSTNAME	El nombre de dominio completo o la dirección IP de vCenter Server. Esta característica es necesaria cuando se especifica **GUI_MODE=vcenter**.	Ninguna.
VCENTER_USERNAME	ID de usuario de vCenter. Este ID de usuario debe ser un administrador de VMware que tenga permiso para registrar extensiones y anular el registro de las mismas. Esta característica es necesaria cuando se especifica **GUI_MODE=vcenter**.	Ninguna.
VCENTER_PASSWORD	Contraseña de vCenter. Esta característica es necesaria cuando se especifica **GUI_MODE=vcenter**.	Ninguna.

Tabla 8. Parámetros de instalación silenciosa de Data Protection for VMware (continuación)

Parámetro	Descripción	Valor predeterminado
DIRECT_START	(Sólo vSphere) Para acceder a la Interfaz gráfica de usuario de Data Protection for VMware vSphere en un navegador web, especifique **DIRECT_START=1**. Se accede a la Interfaz gráfica de usuario de Data Protection for VMware vSphere a través de un marcador de URL en el servidor web de GUI. Si no desea acceder la Interfaz gráfica de usuario de Data Protection for VMware vSphere en un navegador web, especifique **DIRECT_START=0**.	1 **Importante:** Cuando la instalación se ha completado, el valor **DIRECT_START** no se puede cambiar excepto si se reinstala el producto.
REGISTER_EXTENSION	(Sólo VSphere) Para acceder a la GUI de vSphere de Data Protection for VMware como una extensión del cliente web de vSphere, especifique **REGISTER_EXTENSION=1**.	0
DB_PORT	Número de puerto TCP/IP para la base de datos Derby.	1527
WC_DEFAULTHOST	Protocolo HTTP para el servidor web de GUI.	9080
WEBSERVER_SECUREPORT	Protocolo HTTPS para el servidor web de GUI.	9081

Tabla 9. Características de instalación silenciosa de Data Protection for VMware

Característica	Descripción	¿Instalada de forma predeterminada?
shell	Interfaz de línea de mandatos de agente de recuperación Interfaz de línea de mandatos que se utiliza para operaciones de montaje (`RecoveryAgentShell.exe`).	Sí
LAP	Licencia de Data Protection for VMware	Sí
TSMLicence	Archivo de habilitación de Data Protection for VMware Permite a IBM Spectrum Protect ejecutar los siguientes tipos de copia de seguridad: • Copia de seguridad incremental constante • Copia de seguridad completa incremental constante Si descarga cargas de trabajo de copia de seguridad, este archivo debe estar instalado en el servidor de seguridad vStorage.	Sí
documents	Archivo léame	Sí
gui	Interfaz gráfica de usuario de Data Protection for VMware vSphere	No

Utilice los siguientes parámetros de transportador de datos con las características de instalación silenciosa:

Tabla 10. Parámetros de instalación silenciosa de transportador de datos

Parámetro	Descripción	Valor predeterminado
BackupArchiveGUI	GUI del transportador de datos de IBM Spectrum Protect	Ninguna.
BackupArchiveWeb	Cliente web del transportador de datos de IBM Spectrum Protect	Ninguna.
Api64Runtime	Tiempos de ejecución de API de IBM Spectrum Protect	Ninguna.
AdministrativeCmd	Línea de mandatos administrativos de IBM Spectrum Protect	Ninguna.

Acerca de esta tarea

Restricción: Todas las característica se instalan en la ubicación predeterminada. Para localizar los directorios de instalación predeterminados para los componentes, consulte los subtemas en "Componentes instalables" en la página 1.

Procedimiento

Para instalar Data Protection for VMware, complete los siguientes pasos desde el directorio donde ha extraído el paquete:

1. Abra un indicador de mandatos y acceda a la ubicación del archivo `spinstall.exe` para el componente que quiere instalar.
2. Especifique las características a instalar.
   El ejemplo siguiente instala el agente de recuperación, el controlador de dispositivo y la interfaz de línea de mandatos del agente de recuperación de IBM Spectrum Protect:

   ```
   spinstall.exe ISFeatureInstall=TSM4VE ComponentsToInstallVe=mount,mountdriver,shell
   REBOOT=ReallySuppress SUITE_MODE=1 /silent
   ```

   El ejemplo siguiente instala un subconjunto de Data Protection for VMware y las características del transportador de datos:

   ```
   spinstall.exe ISFeatureInstall=Client,TSM4VE /silent
   ComponentsToInstallBa=BackupArchiveGUI,BackupArchiveWeb,Api64Runtime
   ComponentsToInstallVe=LAP,TSMLicence,documents,gui  SUITE_MODE=1 REBOOT=ReallySuppress
   GUI_MODE=vcenter VCENTER_HOSTNAME=nombre_host
   VCENTER_USERNAME=nombre_usuario VCENTER_PASSWORD=contraseña
   DIRECT_START=1
   ```

   En el ejemplo siguiente se instalan todas las características del transportador de datos y de Data Protection for VMware:

   ```
   spinstall.exe /silent SUITE_MODE=1 REBOOT=ReallySuppress
   GUI_MODE=vcenter VCENTER_HOSTNAME=nombre_host VCENTER_USERNAME=nombre_usuario
   VCENTER_PASSWORD=contraseña DIRECT_START=1
   ```

3. Opcional: Cuando se instale el controlador de dispositivo, debe reiniciar el sistema.

Nota: El mensaje siguiente se visualiza la primera vez que se monta un volumen:

```
El Virtual Volume Driver aún no está registrado. El agente de recuperación puede registrar
el controlador ahora. Durante el registro, puede aparecer un aviso de logotipo de Microsoft
Windows.
Acepte esta advertencia para permitir que se complete el registro.
¿Desea registrar ahora el conductor de volumen virtual?
```

Debe registrar el controlador de volumen virtual para continuar con las operaciones de agente de recuperación.

Tareas relacionadas:

"Desinstalación de Data Protection for VMware for Windows en modalidad silenciosa" en la página 38

Instalación de Data Protection for VMware en sistemas Linux en modalidad silenciosa

Puede personalizar qué características de Data Protection for VMware se deben instalar silenciosamente en un sistema operativo Linux.

Antes de empezar

Antes de instalar Data Protection for VMware, asegúrese de que se cumplen los siguientes requisitos:

- Asegúrese de que el ID de usuario tiene el nivel de permiso necesario y que los puertos de comunicación necesarios están abiertos antes de continuar.
- El proceso de instalación crea el usuario `tdpvmware`. Debe emitir todos los mandatos de **`vmcli`** como usuario `tdpvmware` y con el ID de usuario root.
- X Window Server es necesario cuando se instala en modalidad de consola.
- Asegúrese de revisar los siguientes requisitos:
  - "Requisitos del sistema" en la página 11
  - "Permisos de instalación necesarios" en la página 12
  - "Puertos de comunicación necesarios" en la página 13

Acerca de esta tarea

Data Protection for VMware proporciona las características de instalación silenciosa siguientes para los sistemas operativos Linux:

Tabla 11. Características de instalación silenciosa de Data Protection for VMware

Característica	Descripción	¿Instalada de forma predeterminada?
Documentos	Archivo léame	Sí

Tabla 11. Características de instalación silenciosa de Data Protection for VMware (continuación)

Característica	Descripción	¿Instalada de forma predeterminada?
TDPVMwareDM	La instalación de esta característica incluye el archivo de habilitación. Permite a IBM Spectrum Protect ejecutar los siguientes tipos de copia de seguridad: • Copia de seguridad de VM incremental periódica • Copia de seguridad incremental para siempre de VM completa • Copia de seguridad de VM incremental para siempre Si descarga cargas de trabajo de copia de seguridad, este archivo debe estar instalado en el servidor de seguridad vStorage.	Sí
TDPVMwareGUI	Interfaz gráfica de usuario de Data Protection for VMware vSphere. **Nota:** También incluye la instalación del archivo de habilitación.	No

Utilice los siguientes parámetros de Data Protection for VMware con las características de instalación silenciosa:

Tabla 12. Parámetros de instalación silenciosa de Data Protection for VMware para el archivo `installer.properties`

Parámetro	Descripción	Valor predeterminado
VCENTER_HOSTNAME	El nombre de dominio completo o la dirección IP de vCenter Server.	Ninguna.
VCENTER_USERNAME	ID de usuario de vCenter. Este ID de usuario debe ser un administrador de VMware que tenga permiso para registrar extensiones y anular el registro de las mismas.	Ninguna.
VCENTER_PASSWORD	Contraseña de vCenter.	Ninguna.
DIRECT_START	(Sólo vSphere) Para acceder a la Interfaz gráfica de usuario de Data Protection for VMware vSphere en un navegador web, especifique **DIRECT_START=YES**. Se accede a la Interfaz gráfica de usuario de Data Protection for VMware vSphere a través de un marcador de URL en el servidor web de GUI. Si no desea acceder a la Interfaz gráfica de usuario de Data Protection for VMware vSphere en un navegador web, especifique **DIRECT_START=NO**.	`YES` **Importante:** Cuando la instalación se ha completado, el valor **DIRECT_START** no se puede cambiar excepto si se reinstala el producto.
USERNAME	Nombre de usuario. Se crea un perfil para este nombre de usuario en `/home/<nombreusuario>/tdpvmware/config`.	`tdpvmware`

Tabla 12. Parámetros de instalación silenciosa de Data Protection for VMware para el archivo `installer.properties` (continuación)

Parámetro	Descripción	Valor predeterminado
REGISTER_EXTENSION	(Sólo VSphere) Para acceder a la GUI de vSphere de Data Protection for VMware como una extensión del cliente web de vSphere, especifique **REGISTER_EXTENSION=1**.	0
VMCLI_DB_PORT	Número de puerto TCP/IP para la base de datos Derby.	1527
WC_defaulthost	Protocolo HTTP para el servidor web de GUI.	9080
WebServer_Https	Protocolo HTTPS para el servidor web de GUI.	9081
Keystore_Password	Contraseña de almacén de claves para el servidor web de GUI. La contraseña debe tener un mínimo de seis caracteres válidos (a-z A-Z 0-9).	Ninguna.
SSL_Certificate	El proceso de instalación genera un certificado SSL autofirmado. Especifique el número de años a mantener activo este certificado SSL.	10

Procedimiento

Para instalar Data Protection for VMware, complete los siguientes pasos desde el directorio donde ha extraído el paquete de instalación:

1. Abra el archivo *vía_acceso*../Linux/DataProtectionForVMware/installer.properties y elimine el comentario en la siguiente entrada para aceptar la licencia (donde *vía_acceso* es la carpeta de instalación):

   ```
   LICENSE_ACCEPTED=TRUE
   ```

2. Seleccione uno de los siguientes métodos para instalar los componentes de Data Protection for VMware:
   - En una instalación predeterminada, abra la carpeta CD/Linux/DataProtectionForVMware y escriba el mandato siguiente:

     ```
     ./install-Linux.bin -i silent -LICENSE_ACCEPTED=true
     ```

   - Para una instalación personalizada, complete los siguientes pasos:
     a. Edite el archivo installer.properties con los valores adecuados:
        1) Especifique **INSTALL_MODE=Custom**. Asegúrese de que el signo de almohadilla (#) se ha eliminado de esta sentencia.
        2) Especifique las características que desea instalar con la opción **CHOSEN_INSTALL_FEATURE_LIST**. Por ejemplo, todas las características se instalan con el siguiente valor:

           ```
           CHOSEN_INSTALL_FEATURE_LIST=Docs,TDPVMwareDM,TDPVMwareGUI
           ```

        3) Especifique los parámetros installer.properties como se describe en Tabla 12 en la página 29.
     b. Desde la carpeta CD/Linux/DataProtectionForVMware, emita el siguiente mandato:

        ```
        ./install-Linux.bin -i silent -f installer.properties
        ```

Primeros pasos después de instalar Data Protection for VMware

Después de instalar Data Protection for VMware, prepárese para la configuración. El método preferido para configurar Data Protection for VMware consiste en utilizar el asistente de instalación.

Hoja de trabajo de configuración

Utilice esta hoja de trabajo para registrar la información que necesita al configurar y administrar Data Protection for VMware. La hoja de trabajo está destinada a ayudarle a recordar los valores que ha especificado después de la configuración.

Tabla 13. Hoja de trabajo de configuración de Data Protection for VMware

Elemento	Su valor	Notas
Información de servidor de IBM Spectrum Protect		
Dirección de servidor de IBM Spectrum Protect		
Puerto de servidor de IBM Spectrum Protect		
ID de administrador/contraseña de servidor de IBM Spectrum Protect		
Puerto de administrador de servidor de IBM Spectrum Protect		
Opciones de definición de nodo		
Prefijo a añadir a los nodos		
Dominio de políticas a utilizar al registrar nodos nuevos		
Nombre/Contraseña de nodo de vCenter		
Nombre/Contraseña de nodo de VMCLI		
Nombres/Contraseñas de nodo de Centro de datos **Recuerde:** Puede crear varios nodos de centro de datos.		El nombre de nodo de centro de datos consta del prefijo especificado, seguido de un carácter de subrayado, seguido del nombre de centro de datos. Por ejemplo: *prefijoNodo_nombreCentroDatos*
Nombres/Contraseñas de nodo de transportador de datos en el servidor de seguridad de vStorage **Recuerde:** Puede crear varios nodos de transportador de datos.		El nodo de transportador de datos consta del nombre de nodo de centro de datos, seguido de un carácter de subrayado, seguido de `DM`. Por ejemplo: *nombreNodoCentrodatos*_DM
Nombres/Contraseñas de nodo de transportador de datos en servidores remotos **Recuerde:** Puede crear varios nodos de transportador de datos que no están en el servidor de seguridad de vStorage.		
Nodo proxy de montaje El nodo proxy de montaje se utiliza al restaurar los datos.	Windows: Linux:	

Acceso a la Interfaz gráfica de usuario de Data Protection for VMware vSphere

Utilice Interfaz gráfica de usuario de Data Protection for VMware vSphere para hacer copias de seguridad, restaurar y gestionar máquinas virtuales en un entorno VMware vCenter.

Antes de empezar

Para poder acceder a la Interfaz gráfica de usuario de Data Protection for VMware vSphere, durante la instalación, tiene que haber seleccionado la opción para proteger los datos en un entorno de vSphere.

Procedimiento

- Si ha seleccionado la opción **Habilitar el acceso a la GUI a través de un navegador web**, durante la instalación, puede acceder a Interfaz gráfica de usuario de Data Protection for VMware vSphere desde el navegador:
  1. Abra un navegador web y entre el siguiente URL:

     `https://nombre_host:puerto/TsmVMwareUI`

     donde:
     - *nombre_host* es el nombre del sistema donde está instalada la Interfaz gráfica de usuario de Data Protection for VMware vSphere
     - *puerto* es el número de puerto a través del cual la GUI de vSphere es accesible. El número de puerto predeterminado es 9081.
  2. Inicie sesión utilizando el ID de usuario y contraseña de vCenter.
- Si no ha seleccionado la opción **Habilitar el acceso a la GUI a través de un navegador web**, durante la instalación, puede iniciar Interfaz gráfica de usuario de Data Protection for VMware vSphere realizando los pasos siguientes:
  1. Abra VMware vSphere Client e inicie sesión con el ID de usuario y contraseña de vCenter.
  2. En el panel Soluciones y aplicaciones del cliente de vSphere, pulse el icono de Interfaz gráfica de usuario de Data Protection for VMware vSphere.

Actualización de Data Protection for VMware

Puede actualizar Data Protection for VMware de una versión anterior del software. La actualización de Data Protection for VMware también requiere la actualización de otros componentes.

Consulte la IBM Spectrum Protect Snapshot for VMwareInstalación y guía del usuario cuando trabaje con este producto.

Para información sobre la compatibilidad con versiones anteriores, consulte la nota técnica 1648031.

Actualización de Data Protection for VMware

Este procedimiento documenta cómo actualizar a Data Protection for VMware V8.1.0.

Antes de empezar

Importante: Este procedimiento de actualización se aplica a un sistema sin IBM Spectrum Protect Snapshot for VMware instalado.

Para actualizar Data Protection for VMware, debe tener privilegios de administrador.

Las actualizaciones del Interfaz gráfica de usuario de Data Protection for VMware vSphere existente se llevan a cabo de la siguiente manera:

- Antes de que comience el proceso de actualización de Interfaz gráfica de usuario de Data Protection for VMware vSphere se realiza una copia de seguridad de los archivos de parámetros.
- Se utilizan los mismos números de puerto de base datos Derby y base predeterminada de WebSphere Application Server.
- Linux Los valores del perfil (`vmcliprofile`) se utilizan para Interfaz de línea de mandatos de Data Protection for VMware.

Restricción:

- Windows Cuando IBM Spectrum Protect for Virtual Environments se ha instalado en una ubicación no predeterminada, el proceso de actualización instala características de IBM Spectrum Protect for Virtual Environments V8.1.0 en el directorio de instalación predeterminado. No puede actualizar a una ubicación no predeterminada. Consulte los apartados en “Componentes instalables” en la página 1 para ver los directorios de instalación predeterminados para cada función.
- Linux Windows El proceso de actualización no instala nuevos componentes. Por ejemplo, si su versión anterior solo tiene la GUI de agente de recuperación instalada, el procedimiento de actualización no instalará la interfaz de línea de comandos de agente de recuperación. En este caso, debe volver a ejecutar el programa de instalación y seleccionar el componente que falta para instalarlo.
- Linux La versión de agente de recuperación en Linux debe ser la misma que la versión de agente de recuperación en el proxy Windows. Así, si actualiza agente de recuperación en Linux, también debe actualizar la versión de agente de recuperación en el proxy Windows.

Procedimiento

Para actualizar Data Protection for VMware, siga estos pasos:

1. Detenga los componentes y servicios de Data Protection for VMware que se están ejecutando.
2. Desmonte los volúmenes virtuales montados. Puede utilizar la GUI de agente de recuperación o la interfaz de línea de mandatos (mandato **`mount del`**) para desmontar volúmenes.
3. Si el sistema que está actualizando tiene tanto Interfaz gráfica de usuario de Data Protection for VMware vSphere como el transportador de datos de IBM Spectrum Protect instalados, instale el V8.1.0 de transportador de datos. Siga las

instrucciones de “Instalación de los componentes de Data Protection for VMware en sistemas Windows” en la página 21.

Nota: Linux Si el transportador de datos V6.x está instalado, deberá desinstalarlo antes de instalar V8.1.0. Siga las instrucciones de Desinstalación del cliente de IBM Spectrum Protect Linux x86_64

4. Descargue el paquete de códigos.
5. Desde la carpeta donde guardó el paquete de códigos inicie el proceso de actualización:
   a. Windows Ejecute el archivo `spinstall.exe`.
   b. Linux Ejecute el archivo `install-Linux.bin`.

   Se mostrará el siguiente mensaje: `El Data Protection for VMware existente se va a actualizar.`

   Si confirma la actualización, el instalador actualiza los archivos. Sólo puede instalar una Interfaz gráfica de usuario de Data Protection for VMware vSphere en una máquina. Como resultado, no se permiten varias Interfaz gráfica de usuario de Data Protection for VMware vSphere en la misma máquina.

Actualización de Data Protection for VMware en un sistema Windows de 64 bits en modo silencioso

Puede actualizar de manera silenciosa Data Protection for VMware en un sistema operativo de 64 bits soportado.

Antes de empezar

Cuando Data Protection for VMware V6.x se ha instalado en una ubicación no predeterminada, el proceso de actualización silencioso instala las características de Data Protection for VMware V8.1.0 en el directorio de instalación predeterminado. No puede actualizar de forma silenciosa a una ubicación no predeterminada. Consulte los subtemas en la sección “Componentes instalables” en la página 1 para conocer los directorios de instalación predeterminados para cada característica.

Procedimiento

Para actualizar Data Protection for VMware, siga estos pasos:

1. Detenga los componentes de Data Protection for VMware que estén en ejecución.
2. Desmonte los volúmenes virtuales montados. Puede utilizar la GUI de agente de recuperación o la interfaz de línea de mandatos (mandato **mount del**) para desmontar volúmenes.
3. Desmonte los volúmenes virtuales montados. Puede utilizar la GUI de agente de recuperación o la interfaz de línea de mandatos (mandato **mount del**) para desmontar volúmenes.
4. Descargue el paquete de códigos.
5. En la carpeta para Data Protection for VMware, vaya a la carpeta X64.
6. En la ventana del indicador de mandatos, escriba el mandato siguiente:

   ```
   spinstall.exe /s /v"/qn REBOOT=ReallySuppress"
   ```

Actualización de Data Protection for VMware en un sistema Linux en modo silencioso

Puede actualizar Data Protection for VMware de forma silenciosa en un sistema operativo Linux soportado.

Acerca de esta tarea

Utilice los siguientes parámetros de Data Protection for VMware con la característica de instalación silenciosa:

Tabla 14. Parámetros de actualización de instalación silenciosa de Data Protection for VMware

Parámetro	Descripción	Valor predeterminado
VCENTER_HOSTNAME	El nombre de dominio completo o la dirección IP de vCenter Server.	Ninguna.
VCENTER_USERNAME	ID de usuario de vCenter. Este ID de usuario debe ser un administrador de VMware que tenga permiso para registrar extensiones y anular el registro de las mismas.	Ninguna.
VCENTER_PASSWORD	Contraseña de vCenter.	Ninguna.
DIRECT_START	Para acceder a la Interfaz gráfica de usuario de Data Protection for VMware vSphere en un navegador web, especifique **DIRECT_START=YES**. Se accede a la Interfaz gráfica de usuario de Data Protection for VMware vSphere a través de un marcador de URL en el servidor web de GUI. Si no desea acceder a la Interfaz gráfica de usuario de Data Protection for VMware vSphere en un navegador web, especifique **DIRECT_START=NO**.	YES **Importante:** Cuando la actualización se haya completado, el valor **DIRECT_START** no se podrá cambiar, excepto si se reinstala el producto.

Procedimiento

Para actualizar Data Protection for VMware, siga estos pasos:

1. Asegúrese de que no existan sesiones de copia de seguridad, restauración o montaje activas.
2. Asegúrese de que cualquier Interfaz gráfica de usuario de Data Protection for VMware vSphere o GUI de agente de recuperación existente esté cerrada.
3. Descargue el paquete de códigos.
4. En la carpeta de Data Protection for VMware, vaya a la carpeta de Linux.
5. En una ventana de indicador de mandatos, escriba el mandato `././install-Linux.bin -i silent -DLICENSE_ACCEPTED=true` con los parámetros preferidos.
   Por ejemplo:

```
././install-Linux.bin -i silent -LICENSE_ACCEPTED=true
-VCENTER_HOSTNAME=hostname -VCENTER_USERNAME=username
-VCENTER_PASSWORD=password
-DIRECT_START=yes -REGISTER_EXTENSION=yes
```

Desinstalación de Data Protection for VMware

El proceso para la desinstalación de Data Protection for VMware es el mismo que para una instalación nueva y para una versión de actualización.

Desinstalación de Data Protection for VMware en Windows

Desinstalar componentes de Data Protection for VMware y eliminar archivos y directorios de un sistema Windows.

Antes de empezar

Para garantizar una desinstalación correcta, utilice las siguientes directrices:

- Si otros hosts de la GUI web de Data Protection for VMware utilizan la Extensión de IBM Spectrum Protect, no anule el registro de la extensión del cliente web.
- Al desinstalar la Extensión de IBM Spectrum Protect de un entorno de VMware vSphere 5.5, solo se eliminarán las etiquetas y descripciones de los privilegios asociados. Los privilegios permanecerán instalados. Este problema es una limitación conocida de VMware. Para obtener más información, consulte el siguiente artículo de VMware Knowledge Base: http://kb.vmware.com/kb/2004601.
- El archivo de habilitación de Data Protection for VMware no se elimina tras desinstalar el producto.

Acerca de esta tarea

Los archivos de configuración y propiedad se encuentran en el directorio `C:\Archivos de programa (x86)\Common Files\Tivoli\TDPVMware\VMwarePlugin\config` después de que se haya completado la desinstalación.

Procedimiento

1. Detenga los componentes de Data Protection for VMware que estén en ejecución.
2. Desmonte los volúmenes virtuales montados. Puede utilizar la GUI de agente de recuperación o la interfaz de línea de mandatos (mandato **mount del**) para desmontar volúmenes.
3. Pulse **Inicio** > **Panel de control** > **Programas y características** > **Desinstalar un programa**.
   - Si ha instalado Data Protection for VMware con el instalador de Suite, seleccione `Data Protection for VMware suite` y pulse **Desinstalar**.
   - Si ha instalado el transportador de datos como parte de la instalación de VE, tendrá que eliminar de forma manual la entrada de programas y características de `IBM Spectrum Protect JVM`.

   Esta acción desinstala el programa de Windows Data Protection for VMware. También elimina los servicios que están asociados con el agente de recuperación, el servidor web y la interfaz de línea de mandatos de Data Protection for VMware. Sin embargo, esta acción no elimina los archivos de registro, el transportador de datos ni los servicios del proxy de montaje, ni otros elementos que se han creado al configurar o utilizar Data Protection for VMware. La salida de estos artefactos en el disco no es un problema si desea volver a instalar Data Protection for VMware en el futuro. Sin embargo, si desea eliminar de forma más completa Data Protection for VMware y los archivos y valores relacionados, vaya al paso 4.

4. Elimine los siguientes archivos y directorios de Data Protection for VMware del sistema de archivos. Abra un indicador de mandatos de administrador y complete los siguientes pasos:
   a. Vaya al directorio `C:\Archivos de programa\Tivoli\TSM\` . Por ejemplo:
      ```
      cd /d " C:\Archivos de programa\Tivoli\TSM\"
      ```
      Emita los mandatos siguientes:
      ```
      rd /s RecoveryAgent
      rd /s TDPVMware
      ```
   b. Vaya al directorio `C:\Archivos de programa (x86)\Common Files\Tivoli\` . Por ejemplo:
      ```
      cd /d "C:\Archivos de programa (x86)\Common Files\Tivoli\"
      ```
      Nota: El siguiente mandato elimina todos los archivos de configuración y propiedades que se han guardado después de la desinstalación.
      Emita el comando siguiente:
      ```
      rd /s TDPVMware
      ```
   c. Vaya al directorio `C:\ProgramData`. Por ejemplo:
      ```
      cd /d "C:\ProgramData"
      ```
      Emita los mandatos siguientes:
      ```
      del installed.txt
      del TDPVMwareInstallation.log
      ```
   d. Vaya al directorio `C:\Datos de programa\Tivoli\TSM`. Por ejemplo:
      ```
      cd /d "C:\Datos de programa\Tivoli\TSM"
      ```
      Elimine los archivos siguientes si están en su sistema:
      ```
      del vmFileLevelRestoreDataSet.xml
      del vmFileLevelRestoreDataSet.xml.bak
      del vmFileLevelRestoreDataSet.xml.lock
      ```
      Emita el comando siguiente:
      ```
      rd /s RecoveryAgent
      ```
5. Detenga los componentes del transportador de datos que estén en ejecución.
6. Suprima las copias de seguridad de máquina virtual existentes emitiendo el mandato **`delete backup`** del transportador de datos. Por ejemplo, para suprimir la copia de seguridad activa de una máquina virtual denominada vm1, emita el siguiente mandato:
   ```
   delete backup -objtype=vm vm1
   ```
   Para suprimir una o varias versiones de copia de seguridad de una máquina virtual que se denomina vm_test., emita el siguiente mandato:
   ```
   delete backup -objtype=vm -inactive vm_test
   ```
7. Entre los mandatos siguientes. Puede utilizar el mandato **`dsmcutil list`** para visualizar los servicios del transportador de datos que están instalados.
   a. `cd /d "c:\Archivos de programa\tivoli\tsm\baclient"`
      Si es necesario, sustituya `c:\Archivos de programa\tivoli` por la carpeta de instalación correcta.
   b. `dsmcutil remove /name:"TSM Remote Client Agent"`

Importante: Asegúrese de eliminar `TSM Remote Client Agent` en el Paso 3b antes de eliminar `TSM Client Acceptor` en el Paso 3c. De lo contrario, `TSM Client Acceptor` (Paso 3c) no se puede eliminar.

c. `dsmcutil remove /name:"TSM Client Acceptor"`

Qué hacer a continuación

Compruebe que se hayan eliminado todos los componentes del sistema.

Desinstalación de Data Protection for VMware for Windows en modalidad silenciosa

Puede desinstalar de forma silenciosa Data Protection for VMware en un sistema operativo Windows.

Acerca de esta tarea

Los archivos de configuración y propiedad se encuentran en el directorio `C:\Archivos de programa (x86)\Common Files\Tivoli\TDPVMware\VMwarePlugin\config` después de que se haya completado la desinstalación.

Procedimiento

Para desinstalar Data Protection for VMware, complete los pasos siguientes:

1. Detenga los componentes de Data Protection for VMware que estén en ejecución.
2. Desmonte los volúmenes virtuales montados. Puede utilizar la GUI de agente de recuperación o la interfaz de línea de mandatos (mandato **`mount del`**) para desmontar volúmenes.
3. En una ventana de indicador de mandatos, utilice el mandato **`cd`** para cambiar a una de las carpetas siguientes:
   - Para personalizar la operación de desinstalación, vaya a la carpeta `X64`.
   - Para desinstalar Data Protection for VMware con el Instalador de suite, vaya a la `<carpeta extracción>TSM4VE_WIN`.
4. En la ventana de indicador de mandatos, ejecute el mandato siguiente:
   - Para una operación de desinstalación personalizada, seleccione en los siguientes mandatos:
     – Entre este mandato para desinstalar Data Protection for VMware y anular el registro de la Interfaz gráfica de usuario de Data Protection for VMware vSphere:

     ```
     spinstall.exe /s /v"/qn REBOOT=ReallySuppress REMOVE=ALL
     VCENTER_HOSTNAME=<vCenter hostname or IP>
     VCENTER_USERNAME=<vCenter user name>
     VCENTER_PASSWORD=<vCenter password>"
     ```

   - Para desinstalar todas las características con el instalador de Suite, entre el siguiente mandato:

     ```
     spinstall.exe /silent /remove
     ```

5. Reinicie el sistema después de que se haya completado la desinstalación.

Desinstalación de Data Protection for VMware en un sistema Linux

Puede desinstalar Data Protection for VMware en un sistema operativo Linux soportado.

Acerca de esta tarea

Cuando desinstala Data Protection for VMware en un sistema Linux, de forma predeterminada, el tipo de desinstalación es el mismo proceso que el tipo de instalación original. Para utilizar otro proceso de desinstalación, especifique el parámetro correcto. Por ejemplo, si utilizó un proceso de instalación silenciosa, puede utilizar el asistente de instalación en la desinstalación especificando el parámetro `–i swing`. Ejecute el proceso de desinstalación como usuario root. El perfil de usuario root debe ser importado. Si utiliza el mandato `su` para cambiar a root, utilice el mandato `su` para importar el perfil root.

Cuando el proceso de desinstalación empieza a eliminar los archivos de programa, si cancela el proceso de desinstalación, el sistema no puede volver a un estado limpio. Esta situación puede hacer que falle el intento de reinstalación. Como resultado, limpie el sistema completando las tareas que se describen en "Eliminación manual de Data Protection for VMware de un sistema Linux" en la página 40.

Para desinstalar Data Protection for VMware, complete los pasos siguientes:

Procedimiento

1. Cambie al directorio del programa de desinstalación. La siguiente vía de acceso es la ubicación predeterminada para el programa de desinstalación: `/opt/tivoli/tsm/tdpvmware/_uninst/TDPVMware/`
2. En función del tipo de instalación, utilice uno de los métodos siguientes para desinstalar Data Protection for VMware:

   Nota: Los mandatos de este procedimiento deben especificarse en una línea. Estos ejemplos muestran dos líneas para adaptarse al formato de la página.

   - Para utilizar el asistente de instalación para desinstalar Data Protection for VMware, entre este mandato:

     ```
     ./Uninstall_Tivoli_Data_Protection_for_VMware –i swing
     ```

   - Para utilizar la consola para desinstalar Data Protection for VMware, entre este mandato:

     ```
     ./Uninstall_Tivoli_Data_Protection_for_VMware -i console
     ```

   - Para desinstalar de forma silenciosa Data Protection for VMware, escriba este mandato:

     ```
     ./Uninstall_Tivoli_Data_Protection_for_VMware -i silent
     -f uninstall.properties
     ```

     El archivo `uninstall.properties` contiene la información de conexión de vCenter. Esta información es necesaria para desinstalar el Interfaz gráfica de usuario de Data Protection for VMware vSphere.

Eliminación manual de Data Protection for VMware de un sistema Linux

Acerca de esta tarea

Cuando Data Protection for VMware no puede instalarse utilizando el procedimiento de instalación estándar, debe eliminar manualmente Data Protection for VMware del sistema, tal como se describe en estos pasos. Ejecute este proceso como el usuario root.

Procedimiento

1. Si ya instalado el Interfaz gráfica de usuario de Data Protection for VMware vSphere, elimine su paquete de la base de datos de Package Manager con este mandato:

   ```
   rpm -e TIVsm-TDPVMwarePlugin
   ```

2. Elimine la API de IBM Spectrum Protect con este comando:

   ```
   rpm -e TIVsm-API64
   gskssl64.linux.x86_64.rpm
   skcrypt64.linux.x86_64
   TIVsm-TDPVMwarePlugin.x86_64.rpm
   TIVsm-DPAPI.x86_64.rpm
   ```

3. Elimine las entradas del producto del motor de despliegue:
   a. Emita este mandato para ver una lista de todas las entradas:

      ```
      /usr/ibm/common/acsi/bin/de_lsrootiu.sh
      ```

   b. Emita este mandato para eliminar las entradas de unidad instaladas que están relacionadas con Data Protection for VMware:

      ```
      /usr/ibm/common/acsi/bin/deleteRootIU.sh <UUID> <discriminant>
      ```

      Asegúrese de que estas entradas de unidad se eliminan:

      ```
      FBJRE
      TDPVMwareGUI
      JavaHelp
      TDPVMwareDM
      ```

4. Realice una copia de seguridad del archivo de registro global (`/var/.com.zerog.registry.xml`). Una vez realizada la copia de seguridad del archivo, elimine todas las etiquetas relacionadas con Data Protection for VMware.
5. Elimine todos los archivos en el directorio de instalación (`/opt/tivoli/tsm/tdpvmware`). Elimine también los atajos del escritorio.
6. Realice una copia de seguridad de los archivos de registro que haya en el directorio `/root` que contengan `TDPVMware` en el nombre de archivo. Por ejemplo, `IA-TDPVMware-00.log` o `IA-TDPVMware_Uninstall-00.log`. Elimine estos archivos de registro una vez realizada la copia de seguridad. Al eliminarlos, podrá ver si se emite algún error si el proceso de instalación vuelve a fallar.
7. Intente instalar de nuevo el producto tal como se describe en “Instalación de Data Protection for VMware en sistemas Linux” en la página 22.

Capítulo 2. Configuración de Data Protection for VMware

Esta sección proporciona instrucciones para configurar Data Protection for VMware e iniciar los servicios relacionados.

Configuración de una nueva instalación con el asistente

Utilice el asistente de configuración para obtener la configuración inicial o realizar cambios menores.

Antes de empezar

El sistema donde se ha instalado Data Protection for VMware debe tener conectividad de red con los siguientes servidores:

- Servidor de seguridad vStorage
- Servidor de IBM Spectrum Protect
- Servidor vCenter

Acerca de esta tarea

Para configurar el entorno de Data Protection for VMware, siga estos pasos:

Procedimiento

1. Abra un navegador web y especifique la dirección del servidor web de la GUI. Por ejemplo:

   ```
   https://guihost.mycompany.com:9081/TsmVMwareUI/
   ```

   - En un entorno de vSphere, inicie una sesión con el nombre de usuario y la contraseña de vCenter.
2. En la ventana Cómo empezar, vaya a la ventana Configuración y pulse **Ejecutar asistente de configuración**.
3. Siga las instrucciones indicadas en cada página del asistente hasta llegar a la ventana Resumen. Revise los valores y pulse **Finalizar** para completar la configuración y salir del asistente.

   Consejo: Se proporciona información sobre cada página de configuración en la ayuda online que se instala con la GUI. Pulse en **Learn More** (Más información) en cualquiera de la ventanas de la interfaz gráfica de usuario para abrir la ayuda online y obtener asistencia. Consulte el tema *Running the configuration wizard* (Ejecutar el asistente de configuración).
4. Compruebe si los nodos transportadores de datos se han configurado correctamente:
   a. Pulse en la pestaña **Configuration** para ver la página de Configuration Status.
   b. En la página Estado de configuración, seleccione un nodo transportador de datos para ver la información sobre su estado en el panel Detalles de estado. Si un nodo muestra un aviso o un error, pulse en ese nodo y utilice la información del panel Detalles del estado para resolver el problema. Luego seleccione el nodo y pulse en **Validar nodo seleccionado** para verificar si se ha resuelto el problema. Pulse en **Refresh** para restaurar todos los nodos.

Resultados

Vía de acceso rápida: Tras completar correctamente esta tarea del asistente, no se requieren más tareas de configuración adicionales para realizar copias de seguridad de los datos de sus máquinas virtuales.

Utilizando el cuaderno para editar una instalación existente

Utilice el cuaderno Editar configuración para editar los valores de la configuración existente.

Antes de empezar

El cuaderno Editar configuración proporciona las siguientes tareas para una configuración existente:

- Definir o cambiar el ID de administrador de IBM Spectrum Protect.
- Restablecer la contraseña y desbloquear el nodo de VMCLI.
- (Entorno de vSphere) Añadir o eliminar centros de datos de VMware en el dominio de Interfaz gráfica de usuario de Data Protection for VMware vSphere.
- Añadir o eliminar nodos proxy de montaje. Modifique una contraseña para un nodo proxy de montaje existente.
- Añadir o eliminar nodos del transportador de datos. Modificar una contraseña para un nodo transportador de datos existente.
- Habilitar restauración de archivo.
- Habilitar soporte de descodificación para un nodo de transportador de datos.

Acerca de esta tarea

Para editar una configuración existente, complete estos pasos:

Procedimiento

1. Abra un navegador web y especifique la dirección de servidor web de la GUI. Por ejemplo:

   ```
   https://guihost.mycompany.com:9081/TsmVMwareUI/
   ```

   - En un entorno de vSphere, inicie la sesión con el nombre de usuario y la contraseña de vCenter.
2. En la ventana Cómo empezar, vaya a la ventana Configuración y pulse **Editar configuración**.
3. Vaya a la página que corresponda para la tarea de edición y siga las instrucciones. Debe pulsar **Aceptar** para guardar los cambios antes de continuar en otra página de Valores de configuración. De lo contrario, los cambios no entrarán en vigor.

   Importante: Se proporciona información sobre cada página de configuración en la ayuda en línea que se instala con la GUI. Pulse en **Learn More** (Más información) en cualquiera de las ventanas de la interfaz gráfica de usuario a fin de abrir la ayuda en línea para obtener asistencia de tarea. Consulte el tema *Edición de una configuración existente*.

Resultados

Los valores actualizados se visualizan en la ventana Configuración.

Habilitación del entorno para operaciones de restauración de archivos

Windows

Cuando un administrador habilita la característica de restauración de archivos, los propietarios de archivos pueden restaurar los archivos sin asistencia.

Antes de empezar

Si no ha comprobado que se cumplen todos los requisitos, revise el tema en los requisitos previos de restauración de archivos en la *IBM Spectrum Protect for Virtual Environments: Data Protection for VMware - Guía de usuario*.

Acerca de esta tarea

Complete estos pasos en el sistema en el que está instalada la Interfaz gráfica de usuario de Data Protection for VMware vSphere .

Procedimiento

1. Inicie la Interfaz gráfica de usuario de Data Protection for VMware vSphere abriendo un navegador web y entrando la dirección de servidor web de la GUI. Por ejemplo:

   `https://<dirección del servidor web de la GUI>:9081/TsmVMwareUI/`

   **Inicie sesión con el ID de usuario y contraseña de vCenter.
2. Desde la ventana Cómo empezar, pulse **Configuración** y seleccione una de las siguientes tareas en la lista de tareas Tareas:
   - Si está configurando un nuevo entorno, complete los siguientes pasos:
     a. Seleccione **Ejecutar el asistente para la configuración del cliente**.
     b. Siga las instrucciones de cada página del asistente. Utilice la siguiente información para completar la página Restauración de archivo:
        1) Seleccione la opción **Habilitar restauración de archivo**.
        2) Entre la información de contacto de administrador que se muestra en la interfaz de restauración de archivos. Si no desea proporcionar información de contacto, quite la marca del recuadro de selección.
        3) Si el entorno contiene copias de seguridad de máquinas virtuales de Windows, introduzca las credenciales del administrador de dominios de Windows. De lo contrario, quite la marca del recuadro de selección y no especifique credenciales.

           Consejo: Una operación de restauración de archivo utiliza las credenciales del administrador de dominio para acceder al recurso compartido de red en la máquina virtual remota. Una operación falla cuando el entorno contiene copias de seguridad de máquinas virtuales de Windows y no tiene credenciales o se han especificado credenciales incorrectas. Por lo tanto, quite la marca de este recuadro de selección solo cuando no hay copias de seguridad de máquina virtual de Windows.
        4) Pulse en el URL de la interfaz de restauración de archivos para comprobar que la interfaz está accesible.

Recuerde: Mantenga registro del URL de interfaz de restauración de archivos. El propietario de la máquina virtual huésped accede a la interfaz de restauración de archivos a través de este URL.

5) Pulse **Aceptar** para guardar los cambios.

- Si está actualizando un entorno existente, complete los siguientes pasos:
  a. Seleccione **Editar configuración de TSM**.
  b. En la página Restauración de archivo, utilice las siguientes directrices:
     1) Seleccione la opción **Habilitar restauración de archivo**.
     2) Entre la información de contacto de administrador que se muestra en la interfaz de restauración de archivos. Si no desea proporcionar información de contacto, quite la marca del recuadro de selección.
     3) Si el entorno contiene copias de seguridad de máquinas virtuales de Windows, introduzca las credenciales del administrador de dominios de Windows. De lo contrario, quite la marca del recuadro de selección y no especifique credenciales.

        Consejo: Una operación de restauración de archivo utiliza las credenciales del administrador de dominio para acceder al recurso compartido de red en la máquina virtual remota. Una operación falla cuando el entorno contiene copias de seguridad de máquinas virtuales de Windows y no tiene credenciales o se han especificado credenciales incorrectas. Por lo tanto, quite la marca de este recuadro de selección solo cuando no hay copias de seguridad de máquina virtual de Windows.
     4) Pulse en el URL de la interfaz de restauración de archivos para comprobar que la interfaz está accesible.

        Recuerde: Mantenga registro del URL de interfaz de restauración de archivos. El propietario de la máquina virtual huésped accede a la interfaz de restauración de archivos a través de este URL.
     5) Pulse **Aceptar** para guardar los cambios.

Resultados

El entorno está habilitado para operaciones de restauración de archivos. Los propietarios de archivos pueden restaurar sus archivos utilizando el URL para acceder a la interfaz de restauración de archivos de IBM Spectrum Protect.

Configuración de operaciones de restauración de archivos en Linux

Linux

Para habilitar la característica de restauración de archivos cuando Data Protection for VMware esté instalado en un sistema Linux, se debe configurar un entorno de Data Protection for VMware adicional en un sistema Windows.

Acerca de esta tarea

Al ejecutar Data Protection for VMware en un entorno de Linux o junto con IBM Spectrum Protect Snapshot for VMware, la característica de restauración de archivos debe estar instalada en un sistema Windows para habilitar la característica de restauración de archivos.

Procedimiento

1. Configure un servidor Windows independiente que se utilice para la característica de restauración de archivos.
2. Instale Data Protection for VMware en el sistema Windows. Acepte los valores predeterminados durante la instalación.
3. Al configurar Data Protection for VMware en el sistema Windows, utilice los siguientes nombres de nodo:
   a. Cree un nodo vCenter con el nombre `VCENTER_FR`.
   b. Cree un nodo VMCLI con el nombre `VMCLI_FR`.
   c. Vuelva a utilizar el nombre de nodo de centro de datos desde el entorno de Linux.
      Por ejemplo: `DATACENTER`.
   d. No cree un nodo de transportador de datos. Un nodo de transportador de datos no es necesario para la característica de restauración de archivos en este escenario.
   e. Cree el siguiente nuevo par de nodos proxy de montaje con los nombres `REMOTE_FR_MP_WIN` y `REMOTE_FR_MP_LNX`.
4. En la página Restauración de archivos del asistente de configuración, seleccione la opción `Habilitar restauración de archivo`.
5. Para acceder a la interfaz de restauración de archivos, abra un navegador web y escriba el URL proporcionado por el administrador. Por ejemplo:

   ```
   https:\\nombre_host:9081\FileRestoreUI
   ```

   donde `nombre_host` es el nombre de host del sistema Windows donde está instalado Data Protection for VMware.

Resultados

El siguiente ejemplo muestra las relaciones de nodos proxy en el servidor de IBM Spectrum Protect:

```
tsm: SERVER>q proxy

Target Node       Agent Node
--------------     ------------------------------------------
VCENTER             VMCLI DATACENTER
VCENTER_FR          VMCLI_FR DATACENTER
DATACENTER          VMCLI VMCLI_FR
                     DATAMOVER1
                     REMOTE_MP_WIN REMOTE_MP_LNX
                     REMOTE_FR_MP_WIN REMOTE_FR_MP_LNX
```

Los nodos adicionales que se han creado para habilitar la característica de restauración de archivos tienen el sufijo `_FR`.

Modificación de opciones para las operaciones de restauración de archivos

Windows

Para permitir que los administradores configuren y controlen el proceso de restauración para operaciones de restauración de archivos, modifique las opciones en el archivo `frConfig.props`.

Acerca de esta tarea

Complete estos pasos en el sistema en el que está instalada la Interfaz gráfica de usuario de Data Protection for VMware vSphere .

Procedimiento

1. Vaya al directorio donde se encuentra el archivo `frConfig.props`. Por ejemplo, abra un indicador de mandatos y emita el siguiente mandato:

   ```
   cd C:\IBM\tivoli\tsm\tdpvmware\webserver\usr\servers\veProfile\tsmVmGUI
   ```

2. Abra el archivo `frConfig.props` con un editor de texto en modo administrador y modifique las opciones según sea necesario. Utilice la información en "Opciones de restauración de archivos" para determinar qué opciones se deben modificar.
3. Guarde los cambios y cierre el archivo `frConfig.props`.

Resultados

Las opciones modificadas se aplican a la interfaz de restauración de archivos de IBM Spectrum Protect.

Opciones de restauración de archivos

Las opciones de `frConfig.props` controlan el proceso de configuración, soporte y restauración para las operaciones de restauración de archivos.

enable_contact_info=false | true
Especifique si se debe proporcionar la información de contacto de administrador que los propietarios de archivos pueden utilizar para obtener soporte.

false
Los propietarios de archivo no reciben información de contacto de administrador. Este es el valor predeterminado.

true
Los propietarios de archivo reciben información de contacto de administrador.

Si se especifica **enable_contact_info=true**, se debe proporcionar información en la opción **contact_info** .

enable_filerestore=false | true
Especifique si los propietarios de archivos pueden restaurar los archivos de una máquina virtual con la interfaz de restauración de archivos de IBM Spectrum Protect.

false
Los propietarios de archivo no pueden restaurar sus archivos con la interfaz de restauración de archivos de IBM Spectrum Protect. Este es el valor predeterminado.

true
Los propietarios de archivos pueden restaurar sus archivos con la interfaz de restauración de archivos de IBM Spectrum Protect.

maximum_mount_points=*núm_puntos_montaje*
Especifique el número máximo de puntos de recuperación simultáneos que están disponibles para la cuenta de usuario. El valor mínimo es 1 punto de

recuperación. El valor máximo es de 256 puntos de montaje. El valor predeterminado es 2 puntos de montaje.

Consejo: Para impedir que una máquina virtual se monte varias veces para operaciones de restauración simultáneas, establezca esta opción con un valor bajo.

mount_session_timeout_minutes=*núm_mins*
Especifique la cantidad de tiempo, en minutos, que una restauración y el punto de recuperación montado pueden estar desocupados antes de que se cancele la sesión. Una cancelación desmonta el punto de recuperación. El valor máximo es de 8 horas (480 minutos). El valor predeterminado es de 30 minutos.

Consejo: Para evitar que la sesión se cancele de forma inesperada, aumente el número de minutos.

restore_info_duration_hours=*núm_hrs*
Especifique la cantidad de tiempo, en horas, durante el cual la información sobre la actividad de restauración reciente se retiene en la interfaz de restauración de archivos de IBM Spectrum Protect. Utilice la ventana de actividad de restauración para ver la información de error y las tareas completadas recientemente. Esta información proporciona una forma para localizar archivos restaurados recientemente. El valor máximo es de 14 días (336 horas). El valor predeterminado es de una semana (168 horas).

contact_info=*información de administrador*
Proporcione la información de contacto de administrador que los propietarios de archivos pueden utilizar para obtener soporte. La información de contacto se visualiza en la interfaz de restauración de archivos de IBM Spectrum Protect en las siguientes ubicaciones:

- Ventana de inicio de sesión
- Panel Acerca de en el menú de ayuda
- Enlace de información de soporte en los mensajes de interfaz

Puede sobrescribir las siguientes opciones con el cuaderno o el asistente de configuración de Interfaz gráfica de usuario de Data Protection for VMware vSphere:

- **enable_contact_info**
- **enable_filerestore**
- **contact_info**

Configuración de la actividad de registro para operaciones de restauración de archivos

Para permitir que los administradores configuren y controlen cómo se formatea y registra el contenido para las operaciones de restauración de archivos, modifique las opciones en el archivo `FRLog.config`.

Antes de empezar

El archivo `FRLog.config` se genera la primera vez que se accede a la interfaz de restauración de archivos de IBM Spectrum Protect.

Acerca de esta tarea

Complete estos pasos en el sistema en el que está instalada la Interfaz gráfica de usuario de Data Protection for VMware vSphere .

Procedimiento

1. Vaya al directorio donde se encuentra el archivo `FRLog.config`. Abra un indicador de mandatos y emita el mandato siguiente:

   ```
   cd directorio_instalación\IBM\tivoli\tsm\tdpvmware\webserver\usr\servers\veProfile\frGUI\
   ```

2. Abra el archivo `FRLog.config` con un editor de texto en modo administrador y modifique las opciones según sea necesario. Utilice la información en "Opciones de actividad del registro de restauración de archivos" para determinar qué opciones se deben modificar.
3. Guarde los cambios y cierre el archivo `FRLog.config`.
4. Reinicie el servidor web de la GUI:
   a. Pulse **Inicio** > **Panel de control** > **Herramientas administrativas** > **Servicios**.
   b. Pulse con el botón derecho en **Data Protection for VMware Web Server Service** y pulse en **Restart**.

Resultados

Los valores se aplican al contenido y formato de la información de registro para las operaciones de restauración de archivos.

Opciones de actividad del registro de restauración de archivos

Las opciones `FRLog.config` controlan el contenido y formato de la información de registro para las operaciones de restauración de archivos.

Las siguientes opciones registran información para las tareas de restauración de archivos en el archivo `fr_gui.log`:

MAX_LOG_FILES=*número*
Especifica el número máximo de archivos `fr_gui.log` que se van a retener. El valor predeterminado es 8.

MAX_LOG_FILE_SIZE=*número*
Especifica el tamaño máximo del archivo `fr_gui.log` en KB. El valor predeterminado es 8192 KB.

Las siguientes opciones registran información para los servicios de restauración de archivos en el archivo `fr_api.log`. Estos servicios son servicios de API internos relacionados con la actividad de restauración de archivos:

API_MAX_LOG_FILES=*número*
Especifica el número máximo de archivos `fr_api.log` que se van a retener. El valor predeterminado es 8.

API_MAX_LOG_FILE_SIZE=*número*
Especifica el tamaño máximo del archivo `fr_api.log` en KB. El valor predeterminado es 8192 KB.

API_LOG_FILE_NAME=*API_log_file_name*
Especifica el nombre del archivo de registro de la API. El valor predeterminado es `fr_api.log`.

API_LOG_FILE_LOCATION=*API_log_file_name*
Especifica la ubicación del archivo de registro de la API. La ubicación debe especificarse utilizando una barra inclinada (/). La ubicación predeterminada es `directorio_instalación/IBM/tivoli/tsm/tdpvmware/webserver/usr/servers/veProfile/logs`.

FR.API.LOG=ON | OFF
Especifica si se habilita el registro para los servicios de restauración de archivos.

- Para habilitar el registro para los servicios de restauración de archivos, especifique ON. El valor predeterminado es ON.
- Para inhabilitar el registro para los servicios de restauración de archivos, especifique OFF.

Para resolver los problemas que se puede encontrar durante las operaciones de restauración de archivos, consulte Opciones de rastreo para la restauración de archivos. Las opciones de rastreo también se especifican en el archivo `FRLog.config`.

Configuración de un nodo de transportador de datos para soporte de descodificación

Cuando el soporte de descodificación está habilitado en un nodo de transportador de datos, los administradores pueden aplicar etiquetas de protección de datos a objetos de inventario del VMware vCenter.

Antes de empezar

Asegúrese de que se cumplan los siguientes requisitos:

- VMware vCenter Server debe tener la versión 6.0 Actualización 1 o posterior.
- Para que funcione Interfaz gráfica de usuario de Data Protection para VMware vSphere correctamente con soporte de etiquetado, asegúrese de que se cumplen los siguientes requisitos durante la instalación GUI:
  - Deben instalarse un transportador de datos y Interfaz gráfica de usuario de Data Protection para VMware vSphere en el mismo servidor. El nodo de transportador de datos debe estar configurado de forma que se guarden las credenciales de vCenter. Puede guardar las credenciales ejecutando el asistente para guardar la contraseña del nodo de transportador de datos o utilizando el mandato **dsmc set password** en la línea de mandatos del transportador de datos.

    Si utiliza otros transportadores de datos que se ejecutan en máquinas virtuales o físicas como transportadores adicionales, puede instalarlos en otros servidores. Para soporte de etiquetado, todos estos transportadores de datos deben estar configurados con la opción `vmtagdatamover=yes`. Estos transportadores de datos adicionales no necesitan que se instale Interfaz gráfica de usuario de Data Protection para VMware vSphere to be installed on the same server para que funcionen correctamente como transportadores de datos basados en etiquetas.
  - Linux Para los transportadores de datos de Linux, asegúrese de especificar el directorio de instalación del transportador de datos y la biblioteca compartida de Java™ `libjvm.so` en la variable de entorno `LD_LIBRARY_PATH`. La vía de acceso a `libjvm.so` se utiliza para el soporte de descodificación al habilitar la opción `vmtagdatamover` en el transportador de

datos. Para obtener instrucciones, consulte Configuración de los nodos transportadores de datos en un entorno de vSphere.

– Linux En sistemas operativos Linux, la Interfaz gráfica de usuario de Data Protection para VMware vSphere debe instalarse utilizando el nombre de usuario predeterminado (`tdpvmware`).

– Linux Para los nodos de transportador de datos Linux, debe utilizarse el archivo de contraseña predeterminado (`/etc/adsm/TSM.PWD`).

Acerca de esta tarea

Puede utilizar etiquetas de protección de datos para configurar la política de copia de seguridad de las máquinas virtuales en los objetos de inventario de VMware. Estas etiquetas de protección de datos se presentan como valores que se pueden modificar en la Extensión de IBM Spectrum Protect. Para las etiquetas relacionadas con planificaciones, las máquinas virtuales deben estar en un conjunto de protección protegido por una planificación. Un conjunto de protección consta de las máquinas virtuales de un contenedor a las que se les asigna la etiqueta `Schedule (IBM Spectrum Protect)`.

Procedimiento

Utilice uno de los siguientes métodos:

- Para configurar un *nuevo* transportador de datos para el soporte de etiquetado en Windows utilizando la Interfaz gráfica de usuario de Data Protection para VMware vSphere, siga estos pasos:
  1. En el sistema Windows donde está instalada la Interfaz gráfica de usuario de Data Protection para VMware vSphere, inicie la GUI abriendo un navegador web y escribiendo la dirección del servidor web de la GUI. Por ejemplo:
     `https://<dirección servidor web GUI>:9081/TsmVMwareUI/`

     **Inicie sesión con el ID de usuario y contraseña de vCenter.
  2. Vaya al separador **Configuración** y seleccione la acción **Editar configuración de IBM Spectrum Protect**.
  3. Vaya a la página Nodos del transportador de datos del cuaderno de configuración.
  4. Añada un nodo de transportador de datos al completar los pasos siguientes:
     a. Para el nodo de transportador de datos para el que desee configurar el soporte de etiquetado, seleccione **Crear servicios** y, a continuación, seleccione **Nodo basado en etiquetas**.
     b. Para designar el nodo basado en etiquetas como nodo de transportador de datos predeterminado, seleccione **Transportador de datos predeterminado**. Un nodo de transportador de datos predeterminado realiza copia de seguridad de cualquier nueva MV que se añada a cualquier contenedor del centro de datos, si el contenedor ya se encuentra en un conjunto de protección. El transportador de datos predeterminado también hace copia de seguridad de cualquier MV del conjunto de protección que no esté asignado a la etiqueta `Transportador de datos`.

        Consejo: Si edita la configuración, añada un nuevo nodo de transportador de datos, y selecciona este nuevo transportador de datos para que sea el predeterminado para el centro de datos, y la opción `vmtagdefaultdatamover` se establece en el resto de los archivos de opciones del transportador de datos, debe editar manualmente los

archivos de opciones del transportador de datos para el resto de los transportadores de datos del centro de datos para cambiar el valor `vmtagdefaultdatamover` al transportador de datos recién creado.

c. Pulse **Aceptar** para guardar los cambios.

Las opciones `vmtagdefaultdatamover` y `vmtagdefaultdatamover` (si están establecidas) se añaden al archivo de opciones del transportador de datos (`dsm.opt`).

- Para configurar un nodo de transportador de datos *nuevo* o *existente* de Linux, o un nodo de transportador de datos *existente* de Windows, para el soporte de descodificación:
  1. Añada la opción `vmtagdatamover yes` del archivo de opciones del transportador de datos (`dsm.sys` para Linux y `dsm.opt` para Windows).
  2. Para designar el nodo basado en etiquetas como el nodo de transportador de datos predeterminado, añada la opción `vmtagdefaultdatamover yes` o `vmtagdefaultdatamover` *dm_name* al archivo de opciones del transportador de datos.

     Consejo: Si edita la configuración, añada un nuevo nodo de transportador de datos, y selecciona este nuevo transportador de datos para que sea el predeterminado para el centro de datos, y la opción `vmtagdefaultdatamover` se establece en el resto de los archivos de opciones del transportador de datos, debe editar manualmente los archivos de opciones del transportador de datos para el resto de los transportadores de datos del centro de datos para cambiar el valor `vmtagdefaultdatamover` al transportador de datos recién creado.

Resultados

Una vez que se habilite el nodo de transportador de datos para el soporte de etiquetado, el transportador de datos consultará al inventario de VMware la información de etiquetado cuando ejecute una copia de seguridad. A continuación, el transportador de datos realizará una copia de seguridad de las máquinas virtuales según las etiquetas de protección de datos que se configuren. Si el nodo de transportador de datos no está configurado para el soporte de etiquetado, se omitirá cualquier etiqueta de protección de datos durante una operación de copia de seguridad.

Información relacionada:

- `Vmtagdatamover`
- `Vmtagdefaultdatamover`
- Configuración de políticas de copia de seguridad

Configuración del entorno para las operaciones de restauración instantánea de máquinas virtuales completas

Configure una red iSCSI para operaciones de restauración instantánea de máquina virtual completa y de acceso instantáneo.

Antes de empezar

Utilice la documentación de VMware adecuada (ESXi o vSphere) para determinar los pasos específicos que ha de seguir para configurar el conmutador virtual iSCSI y la red de la máquina virtual. Aunque se proporcionan directrices generales, la

documentación y las explicaciones específicas acerca de cómo añadir redes virtuales y conmutadores virtuales está fuera del ámbito de la documentación del producto. En el momento de la publicación, la documentación de VMware vSphere ESXi y vCenter 5.5 se encuentra disponible en Documentación de VMware ESXi y vCenter Server 5. Los temas de "Red" contienen información sobre cómo añadir y configurar conmutadores virtuales y redes virtuales.

Importante: Estos ajustes de configuración se proporcionan para ayudarle a configurar el entorno de VMware para realizar de forma eficaz las operaciones de restauración instantánea de máquina virtual completa y de acceso instantáneo. Sin embargo, dado que estos ajustes se aplican a las tareas de configuración de VMware y las interfaces de usuario de VMware, debe hacer referencia a la documentación de VMware apropiada para obtener las instrucciones detalladas paso a paso.

Acerca de esta tarea

Este procedimiento requiere un adaptador iSCSI en cada host ESXi que se utilice para las operaciones de restauración instantánea. Utilice la documentación de VMware adecuada para configurar el adaptador. En el momento de la publicación, los procedimientos siguientes se encuentran disponibles en la Documentación de VMware ESXi y vCenter Server 5.

- Para configurar un adaptador iSCSI de software, siga las instrucciones del procedimiento "Configurar adaptadores iSCSI de software" de VMware.
- Para configurar un adaptador iSCSI de hardware, siga las instrucciones del procedimiento "Configuración de adaptadores iSCSI de hardware independientes" de VMware.

1. Configuración del software de iSCSI en el host de ESXi

Procedimiento

Esta tarea configura el software de iSCSI para una configuración básica.

1. Inicie sesión en el host de ESXi que se utilizará para las operaciones de restauración instantánea.
2. Siga las instrucciones de este artículo de VMware Knowledge Base hasta que se haya habilitado el adaptador iSCSI: http://kb.vmware.com/kb/1008083
   IBM Spectrum Protect descubre automáticamente el servidor de destino iSCSI.
3. Verifique que la dirección IP del adaptador iSCSI (en el host de ESXi) sea la misma dirección de subred que utiliza el transportador de datos.
4. Verifique la licencia de Storage vMotion esté habilitada en el host de ESXi.

Qué hacer a continuación

Una vez configurado el software de iSCSI en el host de ESXi, instale y configure las aplicaciones en el sistema del transportador de datos.

2. Instalación y configuración de aplicaciones en transportador de datos

Antes de empezar

Si el Recovery Agent V8.1.0 y el transportador de datos de IBM Spectrum Protect V8.1.0 están instalados y configurados en el sistema transportador de datos, comience en el paso 3.

Procedimiento

Esta tarea configura el sistema del transportador de datos con las aplicaciones y valores para las operaciones de restauración instantánea.

1. Instale el Recovery Agent V8.1.0 y el transportador de datos de IBM Spectrum Protect V8.1.0 en el sistema transportador de datos.
   En el Paso 4 del procedimiento Instalación de Data Protection for VMware, seleccione el tipo de instalación **Instalar un transportador de datos completo para la protección de aplicaciones en el invitado**.
2. Configure el transportador de datos.
   Siga las instrucciones de Configuración del transportador de datos.
3. Establezca la dirección IP del servidor iSCSI:
   a. Vaya al archivo `C:\Archivos de programa\Tivoli\TSM\baclient\dsm.opt` y especifique el parámetro siguiente:

      ```
      VMISCSIServeraddress=<dirección IP de la tarjeta de red en el sistema del
      transportador de datos
      que expone los destinos de iSCSI.>
      ```

      Si su sistema transportador de datos tiene más de una tarjeta de red, asegúrese de que especifica la tarjeta de red correcta para la red iSCSI.

Qué hacer a continuación

Una vez configurado el sistema del transportador de datos, establezca una conexión entre la CLI del agente de configuración y la GUI del agente de configuración.

3. Configuración de la conexión del agente de recuperación

Antes de empezar

La interfaz de línea de mandatos (CLI) del agente de recuperación V7.1.x se puede visualizar como una API de línea de mandatos en la GUI del agente de recuperación. Puede utilizar la CLI del agente de recuperación para comunicarse con la GUI del agente de recuperación.

Procedimiento

Esta tarea establece una conexión entre la CLI del agente de recuperación y la GUI del agente de recuperación.

1. Inicie la CLI del agente de recuperación en el sistema del transportador de datos.
   En el menú **Inicio** de Windows, pulse **Programas** > **IBM Spectrum Protect** > **IBM Spectrum Protect for Virtual Environments** > **IBM Spectrum Protect Recovery Agent**.
2. En la ventana del indicador de mandatos, escriba el mandato siguiente:

```
RecoveryAgentShell.exe -c set_connection mount_computer < dirección IP
de la tarjeta de red del sistema del transportador de datos que expone los
destinos de iSCSI.>
```

Este mandato establece una conexión entre la CLI del agente de recuperación y la GUI del agente de recuperación.

Qué hacer a continuación

Una vez establecida una conexión, configure una red iSCSI dedicada.

4. Configuración de una red iSCSI dedicada para el host de ESXi y el transportador de datos

Antes de empezar

Revise estas directrices antes de continuar con esta tarea:

- Utilice una red iSCSI dedicada para las operaciones de restauración instantánea.
- Cada host de ESXi que se utilice para las operaciones de restauración instantánea debe tener una segunda tarjeta de red física disponible. Esta segunda tarjeta de red está enlazada al adaptador iSCSI de software del host de ESXi respectivo.
- El sistema del transportador de datos que se ejecuta en una máquina virtual debe tener disponible una segunda tarjeta de red. Esta segunda tarjeta de red está enlazada al adaptador iSCSI de software de este host de ESXi.
- Cada host de ESXi que se utilice para las operaciones de restauración instantánea debe tener un almacén de datos VMware secundario disponible. Este almacén de datos temporal contiene la información de configuración y los datos de la máquina virtual que se crean durante la operación.

Procedimiento

Esta tarea configura una red iSCSI dedicada para el host de ESXi y para el transportador de datos que se ejecuta en una máquina virtual.

1. Inicie sesión en el host de ESXi que se utilizará para las operaciones de restauración instantánea.
2. Configure el conmutador virtual para la red iSCSI.
   Estos pasos utilizan *vSwitch1* para el conmutador virtual.
   a. Seleccione **Adaptador de red VMkernel** como **Tipo de conexión**.
      La red iSCSI requiere este tipo de conexión.
   b. Seleccione **Crear un conmutador vSphere estándar** para **VMkernel Network Access**.
   c. Seleccione **Etiqueta de red** en **VMkernel Connection Settings**.
      Especifique una etiqueta que indique que *vSwitch1* y esta red son para su tráfico iSCSI.
      Por ejemplo: *VMkernel iSCSI*.
   d. Especifique una dirección IP y una máscara de subred para *vSwitch1* en **VMkernel IP Connection Settings**.
      No cambie los valores de **Subnet Mask** o **VMkernel Default Gateway**.
   e. Especifique el puerto del kernel para que opere la red iSCSI.
3. Configure el conmutador virtual para la red de máquina virtual.
   Estos pasos utilizan *vSwitch0* para el conmutador virtual.
   a. Seleccione **Máquina virtual** como **Tipo de conexión**.

b. Seleccione **Crear un conmutador vSphere estándar** para **VMkernel Network Access**.

c. Vaya al separador **Propiedades del grupo de puertos** y seleccione **Etiqueta de red**.
Especifique la misma etiqueta que ha especificado para la red de máquina virtual *vSwitch1*.
Por ejemplo: *VMkernel iSCSI*.

4. Enlace el adaptador iSCSI que acaba de crear con **VMkernel Network Adapter**. Siga las instrucciones del procedimiento “Vincular adaptadores iSCSI con adaptadores VMkernel" de VMware. En el momento de la publicación, este procedimiento se encuentra disponible en Documentación de VMware ESXi y vCenter Server 5.

   Consejo: Si se produce un tiempo de espera excedido cuando se vuelven a escanear los dispositivos de iSCSI, reduzca el número de dispositivos iSCSI conectados al host de ESXi. A continuación, vuelva a escanear los dispositivos iSCSI.

5. Verifique que las propiedades de vinculación del adaptador iSCSI sean correctas.

   a. Vaya a **Hardware** > **Adaptadores de almacenamiento** en el cliente de VMware vSphere.

   b. Pulse con el botón derecho el adaptador iSCSI y seleccione **Propiedades del iniciador de iSCSI**. Asegúrese de que existan las siguientes propiedades de vinculación:

Tabla 15. Valores de red iSCSI

Red de máquinas virtuales	Red iSCSI
Standard Switch: *vSwitch0*	**Standard Switch**: *vSwitch1*
Virtual Machine Port Group: *VM Network*	**VMkernel Port**: *VMkernel iSCSI* **Consejo:** *VMkernel iSCSI* está vinculado con **VMkernel Adapter**: *vmk1*, el cual está en **Physical Network Adapter**: *vmnic1*.
Physical Adapter: *vmnic0*	**VMkernel Network Adapter**: *vmk1*
	Physical Network Adapter: *vmnic1*
	Virtual Network Adapter **IP address**: 192.168.42.x (subred para la red iSCSI)

Resultados

Una red iSCSI dedicada está preparada para las operaciones de restauración instantánea de máquina virtual y para las operaciones de acceso instantáneo.

Configuración de la comunicación con Seguridad de la capa de transporte

La Interfaz gráfica de usuario de Data Protection for VMware vSphere utiliza el protocolo Seguridad de la capa de transporte (TLS) para comunicarse con su cliente de la GUI web y el servidor de IBM Spectrum Protect.

Acerca de esta tarea

La Interfaz gráfica de usuario de Data Protection for VMware vSphere siempre utiliza el protocolo HTTPS para comunicarse con navegadores web. En otras palabras, TLS siempre está habilitado. Durante la instalación de Data Protection for VMware, se generará un certificado digital autofirmado y se utilizará para sesiones de navegador web.

Si desea utilizar un certificado firmado por un tercero (conocido como entidad emisora de certificados), siga los pasos descritos en "Uso de un certificado de tercero".

La comunicación de TLS con el servidor de IBM Spectrum Protect es opcional y no está habilitada de forma predeterminada. Para habilitarla, siga los pasos descritos en "Habilitación de comunicación segura con el servidor IBM Spectrum Protect" en la página 60.

Uso de un certificado de tercero

Para usar un certificado que esté firmado por un tercero (también conocido como entidad emisora de certificados), debe realizar varios pasos.

Acerca de esta tarea

Los siguientes procedimientos utilizan la herramienta de gestión de certificados y claves estándar denominada **keytool**.

En sistemas operativos Linux, se encuentra en el directorio `/opt/tivoli/tsm/tdpvmware/common/jre/jre/bin/`.

En sistemas operativos Microsoft Windows, se encuentra en el directorio `C:\IBM\tivoli\tsm\tdpvmware\webserver\jre\jre\bin`.

Puede que tenga que especificar la vía de acceso completa al ejecutar **keytool** desde la línea de mandatos.

Procedimiento

1. Obtenga acceso al almacén de claves.
2. Cree una solicitud de firma de certificado (CSR).
3. Envié la solicitud de firma de certificado a la entidad emisora de certificados para su firma.
4. Reciba el certificado firmado en Interfaz gráfica de usuario de Data Protection para VMware vSphere.

Obtención de acceso al almacén de claves

Los certificados se almacenan en un almacén de claves Java™. El contenido del almacén de claves está protegido con una contraseña. Para manipular los certificados del almacén de claves, debe obtener acceso al almacén de claves.

Acerca de esta tarea

El certificado firmado automáticamente predeterminado y la contraseña del almacén de claves se generan automáticamente durante la instalación, así que es poco probable que conozca la contraseña inicial.

Lleve a cabo el siguiente procedimiento para sustituir el almacén de claves original por un almacén de claves nuevo y un certificado firmado automáticamente nuevo. El almacén de claves nuevo se protege mediante una contraseña de su elección.

Si ya conoce la contraseña del almacén de claves, omita este procedimiento.

Procedimiento

1. Detenga el servicio de Interfaz gráfica de usuario de Data Protection para VMware vSphere.
2. En la línea de mandatos, cambie el directorio a la ubicación del almacén de claves.
   - En Linux: `/opt/tivoli/tsm/tdpvmware/common/webserver/usr/servers/veProfile/resources/security/`
   - En Windows: `C:\IBM\tivoli\tsm\tdpvmware\webserver\usr\servers\veProfile\resources\security\`
3. Realice una copia de seguridad del archivo del almacén de claves (`key.jks`) cambiándole el nombre o moviéndolo a una ubicación diferente.
4. Cree un nuevo almacén de claves y un nuevo certificado firmado automáticamente emitiendo el siguiente mandato:

   ```
   keytool -genkeypair -alias vekey -dname
   CN=fqdn,OU=Tivoli_Storage_Manager_for_VMware,O=IBM -keyalg RSA
   -sigalg SHA256withRSA -keysize 2048 -validity days -keystore
   key.jks -storepass password -keypass password
   ```

   Donde:

   -dname CN=*fqdn***,OU=Tivoli_Storage_Manager_for_VMware,O=IBM**
   : *fqdn* es el nombre de DNS o nombre de dominio totalmente calificado en el que se ha instalado Interfaz gráfica de usuario de Data Protection para VMware vSphere.

   -validity *days*
   : El período de validez del certificado.

   -storepass *password*
   : La contraseña del almacén de claves. Asegúrese de memorizar esta contraseña para su futuro uso.

   -keypass *password*
   : La contraseña de clave privada del certificado. Esta contraseña debe coincidir con la contraseña del almacén de claves.
5. Codifique la contraseña del almacén de claves usando la herramienta **securityUtility**. Emita el mandato siguiente:
   - En Linux: `/opt/tivoli/tsm/tdpvmware/common/webserver/bin/securityUtility encode`
   - En Windows: `C:\IBM\tivoli\tsm\tdpvmware\webserver\bin\securityUtility.bat encode`

   Escriba la contraseña del almacén de datos cuando se le solicite y, a continuación, guarde la salida (por ejemplo, cópiela en el portapapeles).
6. Abra el archivo `bootstrap.properties` en un editor y establezca la propiedad `veProfile.keystore.pswd` en el valor codificado en el paso anterior. El archivo `bootstrap.properties` se encuentra en la siguiente ubicación:
   - En Linux: `/opt/tivoli/tsm/tdpvmware/common/webserver/usr/servers/veProfile/`

- En Windows: `C:\IBM\tivoli\tsm\tdpvmware\webserver\usr\servers\veProfile\`

7. Inicie el servicio Interfaz gráfica de usuario de Data Protection para VMware vSphere.

Referencia relacionada:

"Inicio y ejecución de los servicios de Data Protection for VMware" en la página 81

Creación de una solicitud de firma de certificado

Después de obtener acceso al almacén de claves, debe crear una solicitud de firma de certificado (CSR).

Procedimiento

Lleve a cabo los siguientes pasos para crear una CSR:

1. En la línea de mandatos, cambie el directorio a la ubicación del almacén de claves.
   - En Linux: `/opt/tivoli/tsm/tdpvmware/common/webserver/usr/servers/veProfile/resources/security/`
   - En Windows: `C:\IBM\tivoli\tsm\tdpvmware\webserver\usr\servers\veProfile\resources\security\`
2. Cree un nuevo certificado emitiendo el siguiente mandato:

   ```
   keytool -genkeypair -alias mykey -dname
   CN=fqdn,OU=unit,O=organization -keyalg RSA -sigalg SHA256withRSA
   -keysize 2048 -validity days -keystore key.jks -storepass
   password -keypass password
   ```

   Donde:

   -alias *mykey*
   : *mykey* es el alias exclusivo que identifica el certificado en el almacén de claves. Se le cambia el nombre al recibirse el certificado firmado.

   -dname CN=*fqdn***,OU=***unit***,O=***organization*
   : *fqdn* es el nombre de DNS o nombre de dominio completo del equipo en el que está instalado Interfaz gráfica de usuario de Data Protection for VMware vSphere.

     Unit y *organization* son información acerca de la organización que necesitan sus políticas o la entidad emisora de certificados.

   -validity *days*
   : El período de validez del certificado.

   -storepass *password*
   : La contraseña del almacén de claves. Si no sabe o ha olvidado la contraseña del almacén de claves, consulte "Obtención de acceso al almacén de claves" en la página 56.

   -keypass *password*
   : La contraseña de clave privada del certificado. Esta contraseña debe coincidir con la contraseña del almacén de claves.

3. Cree una CSR emitiendo el siguiente mandato:

   ```
   keytool -certreq -alias mykey -file certreq.pem -keystore key.jks
   ```

   Donde:

-alias *mykey*
El alias de certificado del paso anterior.

-file *certreq.pem*
El archivo para almacenar la solicitud de firma de certificado.

Envío de la solicitud de firma de certificado a la entidad emisora de certificados

Después de crear la solicitud de certificado (`certreq.pem`), debe enviarla a la entidad emisora de certificados para su firma. Siga las instrucciones específicas de la entidad emisora de certificados.

Recepción del certificado firmado

Después de recibir el certificado firmado de la entidad emisora de certificados (CA), debe recibir el certificado en el almacén de claves.

Procedimiento

Para recibir el certificado firmado, lleve a cabo los siguientes pasos:

1. En la línea de mandatos, cambie el directorio a la ubicación del almacén de claves.
   - En Linux: `/opt/tivoli/tsm/tdpvmware/common/webserver/usr/servers/veProfile/resources/security/`
   - En Windows: `C:\IBM\tivoli\tsm\tdpvmware\webserver\usr\servers\veProfile\resources\security\`
2. Copie los archivos que ha recibido de la CA en esta ubicación. Estos archivos incluyen el certificado raíz de CA, los certificados CA intermedios (si los hubiera) y el certificado firmado para Interfaz gráfica de usuario de Data Protection para VMware vSphere.
3. Detenga el servicio de Interfaz gráfica de usuario de Data Protection para VMware vSphere.
4. Realice copia de seguridad del archivo de almacén de claves (`key.jks`) copiándolo en una ubicación o con un nombre diferente.
5. Importe los certificados CA intermedios, si los hubiera, con el siguiente mandato. Si se le solicita confiar en los certificados, responda *sí*. Repita este paso para todos los CA intermediarios que sean necesarios.

   ```
   keytool -importcert -alias ca-intermediate -file intermediate.pem
   -keystore key.jks -storepass password
   ```

   Donde:

   -alias *ca-intermediate*
   El alias exclusivo que identifica el certificado en el almacén de claves. Cada certificado intermedio debe tener un alias exclusivo.

   -file *intermediate.pem*
   El archivo de certificado intermedio que se obtiene de la CA.

   -storepass *password*
   La contraseña del almacén de claves.
6. Importe el certificado raíz de CA emitiendo el siguiente mandato. Si se le solicita confiar en este certificado, responda *sí*.

   ```
   keytool -importcert -alias ca-root -file root.pem -keystore
   key.jks -storepass password
   ```

   Donde:

-alias *ca-root*
El alias exclusivo que identifica el certificado en el almacén de claves.

-file *root.pem*
El archivo de certificado raíz obtenido de la CA.

-storepass *password*
La contraseña del almacén de claves.

7. Importe el certificado firmado emitiendo el siguiente mandato:

```
keytool -importcert -alias mykey -file signedcert.pem -keystore
key.jks -storepass password
```

Donde:

-alias *mykey*
El alias del certificado firmado. El alias debe ser el mismo que se ha utilizado cuando generó la solicitud de firma de certificado (CSR).

-file *signedcert.pem*
El archivo de certificado firmado recibido de la CA.

-storepass *password*
La contraseña del almacén de claves.

8. Suprima el certificado existente que contiene el alias vekey:

```
keytool -delete -alias vekey -keystore key.jks -storepass password
```

Donde -storepass *password* es la contraseña del almacén de claves.

9. Cambie el nombre del certificado firmado a vekey:

```
keytool -changealias -alias mykey -destalias vekey -keystore
key.jks -storepass password
```

Donde:

-alias *mykey*
El alias del certificado firmado.

-storepass *password*
La contraseña del almacén de claves.

10. Inicie el servicio Interfaz gráfica de usuario de Data Protection para VMware vSphere.

Referencia relacionada:

"Inicio y ejecución de los servicios de Data Protection for VMware" en la página 81

Habilitación de comunicación segura con el servidor IBM Spectrum Protect

Si el servidor IBM Spectrum Protect está configurado para utilizar un protocolo Secure Sockets Layer (SSL) o Transport Layer Security (TLS), puede habilitar Interfaz gráfica de usuario de Data Protection para VMware vSphere para que se comunique con el servidor a través del protocolo SSL o TLS.

Antes de empezar

Si el servidor utiliza un certificado firmado automáticamente, debe obtener una copia de dicho certificado del administrador del servidor.

Si el servidor utiliza un certificado de tercero, debe obtener el certificado raíz de la entidad emisora de certificados (CA).

Acerca de esta tarea

El siguiente procedimiento utiliza la herramienta de gestión de certificados y claves Java **keytool**.

En sistemas operativos Linux, la herramienta está en el directorio `/opt/tivoli/tsm/tdpvmware/common/jre/jre/bin/`.

En sistemas operativos Microsoft Windows, la herramienta está en el directorio `C:\IBM\tivoli\tsm\tdpvmware\webserver\jre\jre\bin\`.

Es posible que tenga que especificar la vía de acceso completa al ejecutar el mandato **keytool**.

Procedimiento

1. En la línea de mandatos, cambie el directorio a la ubicación del almacén de confianza:
   - En Linux: `/opt/tivoli/tsm/tdpvmware/common/scripts/`
   - En Windows: `C:\Program Files (x86)\Common Files\Tivoli\TDPVMware\VMwarePlugin\scripts\`
2. Cree el almacén de confianza e importe el certificado con el siguiente mandato:

   ```
   keytool -importcert -alias my-cert -file cert.pem -keystore
   tsm-ve-truststore.jks -storepass password
   ```

   Donde:

   -alias *my-cert*
   : El alias exclusivo que identifica el certificado en el almacén de confianza.

   -file *cert.pem*
   : El archivo que contiene el certificado firmado automáticamente del servidor o el certificado raíz de CA.

   -storepass *password*
   : La contraseña del almacén de claves. Asegúrese de memorizar esta contraseña para su futuro uso.
3. Inicie Interfaz gráfica de usuario de Data Protection para VMware vSphere y vaya a la ventana Configuración.
   - Si desea crear una configuración inicial, pulse **Ejecutar asistente de configuración** y vaya a la página Credenciales del servidor.
   - Si desea modificar una configuración existente, pulse **Editar configuración** y vaya a la página Credenciales del servidor.
4. Especifique el número de puerto en el campo **Puerto de administración de IBM Spectrum Protect**.

   El número de puerto que usar es normalmente el valor especificado por la opción `SSLTCPPort` en el archivo de opciones del servidor (`dsmserv.opt`). No obstante, si la sentencia `ADMINONCLIENT NO` está especificada en el archivo `dsmserv.opt`, entonces el número de puerto correcto que utilizar para el protocolo SSL será el valor especificado por la opción `SSLTCPADMINPort`.
5. Seleccione **Usar comunicaciones SSL en el puerto de administrador**.

6. Si desea utilizar este valor para futuras sesiones de GUI, seleccione **Guardar el ID de administrador, la contraseña y la configuración de puerto**.
7. Pulse **Aceptar** para aplicar los cambios.

Requisitos de privilegios de usuario del servidor de VMware vCenter

Son necesarios ciertos privilegios del servidor de VMware vCenter para ejecutar operaciones de Data Protection for VMware.

Privilegios del servidor vCenter necesarios para proteger los centros de datos de VMware con la vista del explorador web para la Interfaz gráfica de usuario de Data Protection for VMware vSphere

El ID de usuario del servidor de vCenter que inicia sesión en la vista de navegador para la Interfaz gráfica de usuario de Data Protection for VMware vSphere

debe tener suficientes privilegios de VMware para ver el contenido del centro de datos gestionado mediante la GUI.

Por ejemplo, un entorno de VMware vSphere contiene cinco centros de datos. Un usuario, "jenn", tiene privilegios suficientes únicamente para dos de estos centros de datos. Como resultado, únicamente estos dos centros de datos donde existen privilegios suficientes son visibles para "jenn" en las vistas. Los otros tres centros de datos (donde "jenn" no tiene privilegios) no son visibles para el usuario "jenn".

El servidor de VMware vCenter define un conjunto de privilegios de forma colectiva como rol. Un rol se aplica a un objeto para usuario o grupo especificado para crear un privilegio. Desde el cliente web de VMware vSphere, debe crear un rol con un conjunto de privilegios. Para crear un rol del servidor de vCenter para operaciones de copia de seguridad y restauración, utilice la función **Añadir un rol** del cliente de VMware vSphere. Debe asignar este rol a un ID de usuario para un vCenter Server o centro de datos especificados. Si quiere propagar los privilegios a todos los centros de datos del vCenter, especifique el servidor vCenter y seleccione la casilla de verificación `propagar a hijos`. También puede limitar los permisos si asigna el rol solo a los centros de datos necesarios con la casilla de verificación `propagar a hijos` seleccionada. La implementación para la del navegador se encuentra en el nivel del centro de datos.

El ejemplo siguiente muestra cómo controlar el acceso a los centros de datos para dos grupos de usuarios de VMware. En primer lugar, cree un rol que contenga todos los privilegios definidos en nota técnica 7047438. El conjunto de privilegios de este ejemplo se identifica mediante el rol denominado "TDPVMwareManage". El grupo 1 necesita acceso para gestionar máquinas virtuales en los centros de datos `Primary1_DC` y `Primary2_DC`. El grupo 2 necesita acceso para gestionar máquinas virtuales en los centros de datos `Secondary1_DC` y `Secondary2_DC`.

Para el grupo 1, asigne el rol "TDPVMwareManage" a los centros de datos `Primary1_DC` y `Primary2_DC`. Para el grupo 2, asigne el rol "TDPVMwareManage" a los centros de datos `Secondary1_DC` y `Secondary2_DC`.

Los usuarios de cada grupo de usuarios de VMware pueden utilizar la GUI Data Protection for VMware para gestionar máquinas virtuales únicamente en sus respectivos centros de datos.

Consejo: Cuando cree un rol, plantéese añadir privilegios adicionales al rol que pueda necesitar más adelante para completar otras tareas en los objetos.

Privilegios del servidor de vCenter para utilizar el transportador de datos

El transportador de datos de IBM Spectrum Protect instalado en el Servidor de seguridad vStorage (el nodo de transportador de datos) necesita las opciones `VMCUser` y `VMCPw`. La opción `VMCUser` especifica el ID de usuario del vCenter o servidor ESX que quiere consultar, restaurar o del que quiere hacer una copia de seguridad. Los privilegios asignados a este ID de usuario (`VMCUser`) garantizan que el cliente puede ejecutar operaciones en la máquina virtual y en el entorno VMware. Este ID de usuario debe tener los privilegios de VMware descritos en nota técnica 7047438.

Para crear un rol del servidor de vCenter para operaciones de copia de seguridad y restauración, utilice la función **Añadir un rol** del cliente de VMware vSphere. Tiene que seleccionar la opción `propagar a hijos` al añadir privilegios para este ID de usuario (`VMCUser`). Considere además si quiere añadir otros privilegios a este rol para desempeñar tareas distintas a la copia de seguridad y restauración. Para la opción `VMCUser`, la implementación se produce en el objeto de más alto nivel.

Privilegios del servidor vCenter necesarios para proteger los centros de datos de VMware con la vista de la Extensión de IBM Spectrum Protect para la Interfaz gráfica de usuario de Data Protection for VMware vSphere

La Extensión de IBM Spectrum Protect necesita un conjunto de privilegios independientes de los privilegios necesarios para iniciar sesión en la GUI.

Durante la instalación, se crean los privilegios personalizados siguientes para la Extensión de IBM Spectrum Protect:

- **Centro de datos** > **IBM Data Protection**
- **Global** > **IBM Data Protection**

Los privilegios personalizados necesarios para la Extensión de IBM Spectrum Protect se registran como una extensión independiente. La clave de extensión de privilegios es `com.ibm.tsm.tdpvmware.IBMDataProtection.privileges`.

Estos privilegios permiten que el administrador de VMware pueda habilitar e inhabilitar el acceso al contenido de la Extensión de IBM Spectrum Protect. Únicamente los usuarios que tengan estos privilegios personalizados en el objeto de VMware necesario podrán acceder al contenido de la Extensión de IBM Spectrum Protect. Se registra una Extensión de IBM Spectrum Protect para cada servidor de vCenter, y se comparte entre todos los hosts de la GUI configurados para dar soporte al servidor de vCenter.

Desde el cliente web de VMware vSphere, debe crear un rol para los usuarios que puedan completar funciones de protección de datos para máquinas virtuales utilizando la Extensión de IBM Spectrum Protect. Para este rol, además de los privilegios de rol de administrador de máquina virtual estándares necesarios para el cliente web, debe especificar el privilegio **Centro de datos** > **IBM Data Protection**. Para cada centro de datos, asigne este rol para cada usuario o grupo de usuarios donde desee otorgar permiso para que el usuario pueda gestionar máquinas virtuales.

El privilegio **Global** > **IBM Data Protection** es necesario para el usuario a nivel vCenter. Este privilegio permite al usuario gestionar, editar o eliminar la conexión entre el servidor vCenter y el servidor web de Interfaz gráfica de usuario de Data Protection para VMware vSphere. Asigne este privilegio a los administradores que estén familiarizados con la Interfaz gráfica de usuario de Data Protection para VMware vSphere que protege sus respectivos servidores vCenter. Gestione sus conexiones de Extensión de IBM Spectrum Protect en la página Conexiones de la extensión.

El siguiente ejemplo muestra cómo controlar el acceso a los centros de datos para dos grupos de usuarios. El grupo 1 necesita acceso para gestionar máquinas virtuales para los centros de datos `NewYork _DC` y `Boston_DC`. El grupo 2 necesita acceso para gestionar máquinas virtuales para los centros de datos `LosAngeles_DC` y `SanFrancisco_DC`.

Desde el cliente de VMware vSphere, cree por ejemplo el rol "IBMDataProtectManage", asigne los privilegios de rol de administrador de máquina virtual y también el privilegio **Centro de datos** > **IBM Data Protection**.

Para el grupo 1, asigne el rol "IBMDataProtectManage" a los centros de datos `NewYork_DC` y `Boston_DC`. Para el grupo 2, asigne el rol "IBMDataProtectManage" a los centros de datos `LosAngeles_DC` y `SanFranciso_DC`.

Los usuarios de cada grupo pueden utilizar la Extensión de IBM Spectrum Protect en el cliente web de vSphere para gestionar máquinas virtuales sólo en sus respectivos centros de datos.

Problemas relacionados con permisos insuficientes

Cuando el usuario del explorador web no tiene permisos suficientes para cualquier centro de datos, se bloquea el acceso a la vista. En su lugar, se emite el mensaje de error GVM2013E para indicar que el usuario no está autorizado a acceder a ningún centro de datos gestionado debido a que no tiene los permisos suficientes. También hay disponibles otros mensajes nuevos que informan al usuario de problemas derivados de no tener suficientes permisos. Para solucionar cualquier problema relacionado con permisos, asegúrese de que el rol de usuario esté configurado tal y como se describe en las secciones anteriores. El rol de usuario tiene que tener todos los privilegios identificados en la tabla Privilegios necesarios para el ID de usuario del servidor de vCenter y para el transportador de datos, y estos privilegios tienen que aplicarse a nivel de centro de datos con la casilla de verificación `propagar a hijos`.

Cuando el usuario de Extensión de IBM Spectrum Protect no tiene los permisos suficientes para un centro de datos, las funciones de protección de datos para dicho centro de datos y su contenido se convierten en no disponibles en la extensión.

Cuando el ID de usuario IBM Spectrum Protect (especificado por la opción `VMCUser`) contiene permisos insuficientes para una operación de copia de seguridad y restauración, se muestra el siguiente mensaje:

```
ANS9365E Error de la API de VMware vStorage.
"El permiso para realizar esta operación se ha denegado".
```

Cuando el ID de usuario de IBM Spectrum Protect no contiene permisos suficientes para ver una máquina, se muestran los mensajes siguientes:

```
Se ha iniciado el mandato de copia de seguridad de la máquina virtual.  Número total de máquinas v
ANS4155E No se ha podido encontrar la máquina virtual 'tango' en el servidor
de VMware.
ANS4148E La copia de seguridad de máquina virtual completa de la máquina virtual
'foxtrot' ha fallado con RC 4390
```

Para recuperar la información de registro a través del servidor del centro virtual VMware para ver problemas de permisos, realice estos pasos:

1. En Valores del servidor de vCenter, seleccione **Opciones de registro** y establezca **Registro de vCenter** en **Trivia (Trivialidad)**.
2. Vuelva a crear el error de permisos.
3. Restablezca el **Registro de vCenter** a su valor anterior para evitar el registro de una cantidad excesiva de información de registro.
4. En Registros del sistema, busque el registro del servidor de vCenter más actual (`vpxd-`*`wxyz`*`.log`) y busque la serie `NoPermission`. Por ejemplo:

   ```
   [2011-04-27 15:15:35.955 03756 verbose 'App'] [VpxVmomi] Invoke error:
   vim.VirtualMachine.createSnapshot session: 92324BE3-CD53-4B5A-B7F5-96C5FAB3F0EE
   Throw: vim.fault.NoPermission
   ```

   Este mensaje de registro indica que el ID de usuario no contenía permisos suficientes para crear una instantánea (`createSnapshot`).

Roles de usuario de Interfaz gráfica de usuario de Data Protection for VMware vSphere

Las disponibilidad de las funciones de Interfaz gráfica de usuario de Data Protection for VMware vSphere se basa en el nivel de autoridad asignado a su ID de administrador de IBM Spectrum Protect.

El ID de administrador debe coincidir con el nombre de nodo. En releases de producto anteriores, el comando **REGISTER NODE** creó automáticamente un ID de usuario de administración cuyo nombre coincidía con el nombre de nodo. A partir de IBM Spectrum Protect V8.1, el comando **REGISTER NODE** no crea automáticamente un ID de usuario de administración que coincida con el nombre de nodo.

Al registrar un nodo nuevo, el administrador del servidor de IBM Spectrum Protect debe especificar el parámetro `userid` con el mandato de servidor **REGISTER NODE**:

```
REGISTER NODE nombre_nodo contraseña userid=id_usuario
```

Donde el nombre de nodo y el ID de usuario de administración deben ser el mismo. Por ejemplo:

```
REGISTER NODE node_a mypassw0rd userid=node_a
```

De forma predeterminada, el nodo tiene autorización de propietario de cliente.

Las tareas que puede ejecutar con la Interfaz gráfica de usuario de Data Protection for VMware vSphere se basan en la clase de privilegio que se asigna al ID de administrador.

Cuando el ID de administrador no tiene privilegios de dominio de políticas sin restringir, no puede registrar nuevos nodos o establecer su relación de proxy en el servidor de IBM Spectrum Protect. Si no especifica un ID de administrador, se crea un script de macro que se puede ejecutar en el servidor de IBM Spectrum Protect.

Se requiere un ID de administrador de IBM Spectrum Protect al configurar la Interfaz gráfica de usuario de Data Protection for VMware vSphere. Esta tabla lista las funciones que están disponibles según la clase de privilegios asignada a dicho ID:

- Un valor Sí indica una función disponible para el rol de usuario.
- Un valor No indica una función que no está disponible para el rol de usuario.

Para ver el rol de Interfaz gráfica de usuario de Data Protection for VMware vSphere actual, pase el cursor sobre el ID de usuario en la barra de navegación.

Tabla 16. Funciones disponibles basadas en los requisitos de privilegio de ID de administrador de IBM Spectrum Protect

	Operador	**Operador con creación de informes**	**Administrador restringido**	**Administrador**
Resumen	Ejecutar ahora copia de seguridad y restauración	Operador más creación de informes	Operador más operaciones de creación de informes y planificación para dominios de políticas listados	Todos los roles, incluida la configuración inicial
Clase de privilegios del **ID de administración de IBM Spectrum Protect**	Ninguna.	Una de las siguientes clases de privilegios: • Almacena-miento • Operador • Analista	Política (restringida) o una de las siguientes clases de privilegios: • Almacena-miento • Operador • Analista	Política (sin restricciones) o sistema
Pestaña Copia de seguridad				
Gestionar **Ejecutar ahora** tareas de copia de seguridad	Sí	Sí	Sí	Sí
Gestionar tareas de copia de seguridad **Planificadas**	No[1]	No[1]	Sí, en dominios de políticas	Sí
Ver **Ejecutar ahora** tareas de copia de seguridad	Sí	Sí	Sí	Sí
Ver tareas de copia de seguridad **Planificadas**	No	Sí	Sí	Sí
Suprimir una tarea de copia de seguridad **Planificada**	No	No	Sí, con dominios de políticas	Sí

Tabla 16. Funciones disponibles basadas en los requisitos de privilegio de ID de administrador de IBM Spectrum Protect (continuación)

	Operador	Operador con creación de informes	Administrador restringido	Administrador
Pestaña Restaurar				
Ejecutar una tarea **Restaurar**	Sí	Sí	Sí	Sí
Pestaña Informes				
Sucesos	No	Sí	Sí	Sí
Tareas recientes	Sí	Sí	Sí	Sí
Estado de copia de seguridad	No	Sí	Sí	Sí
Protección de aplicación	No	Sí	Sí	Sí
Ocupación del centro de datos	No	Sí	Sí	Sí
Pestaña Configuración				
Registro de nodo (Estado de configuración -> **Ejecutar asistente de configuración**)	No	No	No[2]	Sí
Cambiar credenciales de ID de administrador de IBM Spectrum Protect (Estado de configuración -> **Editar configuración**)	Sí	Sí	Sí	Sí
Cambiar contraseña de nodo de VMCLI (Estado de configuración -> **Editar configuración**)	No	No	Sí	Sí
Cambiar dominios de GUI (Estado de configuración -> **Editar configuración**)	Sí[3]	Sí[3]	Sí[3]	Sí

Tabla 16. Funciones disponibles basadas en los requisitos de privilegio de ID de administrador de IBM Spectrum Protect (continuación)

	Operador	Operador con creación de informes	Administrador restringido	Administrador
Cambiar nodos de transportador de datos (Estado de configuración -> **Editar configuración**)	No	No	No[2]	Sí
Cambiar nodos proxy de montaje (Estado de configuración -> **Editar configuración**)	No	No	No[2]	Sí

1. No puede registrar el nodo porque se necesita un política de dominios sin restricciones.
2. Puede añadir o eliminar centros de datos VMware y registrar nodos de centro de datos.

Para ver el nivel de autorización de ID de administrador de IBM Spectrum Protect y el rol de Interfaz gráfica de usuario de Data Protection for VMware vSphere correspondiente:

1. Vaya a la ventana Configuración.
2. Pulse **Editar configuración**.
3. La información relevante se muestra en la página Spectrum Protect Server Credentials.

Importante:

- Si el nivel de autoridad del ID de administrador de IBM Spectrum Protect cambia en el servidor deIBM Spectrum Protect, debe reiniciarse Interfaz gráfica de usuario de Data Protection for VMware vSphere para que el cambio surta efecto.
- Al cambiar el Rol del usuario, debe pulsar **Aceptar** para guardar los cambios antes de ir a otra página de Valores de configuración o intentar realizar otro cambio en la configuración. De lo contrario, sus cambios en el Rol del usuario no tendrán efecto.

Claves de registro de la GUI de Data Protection for VMware

Dependiendo de las opciones que seleccione durante la instalación, puede acceder a la GUI de Data Protection for VMware utilizando distintos métodos. Se crean claves de registro para las GUI de Data Protection for VMware.

La frase “GUI de Data Protection for VMware” se aplica a las siguientes GUI:

- La Interfaz gráfica de usuario de Data Protection for VMware vSphere accedida en un navegador web
- La Extensión de IBM Spectrum Protect en la GUI de vSphere Web Client.

La clave de registro de la Extensión de IBM Spectrum Protect es `com.ibm.tsm.tdpvmware.IBMDataProtection`. Esta clave se registra cuando

selecciona el recuadro de selección **Registrar la extensión vSphere Web Client** durante la instalación. Se registra una única instancia de Extensión de IBM Spectrum Protect por servidor de vCenter.

No se crea una clave de registro para la Interfaz gráfica de usuario de Data Protection for VMware vSphere a la que se accede en un navegador web.

Para ver las claves de registro, inicie una sesión en VMware Managed Object Browser (MOB). Después de iniciar una sesión en MOB, vaya a **Content→Extension Manager** para ver las claves de registro.

Configuración de la interfaz gráfica de usuario agente de recuperación

Instrucciones para configurar la interfaz gráfica de usuario de agente de recuperación para operaciones de montaje, restauración de archivos y restauración instantánea.

Antes de empezar

Deben completarse estas tareas de configuración antes de intentar realizar una operación en la interfaz gráfica de usuario de agente de recuperación.

Importante: Se proporciona información sobre cómo completar tareas de restauración con la interfaz gráfica de usuario del agente de recuperación en la ayuda en línea que se instala con la GUI. Pulse en **Help** en cualquiera de las ventanas de la GUI para abrir la ayuda online para las asistencias de tareas.

Procedimiento

1. Inicie sesión en un sistema donde desee restaurar archivos. agente de recuperación debe estar instalado en el sistema.
2. Pulse **Seleccionar servidor TSM** en la interfaz gráfica de usuario de agente de recuperación para conectar con un servidor de IBM Spectrum Protect. Cuando se instala el agente de recuperación en el mismo sistema que la Interfaz gráfica de usuario de Data Protection for VMware vSphere y las aplicaciones se han configurado satisfactoriamente con el asistente de configuración de la Interfaz gráfica de usuario de Data Protection for VMware vSphere, existen las siguientes condiciones:
   - El nodo de nodo de transportador de datos y el servidor deIBM Spectrum Protect se llenan en el campo agente de recuperación TSM Server.
   - Los siguientes campos se llenan en el panel Información del servidor TSM:
     - **Nodo de autenticación** contiene una lista de los nodos del transportador de datos disponibles.
     - **Nodo de destino** contiene una lista de los nodos del centro de datos disponibles para el nodo del transportador de datos seleccionado.

   Cuando solo se ha definido un nodo de transportador de datos localmente con el asistente de configuración, el agente de recuperación usa ese nodo para autenticar cuando se inició.agente de recuperación recuerda el último nombre de nodo conectado con el servidor de IBM Spectrum Protect. Si se ha seleccionado **Utilizar Generación de contraseña de acceso** para este nodo (el último nombre de nodo para establecer la conexión), el agente de recuperación utiliza estas credenciales para conectarse con el servidor de IBM Spectrum Protect durante el inicio. Si no se ha realizado ninguna conexión anterior con el servidor de IBM Spectrum Protect y sólo se han configurado un nodo del transportador de datos y un nodo de centro de datos con el asistente, agente de

recuperación utiliza estas credenciales para establecer la conexión con el servidor de IBM Spectrum Protect durante el inicio.

Especifique las opciones siguientes:

Dirección de servidos
Especifique la dirección IP o nombre de host de IBM Spectrum Protect.

Puerto de servidor
Especifique el número de puerto que se utiliza para la comunicación TCP/IP con el servidor. El número de puerto predeterminado es 1500.

Método de acceso a nodo:

Asnodename
Seleccione esta opción para utilizar un nodo proxy para acceder a copias de seguridad de máquina virtual que estén en el nodo de destino. El nodo proxy es un nodo al que se ha otorgado autoridad de "proxy" para realizar operaciones en nombre del nodo de destino.

Normalmente, el administrador de IBM Spectrum Protect utiliza el mandato `grant proxynode` para crear la relación de proxy entre dos nodos existentes.

Si selecciona esta opción, complete los siguientes pasos:

a. Escriba el nombre del nodo de destino (el nodo en el que están ubicadas las copias de seguridad de máquina virtual) en el campo **Nodo de destino**.
b. Escriba el nombre del nodo de proxy en el campo **Nodo de autenticación**.
c. Escriba la contraseña para el nodo de proxy en el campo **Contraseña**.
d. Pulse en **Aceptar** para guardar estos valores y salir al diálogo de información de IBM Spectrum Protect.

Si utiliza este método, el usuario de agente de recuperación solo conoce la contraseña del nodo de proxy, mientras que la contraseña del nodo de destino está protegida.

Fromnode
Seleccione esta opción para utilizar un nodo con acceso limitado únicamente a los datos de instantánea de máquinas virtuales específicas del nodo de destino.

Normalmente, este nodo recibe acceso desde el nodo de destino propietario de las copias de seguridad de máquinas virtuales utilizando el comando `set access`:

```
set access backup -TYPE=VM vmdisplayname mountnodename
```

Por ejemplo, este comando da al nodo `myMountNode` autoridad para restaurar archivos desde la máquina virtual `myTestVM`:

```
set access backup -TYPE=VM myTestVM myMountNode
```

Si selecciona esta opción, complete los siguientes pasos:

a. Escriba el nombre del nodo de destino (el nodo en el que están ubicadas las copias de seguridad de máquina virtual) en el campo **Nodo de destino**.
b. Escriba el nombre del nodo al que se concede acceso limitado en el campo **Nodo de autenticación**.

c. Escriba la contraseña del nodo al que se concede acceso limitado en el campo **Contraseña**.

d. Pulse en **Aceptar** para guardar estos valores y salir al diálogo de información de IBM Spectrum Protect.

Si utiliza este método, puede ver una lista completa de máquinas virtuales con copias de seguridad. Sin embargo, solo puede restaurar las copias de seguridad de máquina virtual a las que se haya concedido acceso al nodo. Además, los datos de instantánea no están protegidos contra la caducidad en el servidor. Por lo tanto, en este método la restauración instantánea no está soportada.

Directo

Seleccione esta opción para autenticar directamente ante el nodo de destino (el nodo en el que las copias de seguridad de máquina virtual están ubicadas).

Si selecciona esta opción, complete los siguientes pasos:

a. Escriba el nombre del nodo de destino (el nodo en el que están ubicadas las copias de seguridad de máquina virtual) en el campo **Nodo de autenticación**.

b. Escriba la contraseña para el nodo de destino en el campo **Contraseña**.

c. Pulse en **Aceptar** para guardar estos valores y salir al diálogo de información de IBM Spectrum Protect.

Utilizar generación de contraseñas de acceso

Cuando se selecciona esta opción y el campo de contraseña está vacío, agente de recuperación realiza la autenticación con una contraseña existente que se ha almacenado en el registro. Si no se ha seleccionado, deberá introducir la contraseña manualmente.

Para utilizar esta opción, primero debe establecer manualmente una contraseña inicial para el nodo al cual la opción aplica. Debe especificar la contraseña inicial cuando se conecta al nodo IBM Spectrum Protect por primera vez al ingresar la contraseña en el archivo **Contraseña** y seleccionar la casilla de verificación **Usar la generación de acceso de contraseña**.

Sin embargo, cuando usa el nodo de removedor de datos local como el **Nodo de autenticación**, la contraseña posiblemente ya está almacenada en el registro. Como resultado, seleccione la casilla de verificación **Use generar el acceso a la contraseña** y no ingrese una contraseña.

agente de recuperación solicita al servidor especificado una lista de máquinas virtuales protegidas y muestra la lista.

3. Defina las siguientes opciones de montaje, copia de seguridad y restauración pulsando en **Valores**:

La opción de Memoria caché de escritura de volumen virtual

El agente de recuperación que se ejecuta en el host proxy de copia de seguridad de Windows guarda los cambios de datos creados durante la restauración instantánea y el montaje. Estos cambios se guardan en un volumen virtual en la memoria caché de escritura. De forma predeterminada, la memoria caché de escritura está habilitada y especifica la vía de acceso `C:\ProgramData\Tivoli\TSM\TDPVMware\mount\` y el tamaño máximo de la memoria caché es el 90% del espacio disponible para la carpeta seleccionada. Para evitar que se llene el

volumen de sistema, cambie la memoria caché de escritura a una vía de acceso de un volumen que no sea el volumen de sistema.

Carpeta para los datos temporales
Especifique la vía de acceso en la cual se guardarán los cambios en los datos. La memoria caché de escritura debe estar en una unidad local y no se puede establecer a una vía de acceso en la carpeta compartida. Si la memoria caché de escritura está inhabilitada o llena, se producirá un fallo al intentar iniciar una sesión de restauración o montaje.

Tamaño de memoria caché
Especifique el tamaño de la memoria caché de escritura. El tamaño máximo de la memoria caché permitido es el 90% del espacio disponible para la carpeta seleccionada.

Restricción: Para evitar interrupciones durante los procesos de restauración, excluya la vía de acceso de la memoria caché de escritura de todos los valores de protección de software antivirus.

La opción de Acceso a datos
Especifique el tipo de datos al que desea acceder. Si está utilizando un dispositivo fuera de línea (como una cinta o una biblioteca de cintas virtuales), deberá especificar el tipo de datos correspondiente.

Tipo de almacenamiento
Especifique uno de los dispositivos de almacenamiento siguientes desde el cual desea montar la instantánea:

Disco/Archivo
La instantánea se monta desde un disco o un archivo. Éste es el dispositivo predeterminado.

Cinta La instantánea se monta desde una agrupación de almacenamiento de cintas. Cuando esta opción está seleccionada, no es posible montar varias instantáneas o ejecutar una operación de restauración instantánea.

VTL La instantánea se monta a partir de una biblioteca de cinta virtual fuera de línea. Las sesiones de montaje simultáneas en la misma biblioteca de cintas virtuales están soportadas.

Nota: Al cambiar el tipo de almacenamiento, debe reiniciar el servicio para que los cambios entren en vigor.

Inhabilitar la protección de la caducidad
Durante una operación de montaje, la instantánea en el servidor de IBM Spectrum Protect se bloquea para impedir que caduque durante la operación. La instantánea puede caducar si se añade otra instantánea a la secuencia de instantáneas montada. Este valor especifica si se debe inhabilitar la protección de caducidad durante la operación de montaje.

- Para impedir que la instantánea caduque, no seleccione esta opción. La instantánea en el servidor de IBM Spectrum Protect está bloqueada y la instantánea está protegida para que no caduque durante la operación de montaje.
- Para inhabilitar la protección de caducidad, seleccione esta opción. Esta opción está seleccionada de manera

predeterminada. La instantánea en el servidor de IBM Spectrum Protect no está bloqueada y la instantánea no está protegida para que no caduque durante la operación de montaje. Como resultado, la instantánea puede caducar durante la operación de montaje. El hecho de que la instantánea caduque puede generar resultados inesperados y afectar negativamente al punto de montaje. Por ejemplo, el punto de montaje puede volverse inutilizable o incluir errores. Sin embargo, la caducidad no afecta a la copia activa actual. La copia activa no puede caducar durante una operación.

Cuando la instantánea se encuentra en un servidor de réplica de destino, no puede bloquearse porque está en modalidad de solo lectura. Si el servidor intenta bloquearla, la operación de montaje falla. Para evitar el intento de bloqueo y dicho fallo, inhabilite la protección de caducidad seleccionando esta opción.

Tamaño de lectura anticipada (en bloques de 16 KB)
Especifique el número de bloques de datos adicionales recuperados del dispositivo de almacenamiento después de enviar una solicitud de lectura a un único bloque. Los valores predeterminados son los siguientes:

- Disco o archivo: 64
- Cinta: 1024
- VTL: 64

El valor máximo de cualquier dispositivo es 1024.

Tamaño de la memoria caché de lectura anticipada (en bloques)
Especifique el tamaño de la memoria caché donde se almacenar los bloques de datos adicionales. Los valores predeterminados son los siguientes:

- Disco o archivo: 10000
- Cinta: 75000
- VTL: 10000

Como cada instantánea tiene su propia memoria caché, asegúrese de planificar cuántas instantáneas se montan o se restauran simultáneamente. El tamaño de memoria caché acumulativo no puede exceder los 75000 bloques.

Tiempo de espera del controlador (segundos)
Este valor especifica la cantidad de tiempo que hay para procesar la solicitudes de datos del controlador del sistema de archivos. Si el proceso no se completa a tiempo, la solicitud se cancela y se devuelve un error al controlador del sistema de archivos. Si experimenta tiempos de espera excedidos, considere el aumento de este valor. Los tiempos de espera excedidos se producen, por ejemplo, cuando la red es lenta, el dispositivo de almacenamiento está ocupado, o se han procesado diversas sesiones de restauración instantánea o montaje. Los valores predeterminados son los siguientes:

- Disco o archivo: 60
- Cinta: 180
- VTL: 60

Pulse **Aceptar** para guardar los cambios y salir de **Valores**.

4. Verifique que todos los nodos de servidor de IBM Spectrum Protect (que se especificaran con las opciones `Asnodename` y `Fromnode`) permiten suprimir copias de seguridad. La agente de recuperación crea objetos temporales no usados durante las operaciones. La opción del servidor `BACKDELete=Yes` permite que estos objetos se eliminen de manera que no se acumulen en el nodo.
   a. Inicie sesión en el servidor de IBM Spectrum Protect e inicie una sesión de cliente administrativo en la modalidad de línea de mandatos:
      ```
      dsmadmc -id=admin -password=admin -dataonly=yes
      ```
   b. Escriba este mandato:
      ```
      Query Node <nombre_nodo> Format=Detailed
      ```
      Asegúrese de que la salida del mandato para cada nodo incluye la siguiente sentencia:
      ```
      Backup Delete Allowed?: Yes
      ```
      Si esta sentencia no está incluida, actualice cada nodo con este mandato:
      ```
      UPDate Node <nombre_nodo> BACKDELete=Yes
      ```
      Ejecute el mandato `Query Node` otra vez para cada nodo para verificar que todos los nodos permiten suprimir copias de seguridad.
5. Cuando utilice el Recover Agent en una red iSCSI, y el Recovery Agent no utilice un transportador de datos, vaya al archivo `C:\ProgramData\Tivoli\TSM\RecoveryAgent\mount\RecoveryAgent.conf` y especifique el código `[IMOUNT]` y el parámetro **`Target IP`**:
   ```
   [IMOUNT config]
   Target IP=<dirección IP de la tarjeta de red del sistema
   que expone los destinos de iSCSI.>
   ```
   Por ejemplo:
   ```
   [General config]
   param1
   param2
   ...
   [IMount config]
   Target IP=9.11.153.39
   ```
   Después de añadir o modificar el parámetro Target IP, reinicie el servicio la GUI del agente de recuperación o la CLI del agente de recuperación.

Habilitación de la comunicación segura de agente de recuperación al servidor de IBM Spectrum Protect

Si el servidor de IBM Spectrum Protect está configurado para utilizar el protocolo Capa de sockets seguros (Secure Sockets Layer, SSL) o Seguridad de la capa de transporte (Transport Layer Security, TLS), puede habilitar agente de recuperación para comunicarse con el servidor utilizando el protocolo.

Antes de empezar

Considere los siguientes requisitos antes de comenzar la configuración para la comunicación segura con el servidor:

- Cada servidor habilitado para SSL debe tener un certificado exclusivo. El certificado puede ser de uno de los siguientes tipos:

  - Un certificado autofirmado por el servidor.
  - Un certificado emitido por un certificado de una entidad emisora de certificados de terceros (CA). El certificado de autoridad emisora de certificados puede ser de una empresa como, por ejemplo, Symantec o Thawte, o un certificado interno mantenido dentro de la empresa.
- Por motivos de rendimiento, utilice SSL o TLS sólo para sesiones donde se necesite la seguridad. Considere la posibilidad de añadir más recursos de procesador en el sistema del servidor para gestionar los requisitos aumentados.
- Para que un cliente se conecte a un servidor que está utilizando TLS Versión 1.2, el algoritmo de firma de certificados debe ser Secure Hash Algorithm 1 (SHA-1) o posterior. Si está utilizando un certificado autofirmado en un servidor que utiliza TSL V1.2, debe utilizar el certificado `cert256.arm`. Es posible que el administrador de IBM Spectrum Protect necesite cambiar el certificado predeterminado del servidor.
- Para inhabilitar los protocolos de seguridad que sean menos seguros que TLS 1.2, añada la opción **`SSLDISABLELEGACYtls yes`** al archivo `C:\windows\system32\fb.opt` o `C:\Windows\SysWOW64\fb.opt`. TLS 1.2 o posterior ayuda a impedir ataques de programas malintencionados.

Habilitación de la comunicación segura utilizando un certificado autofirmado de servidor de IBM Spectrum Protect

Si el servidor de IBM Spectrum Protect está utilizando un certificado autofirmado, debe obtener una copia de ese certificado desde el administrador del servidor y configurar el agente de recuperación para comunicarse con el servidor utilizando el protocolo SSL o TLS.

Acerca de esta tarea

Cada servidor genera su propio certificado. Los servidores de Versión 6.3 y posteriores generan archivos que se denominan `cert256.arm` si el servidor está utilizando TLS 1.2 o posterior, o `cert.arm` si el servidor está utilizando una versión anterior de SSL o TLS. Las versiones del servidor anteriores a la V6.3 generan archivos que se denominan `cert.arm`, independientemente del protocolo. Debe seleccionar el certificado que se define como el predeterminado en el servidor.

El archivo de certificado se almacena en la estación de trabajo del servidor en el directorio de instancias del servidor. Por ejemplo, `C:\IBM\tivoli\tsm\server\bin\cert256.arm`. Si el archivo de certificado no existe, este se creará al reiniciar el servidor con este conjunto de opciones.

Procedimiento

Para habilitar la comunicación SSL o TLS desde el agente de recuperación al servidor utilizando un certificado autofirmado:

1. Añada la vía de acceso binaria y la vía de acceso de la biblioteca de GSKit a la variable de entorno PATH del cliente. Por ejemplo:

   ```
   set PATH=C:\Program Files\Common Files\Tivoli\TSM\api64\gsk8\bin\;
       C:\Program Files\Common Files\Tivoli\TSM\api64\gsk8\lib64;%PATH%
   ```

2. Si está configurando SSL o TLS en el cliente por primera vez, debe crear dsmcert.kdb de la base de datos clave local del cliente. Desde el directorio `C:\Windows\SysWOW64`, ejecute el mandato **`gsk8capicmd_64`** como se muestra en el ejemplo siguiente:

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

La contraseña que proporcione se utilizará para cifrar la base de datos de claves. La contraseña se almacena automáticamente cifrada en el archivo stash (dsmcert.sth). El cliente utiliza el archivo stash para recuperar la contraseña de base de datos de claves.

3. Obtenga el certificado autofirmado del servidor.
4. Importe el certificado en la base de datos dsmcert.kdb. Debe importar el certificado para cada cliente del dsmcert.kdb. Desde el directorio `C:\Windows\SysWOW64`, ejecute el mandato **gsk8capicmd_64** como se muestra en el ejemplo siguiente:

   ```
   gsk8capicmd_64 -cert -add -db dsmcert.kdb -stashed -label "Server nombre_servidor self-signed key"
   -file vía_acceso_a_certificado -format ascii -trust enable
   ```

   Se pueden añadir varios certificados de servidor a la base de datos dsmcert.kdb para que el cliente pueda conectarse a servidores diferentes. Distintos certificados deben tener distintas etiquetas. Utilice nombres significativos para las etiquetas.

   Importante: Para una recuperación tras desastre del servidor, si se ha perdido el certificado, el servidor generará automáticamente un nuevo certificado. Cada cliente debe, a continuación, importar el certificado nuevo.
5. Una vez que se añada el certificado de servidor a la base de datos dsmcert.kdb, añada la opción `ssl yes` al archivo `C:\Windows\SysWOW64\fb.opt` y actualice el valor de la opción `tcpport`.

   Importante:

   El servidor está normalmente configurado para conexiones SSL y TLS en un puerto distinto a las conexiones que no sean SSL y TLS. No especifique un número de puerto no SSL o TLS para el valor `tcpport`. Si el valor de `tcpport` es incorrecto, el agente de recuperación no puede conectarse con el servidor.

   No puede conectarse a un puerto no SSL o TLS con un agente de recuperación que está habilitado para SSL o TLS o conectar un puerto SSL o TLS a un agente de recuperación que no está habilitado para SSL o TLS.
6. Establezca los puertos SSL o TLS correctos en los siguientes archivos de configuración del agente de recuperación:
   - `C:\ProgramData\Tivoli\TSM\RecoveryAgent\mount\RecoveryAgent.conf`
   - `C:\ProgramData\Tivoli\TSM\RecoveryAgent\mount\RecoveryAgentDMNodes.conf`

Habilitación de la comunicación segura utilizando un certificado de terceros

Si el servidor de IBM Spectrum Protect está utilizando una entidad emisora de certificados (CA) de terceros, debe obtener el certificado raíz de la CA.

Acerca de esta tarea

Si el certificado lo ha emitido una CA como por ejemplo Symantec o Thawte, el cliente está listo para SSL o TLS y puede omitir los siguientes pasos de configuración. Para obtener la lista de certificados raíz preinstalados de CA, consulte Certificados raíz de entidades emisoras de certificados.

Si el certificado no lo ha emitido un certificado raíz preinstalado o es un certificado de entidad emisora de certificados interno mantenido en su empresa, debe

configurar agente de recuperación para comunicarse con el servidor utilizando el protocolo SSL o TLS.

Procedimiento

Para habilitar la comunicación de SSL o TLS del agente de recuperación al servidor utilizando un certificado de entidad emisora de certificados:

1. Añada la vía de acceso binaria y la vía de acceso de la biblioteca de GSKit a la variable de entorno PATH. Por ejemplo:

   ```
   set PATH=C:\Program Files\Common Files\Tivoli\TSM\api64\gsk8\bin\;
       C:\Program Files\Common Files\Tivoli\TSM\api64\gsk8\lib64;%PATH%
   ```

2. Si está configurando SSL o TLS en el cliente por primera vez, debe crear dsmcert.kdb de la base de datos clave local del cliente. Para los clientes, desde el directorio `C:\Windows\SysWOW64`, ejecute el mandato **gsk8capicmd_64** como se muestra en el ejemplo siguiente:

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

   La contraseña que proporcione se utilizará para cifrar la base de datos de claves. La contraseña se almacena automáticamente cifrada en el archivo stash (dsmcert.sth). El cliente utiliza el archivo stash para recuperar la contraseña de base de datos de claves.

3. Obtenga el certificado de CA.

4. Importe el certificado en la base de datos dsmcert.kdb. Debe importar el certificado para cada cliente del dsmcert.kdb. Para los clientes, desde el directorio `C:\Windows\SysWOW64`, ejecute el mandato **gsk8capicmd_64** como se muestra en el ejemplo siguiente:

   ```
   gsk8capicmd_64 -cert -add -db dsmcert.kdb -stashed -label "XYZ Certificate Authority"
   -file vía_acceso_a_certificado_raíz_CA -format ascii -trust enable
   ```

   Se pueden añadir varios certificados de servidor a la base de datos dsmcert.kdb para que el cliente pueda conectarse a servidores diferentes. Distintos certificados deben tener distintas etiquetas. Utilice nombres significativos para las etiquetas.

   Importante: Para una recuperación tras desastre del servidor, si se ha perdido el certificado, el servidor generará automáticamente un nuevo certificado. Cada cliente debe importar el certificado nuevo.

5. Una vez que se añada el certificado de servidor a la base de datos dsmcert.kdb, añada la opción `ssl yes` al archivo `C:\Windows\SysWOW64\fb.opt` y actualice el valor de la opción `tcpport`.

   Importante:

   El servidor está normalmente configurado para conexiones SSL y TLS en un puerto distinto a las conexiones que no sean SSL y TLS. No especifique un número de puerto no SSL o TLS para el valor `tcpport`. Si el valor de `tcpport` es incorrecto, el agente de recuperación no puede conectarse con el servidor.

   No puede conectarse a un puerto no SSL o TLS con un agente de recuperación que está habilitado para SSL o TLS o conectar un puerto SSL o TLS a un agente de recuperación que no está habilitado para SSL o TLS.

6. Establezca los puertos SSL o TLS correctos en los siguientes archivos de configuración del agente de recuperación:
   - `C:\ProgramData\Tivoli\TSM\RecoveryAgent\mount\RecoveryAgent.conf`

- `C:\ProgramData\Tivoli\TSM\RecoveryAgent\mount\RecoveryAgentDMNodes.conf`

Valores de entorno local

Los valores de entorno local identifican el idioma que se utiliza para las interfaces, los mensajes y la ayuda en línea.

Las GUI de Data Protection for VMware

La frase “GUI de Data Protection for VMware” se aplica a las siguientes GUI:

- La Interfaz gráfica de usuario de Data Protection for VMware vSphere accedida en un navegador web
- La Extensión de IBM Spectrum Protect en la GUI de vSphere Web Client.

Las GUI de Data Protection for VMware no dan soporte a la ejecución en un entorno que contiene valores locales incoherentes entre los procesadores que ejecutan la GUI de Data Protection for VMware, el cliente de VMware vSphere y el servidor de IBM Spectrum Protect.

Especifique los mismos valores locales entre los sistemas que ejecutan la GUI de Data Protection for VMware, el cliente de VMware vSphere y el servidor de IBM Spectrum Protect.

Cuando se accede a una página de ayuda de GUI de Data Protection for VMware a través del enlace "Obtener más información" por primera vez, la ayuda aparece en el idioma especificado por el valor de entorno local del sistema que ejecuta la GUI de Data Protection for VMware. La ayuda no se mostrará en el idioma especificado por el entorno local del cliente de VMware vSphere la primera vez que se acceda a la ayuda. En esta situación, después de que aparezca la página de ayuda de la GUI de Data Protection for VMware, pulse al menos dos enlaces dentro de la ayuda y, a continuación, cierre la ayuda. La siguiente vez que la ayuda se inicia desde el enlace "Obtener más información", se visualiza en el idioma especificado por el valor de entorno local del cliente de VMware vSphere.

Interfaz de restauración de archivos de IBM Spectrum Protect

El idioma de contenido de interfaz y solicitud de mensaje lo determina el valor de idioma del navegador web que accede a la interfaz de restauración de archivos de IBM Spectrum Protect.

Para mensajes de error que se registran en el archivo `fr_api.log`, la interfaz de restauración de archivos de IBM Spectrum Protect utiliza el idioma especificado por el valor de entorno local del sistema que ejecuta la Interfaz gráfica de usuario de Data Protection for VMware vSphere.

Actividad del archivo de registro

Data Protection for VMware crea y modifica diversos archivos de registro durante las operaciones de instalación, copia de seguridad, montaje y restauración.

Los archivos de registro de Data Protection for VMware son archivos sin formato que utilizan una extensión de archivo `.sf`.

Windows Los registros están colocados en el siguiente directorio:
`%ALLUSERSPROFILE%\Tivoli\TSM\TDPVMware`
Los directorios contienen un subdirectorio para cada componente de Data Protection for VMware. Por ejemplo, el subdirectorio de agente de recuperación es `\mount`, y el subdirectorio de la interfaz de línea de mandatos del Agente de recuperación es `\shell`.
Puede buscar archivos de registro desde el menú Inicio de **Windows**, seleccionando **Panel de control** > **Buscar** y escribiendo `*.log`.

Linux Los registros se colocan en las dos vías de acceso siguientes:
`<user.home>/tivoli/tsm/ve/mount/log`
`/opt/tivoli/tsm/TDPVMware/mount/engine/var`
Puede buscar archivos de registro escribiendo este comando:

```
find /opt/tivoli/ -name "*.log"
```

Importante: Los archivos de registro existentes se sobrescriben cada vez que se inicia una instalación. Si observa un problema de instalación y debe reinstalar el producto, recupere el archivo`TDPVMwareInstallation.log` existente del directorio `%allusersprofile%` antes de intentar una nueva instalación.

Nota: Mientras se está ejecutando el servicio Data Protection for VMware, varios archivos de sistema se mantienen en un estado abierto. Como resultado, algunos gestores de archivos no visualizan el estado actual de estos archivos y pueden informar de un tamaño de archivo de cero. Seleccionando o abriendo uno de estos archivos fuerza al gestor de archivos a actualizar los detalles del archivo.

archivos de registro de agente de recuperación

El archivo de registro agente de recuperación es `TDP_FOR_VMWARE_MOUNT`*`nnn`*`.sf`. El archivo de registro con la fecha más reciente se almacena en el archivo de registro con el número *040* (`TDP_FOR_VMWARE_MOUNT040.sf`). Cuando un archivo de registro alcanza el límite de tamaño máximo, se crea un archivo de registro nuevo. El nombre del archivo de registro es el mismo, excepto que el número disminuye en uno. De modo específico, los datos del archivo de registro con el número *040* se copian en un archivo de registro con el número *039*. El archivo de registro con el número *040* contiene los datos del archivo de registro más recientes. Cuando *040* vuelve a alcanzar el tamaño de archivo máximo, el contenido del archivo *039* se traslada al *038* y la información del *040* vuelve a ir al *039*.

Archivos de registro de la GUI de Data Protection for VMware

La Interfaz gráfica de usuario de Data Protection for VMware vSphere ubica archivos de registro en este directorio:

Windows `C:\IBM\tivoli\tsm\tdpvmware\webserver\usr\servers\veProfile\logs`

Linux `/opt/tivoli/tsm/tdpvmware/common/webserver/usr/servers/veProfile/logs`

Al recopilar archivos de registro, asegúrese de incluir todos los subdirectorios en su archivo comprimido.

archivos de registro de Interfaz de línea de mandatos de Data Protection for VMware

Interfaz de línea de mandatos de Data Protection for VMware ubica los archivos de registro en este directorio:

Windows `C:\Archivos de programa (x86)\Common Files\Tivoli\TDPVMware\VMwarePlugin\logs`

Linux `/opt/tivoli/tsm/tdpvmware/common/logs`

Al recopilar archivos de registro, asegúrese de incluir todos los subdirectorios en su archivo comprimido.

Archivos de registro de la interfaz de restauración de archivos IBM Spectrum Protect

La interfaz de restauración de archivos IBM Spectrum Protect registra mensajes de error en los archivos `fr_api.log`, `fr_gui.log` y `messages.log`. Estos archivos están en el siguiente directorio predeterminado:

Windows `C:\IBM\tivoli\tsm\tdpvmware\webserver\usr\servers\veProfile\logs`

Linux `/opt/tivoli/tsm/tdpvmware/common/webserver/usr/servers/veProfile/logs`

Puede cambiar el nombre y ubicación del archivo `fr_api.log` estableciendo las opciones `API_LOG_FILE_NAME` y `API_LOG_FILE_LOCATION` en el archivo de actividad del registro de restauración de archivos (`FRLog.config`).

El servidor IBM Spectrum Protect también registra operaciones de restauración de archivos. Puede buscar estos mensajes con un cliente de línea de mandatos administrativos del servidor.

- Para iniciar una sesión del cliente de administración en modalidad de línea de mandatos, especifique este mandato en la estación de trabajo.

  ```
  dsmadmc -id=admin -password=admin -dataonly=yes
  ```

  Si especifica el mandato **DSMADMC** con las opciones **-ID** y **-PASSWORD** tal como se muestra, no se le solicitará un ID de usuario y una contraseña.
- Para buscar la tabla ampliada de resumen SQL para ver los resultados sobre operaciones de restauración de archivos, emita el mandato **select** desde el cliente de línea de mandatos administrativos:

  ```
  select * from SUMMARY_EXTENDED where ACTIVITY_TYPE='File Restore'
  ```

  Puede limitar la búsqueda incluyendo uno o más de los siguientes criterios en la sentencia SELECT:

  ```
  * ENTITY='DATA_MOVER_NODE_NAME'
  * AS_ENTITY='DATA_CENTER_NODE_NAME'
  * SUB_ENTTTY='VM_HOST_NAME'
  * START_TIME='yyyy-MM-dd HH:mm:ss'
  ```

  Por ejemplo:

  ```
  select * from SUMMARY_EXTENDED where ACTIVITY_TYPE='File Restore'
  and ENTITY='LOCAL_MP_WIN' and AS_ENTITY='DC_NODE' and
  SUB_ENTITY='testvm'
  and START_TIME>'2015-03-11 17:30:00'
  ```

Los criterios START_TIME soportan consultas con los signos siguientes: igual (=), menor que (<) o mayor que (>).

- Para buscar la tabla de registro de actividad SQL para ver sucesos sobre operaciones de restauración de archivos, emita el mandato **select** desde el cliente de línea de mandatos administrativos:

  ```
  select * from ACTLOG
  ```

  Puede limitar la búsqueda incluyendo uno o más de los siguientes criterios en la sentencia SELECT:

  ```
  * NODENAME='DATA_CENTER_NODE_NAME'
  * DATE_TIME='yyyy-MM-dd HH:mm:ss'
  ```

  Por ejemplo:

  ```
  select
  * from ACTLOG where NODENAME='DC_NODE' and DATE_TIME>'2015-03-11 17:30:00'
  ```

Especifique *DATA_MOVER_NODE_NAME* y *DATA_CENTER_NODE_NAME* con los caracteres en mayúscula.

Los criterios DATE_TIME soportan consultas con los signos siguientes: igual (=), menor que (<) o mayor que (>).

Inicio y ejecución de los servicios de Data Protection for VMware

De forma predeterminada, al iniciar el sistema operativo Windows, agente de recuperación se inicia en Local System Account.

Ejecución de servicios de agente de recuperación en Microsoft Windows

Cuando inicia el agente de recuperación desde el menú de Inicio de Windows, el servicio se detiene automáticamente. Cuando el agente de recuperación que se ha iniciado desde el menú de Inicio finaliza, el servicio se inicia de forma automática. Asimismo, para estos sistemas operativos, el servicio no proporciona una GUI. Para utilizar la GUI, vaya al menú Inicio de Windows y seleccione **Todos los programas** > **IBM Spectrum Protect** > **Data Protection for VMware** > **agente de recuperación**.

Interfaz de línea de mandatos de Data Protection for VMware

Puede comprobar si Interfaz de línea de mandatos de Data Protection for VMware se está ejecutando completando la siguiente tarea:

Windows Vaya a **Inicio** > **Panel de control** > **Herramientas administrativas** > **Servicios** y compruebe que el estado de Interfaz de línea de mandatos de Data Protection for VMware sea Iniciado.

Linux Vaya al directorio scripts (/opt/tivoli/tsm/tdpvmware/common/scripts/) y emita este mandato:

```
./vmclid status
```

- Si el daemon no se está ejecutando, emita este mandato para iniciar manualmente el daemon:

  ```
  /opt/tivoli/tsm/tdpvmware/common/scripts/vmcli --daemon
  ```

  Estos scripts init también pueden utilizarse para detener e iniciar el daemon:

```
./vmclid stop
./vmclid start
```

Apéndice A. Tareas de configuración avanzadas

Debe configurar manualmente y verificar cada componente utilizando las interfaces de aplicación disponibles.

Antes de empezar

Asegúrese de que se dan las condiciones siguientes antes de proceder con esta tarea:

- Un servidor de IBM Spectrum Protect debe estar disponible para registrar los nodos.
- Interfaz gráfica de usuario de Data Protection for VMware vSphere está instalado en un sistema que cumple los requisitos previos de sistema operativo. Debe tener conectividad de red con los siguientes sistemas:
  - Servidor de seguridad vStorage
  - Servidor de IBM Spectrum Protect
  - Servidor vCenter

Procedimiento

1. Inicie sesión en el servidor de IBM Spectrum Protect y complete las tareas descritas en"Configuración de los nodos de IBM Spectrum Protect en un entorno de vSphere" en la página 84.
2. Inicie sesión en el servidor de seguridad vStorage y complete las tareas descritas en "Configuración de los nodos transportadores de datos en un entorno de vSphere" en la página 85.
3. Inicie la sesión en el sistema donde está instalada la Interfaz gráfica de usuario de Data Protection for VMware vSphere y complete las tareas descritas en "Configuración de la Interfaz de línea de mandatos de Data Protection for VMware en un entorno de vSphere" en la página 91.
4. En el sistema en el que esté instalado Interfaz gráfica de usuario de Data Protection for VMware vSphere, inicie vSphere Client e inicie sesión en el vCenter. Si el cliente de vSphere ya se está ejecutando, debe detenerlo y reiniciarlo.
5. Vaya al directorio de inicio del cliente de vSphere. Pulse el icono de Interfaz gráfica de usuario de Data Protection for VMware vSphere en el panel de Soluciones y aplicaciones.

   Consejo: Si el icono no aparece, el Interfaz gráfica de usuario de Data Protection for VMware vSphere no se ha registrado o se ha producido un error de conexión.

   a. En el menú Cliente de vSphere, vaya a **Plug-ins** > **Gestionar plug-ins** para iniciar el gestor de plug-ins.
   b. Si puede localizar la Interfaz gráfica de usuario de Data Protection for VMware vSphere y se ha producido un error de conexión, verifique la conectividad a la máquina donde está instalada la Interfaz gráfica de usuario de Data Protection for VMware vSphere emitiendo el mandato `ping`.

Resultados

La Interfaz gráfica de usuario de Data Protection for VMware vSphere está preparada para las operaciones de copia de seguridad y restauración.

Configuración de los nodos de IBM Spectrum Protect en un entorno de vSphere

Este procedimiento describe cómo registrar manualmente nodos en el servidor de IBM Spectrum Protect y otorgar autorización de proxy para estos nodos en un entorno de vSphere.

Antes de empezar

Importante:

Acerca de esta tarea

Todos los pasos de este procedimiento se realizan en el servidor de IBM Spectrum Protect.

Consejo: Esta tarea también se puede completar utilizando el asistente de configuración de Interfaz gráfica de usuario de Data Protection for VMware vSphere o cuaderno de edición de configuración. Inicie la Interfaz gráfica de usuario de Data Protection for VMware vSphere abriendo un navegador web y yendo al servidor web de la GUI. Por ejemplo:

```
https://guihost.mycompany.com:9081/TsmVMwareUI/
```

Inicie sesión mediante el nombre de usuario y la contraseña de vCenter.

- Para una configuración inicial, vaya a **Configuración** > **Ejecutar asistente de configuración**.
- Para una configuración existente, vaya a **Configuración** > **Editar configuración**.

Procedimiento

1. Inicie sesión en el servidor de IBM Spectrum Protect e inicie una sesión de cliente administrativo en la modalidad de línea de mandatos:

   ```
   dsmadmc -id=admin -password=admin -dataonly=yes
   ```

2. Emita el comando `REGister Node` para registrar los siguientes nodos en el servidor deIBM Spectrum Protect:
   a. El nodo que representa en VMware vCenter (nodo de vCenter):

      ```
      REGister Node MY_VCNODE <password for MY_VCNODE>
      ```

   b. El nodo que comunica a IBM Spectrum Protect y Interfaz gráfica de usuario de Data Protection for VMware vSphere (Nodo de VMCLI):

      ```
      REGister Node MY_VMCLINODE <password for MY_VMCLINODE>
      ```

   c. El nodo que representa el centro de datos y en el que se van a almacenar los datos de la máquina virtual (datacenter node):

      ```
      REGister Node MY_DCNODE <password for MY_DCNODE>
      ```

   d. El nodo que "mueve datos" de un sistema a otro (nodo transportador de datos):

      ```
      REGister Node MY_DMNODE <password for MY_DMNODE>
      ```

Atención: Al registrar nodos en el servidor de IBM Spectrum Protect, no utilice el parámetro `userid`.

3. Emita el comando `GRant PROXynode` para definir las relaciones de proxy para estos nodos:

   Recuerde: Los nodos de destino son propietarios de los datos y los nodos de agente actúan en nombre de los nodos de destino. Al otorgar autoridad proxy a un nodo de destino, un nodo de agente puede realizar operaciones de copia de seguridad y restauración para en nodo de destino.

   a. Otorgue autorización de proxy al nodo de vCenter emitiendo este mandato:
      ```
      GRant PROXynode TArget=MY_VCNODE AGent=MY_DCNODE,MY_VMCLINODE
      ```
      Este comando otorga a `MY_DCNODE` y `MY_VMCLINODE` autoridad para copiar y restaurar máquinas virtuales en nombre de`MY_VCNODE`.

   b. Otorgue autorización de proxy al datacenter node emitiendo este mandato:
      ```
      GRant PROXynode TArget=MY_DCNODE AGent=MY_VMCLINODE,MY_DMNODE
      ```
      Este comando otorga a `MY_VMCLINODE` y `MY_DMNODE` autoridad para copiar y restaurar máquinas virtuales en nombre de`MY_DCNODE`.

   c. (Opcional) Conceda autoridad proxy a cualquier nodo de datacenter node o transportador de datos adicional de su entorno.

   d. Compruebe las relaciones proxy emitiendo el comando IBM Spectrum Protect server `Query PROXynode`. La salida del comando esperada es: La salida del comando esperada es:
      ```
      Target Node       Agent Node
      --------------    ------------------------------
      MY_VCNODE               MY_DCNODE  MY_VMCLINODE
      MY_DCNODE             MY_VMCLINODE  MY_DMNODE
      ```

Qué hacer a continuación

Tras configurar correctamente los nodos de IBM Spectrum Protect, la siguiente tarea de configuración manual es configurar los nodos transportadores de datos como se describe en"Configuración de los nodos transportadores de datos en un entorno de vSphere".

Configuración de los nodos transportadores de datos en un entorno de vSphere

Si descarga cargas de trabajo de copia de seguridad en un servidor de seguridad vStorage en un entorno de vSphere, configure los nodos transportadores de datos para ejecutar la operación y mueva los datos al servidor de IBM Spectrum Protect.

Antes de empezar

En un entorno Data Protection for VMware estándar, se utiliza un archivo `dsm.opt` (Windows) o stanza de archivos `dsm.sys` (Linux) diferente para cada nodo de nodo de transportador de datos. Cuando se utilizan varios nodos de transportador de datos en un servidor de copia de seguridad de vStorage para deduplicación de datos y estos nodos tienen autoridad para mover datos para el mismo datacenter node, cada archivo `dsm.opt` o cada stanza de archivo `dsm.sys` deben incluir un valor diferente para la opción `dedupcachepath`. Para obtener los mejores resultados,

especifique una opción schedlogname y errorlogname diferentes para cada archivo dsm.opt o stanza de archivo dsm.sys. El conjunto mínimo de opciones requeridas se facilita en el Paso 2.

Un nodo transportador de datos utiliza normalmente el SAN para realizar copias de seguridad y restaurar datos. Si configura el nodo transportador de datos para acceder directamente a los volúmenes de almacenamiento, desactive la asignación de letra de unidad automática. Si no se desactiva, el cliente del nodo transportador de datos podría dañar la correlación de datos sin procesar (RDM) de los discos virtuales. Si la RDM de los discos virtuales está dañada, la copia de seguridad fallará. Al restaurar configuraciones, tenga en cuenta las siguientes condiciones:

El nodo transportador de datos está en un sistema Windows Server:
Si prevé el uso de la SAN para restaurar datos, debe definir la política de SAN de Windows como OnlineAll. Ejecute diskpart.exe y escriba los comandos siguientes para desactivar la asignación automática de letra de unidad y establezca la política de SAN en **OnlineAll**:

```
diskpart
  automount disable
  automount scrub
  san policy OnlineAll
  exit
```

El transportador de datos está instalado en una máquina virtual en un sistema Windows Server:
Si prevé el uso del transporte hotadd para restaurar datos desde discos añadidos dinámicamente, la política de SAN de ese sistema debe estar definida comoOnlineAll.

Si el cliente utiliza la SAN o el transporte hotadd, la política de SAN deWindows debe estar definida como OnlineAll. Si la política de SAN no está definida como OnlineAll, las operaciones de restauración fallarán y se devolverá el siguiente mensaje:

```
ANS9365E VMware vStoragee API error.
TSM function name: vddksdk Write
TSM file : vmvddkdsk.cpp (2271)
API return code : 1
API error message : Unknown error
ANS0361I DIAG: ANS1111I VmRestoreExtent(): VixDiskLib_Write
FAILURE startSector=512 sectorSize=512 byteOffset=262144,
rc=-1
```

Restricción: Data Protection for VMware no soporta la planificación del servidor de seguridad vStorage (utilizado como transportador de datos) para realizar una copia de seguridad de sí mismo. Asegúrese de que el servidor de seguridad vStorage se excluye de sus propias planificaciones. Utilice un servidor de seguridad vStorage diferente para realizar la copia de seguridad de una máquina virtual que contenga el servidor de seguridad vStorage.

Acerca de esta tarea

Consejo: Todos los pasos de este procedimiento se realizan en el servidor de seguridad vStorage.

Procedimiento

1. Actualice el archivo de opciones del transportador de datos con estos valores:
   - Windows Especifique estas opciones en el archivo de opciones dsm.opt.

- Linux Especifique estas opciones en el archivo `dsm.sys`, en la stanza del nodo de nodo de transportador de datos.

NODENAME
Especifique el nombre de un nodo de nodo de transportador de datos definido anteriormente. Las planificaciones de IBM Spectrum Protect están asociadas al nodo de transportador de datos.

PASSWORDACCESS
Especifique GENERATE para que se genere automáticamente la contraseña (en lugar de un indicador de usuario).

VMCHOST
Especifique el nombre de host del vCenter (o el servidor de ESX) donde se dirigen los mandatos de copia de seguridad fuera del host.

VMBACKUPTYPE
Especifique IFFULLVM. Este valor designa que se ejecute una copia de seguridad de máquina virtual completa. Este valor es necesario para ejecutar copias de seguridad de máquina virtual completa incremental constante y copias de seguridad de máquina virtual incremental constante.

MANAGEDSERVICES
Especifique esta opción para indicar al aceptador de cliente que gestione tanto el cliente web como el programador (`schedule webclient`).

TCPSERVERADDRESS
Especifique la dirección TCP/IP para el servidor de IBM Spectrum Protect.

TCPPORT
Especifique la dirección de puerto TCP/IP para el servidor de IBM Spectrum Protect.

COMMMETHOD
Especifique el método de comunicación que va a utilizar el servidor de IBM Spectrum Protect. En el caso de nodos de transportador de datos, debe especificar el método de comunicación TCP/IP. Si se especifica otro método, las operaciones fallarán.

HTTPPORT
Esta opción especifica una dirección de puerto TCP/IP y es necesaria solo cuando se utiliza más de un servicio aceptador de cliente. Por ejemplo, si se utilizan dos nodos de transportador de datos (y dos servicios aceptadores de cliente), entonces el archivo de opciones de cada nodo de transportador de datos debe especificar un valor de `HTTPPORT` diferente.

A continuación se facilita un ejemplo de archivo dsm.dm.opt con estos valores:

```
NODename MY_DMNODE
PASSWORDAccess            generate
VMCHost vcenter.storage.usca.example.com
VMBACKUPType FUllvm
MANAGEDServices schedule webclient
TCPServeraddress tsmserver.mycompany.xyz.com
TCPPort                   1500
COMMMethod tcpip
HTTPPORT 1583
```

Para las operaciones de acceso instantáneo, restauración instantánea o montaje (restauración de archivo), asegúrese de añadir `VMISCSISERVERADDRESS` en el archivo de opciones del transportador de datos. Especifique la dirección IP de servidor iSCSI de la tarjeta de red en el servidor de seguridad de vStorage que se utiliza para la transferencia de datos de iSCSI durante las operaciones instantáneas. La tarjeta de interfaz de red (NIC) física que está enlazada al dispositivo iSCSI en el host ESX debe estar en la misma subred que la NIC en el servidor de seguridad de vStorage que se utiliza para la transferencia de iSCSI.

2. Emita este comando para definir el usuario y contraseña de VMware vCenter para el nodo transportador de datos:

   ```
   dsmc set password -type=vm vcenter.mycompany.xyz.com <administrator> <password1>
   ```

3. Inicie una sesión de línea de mandatos del transportador de datos con los parámetros de línea de mandatos `-asnodename` y `-optfile`:

   ```
   dsmc -asnodename=VC1_DC1 -optfile=dsm_DM1.opt
   ```

   Asegúrese de que después del inicio de sesión inicial, no se le solicita la contraseña.

   Atención: Para evitar que falle el planificador de IBM Spectrum Protect, asegúrese de que la opción `asnodename` no está definida en el archivo `dsm.opt` (Windows) o stanza de archivos `dsm.sys` (Linux). El planificador solicita al servidor de IBM Spectrum Protect las planificaciones asociadas con `nodename` (nodo transportador de datos), no `asnodename` (datacenter node). Si `asnodename` está definido en `dsm.opt` o `dsm.sys`, se consultan las planificaciones asociadas con `asnodename` (no con `nodename`). Como resultado, fallan las operaciones de planificación.

   Realice estas tareas:

   a. Emita este mandato para verificar la conexión con el servidor de IBM Spectrum Protect:

      ```
      dsmc query session
      ```

      Este mandato muestra información acerca de la sesión como, por ejemplo, el nombre de nodo actual, cuándo se ha establecido la sesión, información del servidor e información de conexión del servidor.

   b. Verifique que puede realizar una copia de seguridad de una máquina virtual emitiendo este mandato:

      ```
      dsmc backup vm vm1
      ```

      En los pasos 3b y 3d, `vm1` es el nombre de la máquina virtual.

   c. Emita este mandato para verificar que la copia de seguridad se ha realizado correctamente:

      ```
      dsmc query vm "*"
      ```

   d. Verifique que la máquina virtual se puede restaurar emitiendo este mandato:

      ```
      dsmc restore vm vm1 -vmname=vm1-restore
      ```

4. Configure el servicio aceptador de cliente y el servicio de planificador de transportador de datos llevando a cabo las tareas siguientes:

   - Windows Este procedimiento utiliza el asistente de configuración de GUI de cliente de IBM Spectrum Protect para configurar el servicio aceptador y el servicio planificador de cliente. De forma predeterminada, el servicio de agente remoto también se configura mediante el asistente. Si utiliza el programa de utilidad de configuración del servicio de cliente (**dsmcutil**) de

IBM Spectrum Protect para esta tarea, asegúrese de haber instalado también el servicio de agente de cliente remoto.

Inicie el asistente Configuración de cliente IBM Spectrum Protect desde el menú de archivos, a través de**Programas de utilidad** > **Asistente de configuración**:

– Seleccione **Obtener ayuda para configurar el cliente web de TSM**. Especifique la información que se le solicite.

  a. En la opción `¿Cuándo desea que se inicie el servicio?` , seleccione **Automáticamente al arrancar Windows**.

  b. En la opción `¿Desea iniciar el servicio al completar este asistente?`, seleccione **Sí**.

  Una vez que la operación se haya realizado correctamente, vuelva a la página de bienvenida del asistente y vaya al paso b.

  Consejo: Si configura más de un nodo de transportador de datos en la misma máquina, debe especificar un valor de puerto diferente para cada instancia de aceptador de cliente.

– Seleccione `Obtener ayuda para configurar el planificador cliente de TSM`. Especifique la información que se le solicite.

  a. Al especificar el nombre del planificador, asegúrese de seleccionar la opción **Utilizar el daemon de aceptador de cliente (CAD) para gestionar el planificador**.

  b. En la opción `¿Cuándo desea que se inicie el servicio?` , seleccione **Automáticamente al arrancar Windows**.

  c. En la opción `¿Desea iniciar el servicio al completar este asistente?`, seleccione **Sí**.

• Linux Para el transportador de datos en Linux, lleve a cabo los pasos siguientes:

  a. Especifique las siguientes opciones en el archivo `dsm.sys`, en la stanza para nodo de nodo de transportador de datos:

  – Especifique la opción `managedservices` con estos dos parámetros:

    ```
    managedservices schedule webclient
    ```

    Este valor indica al aceptador que gestione tanto el cliente web como el programador.

  – (Opcional) Si desea dirigir información de error y planificación a otros archivos de registro distintos de los predeterminados, especifique las opciones `schedlogname` y `errorlogname` con el nombre de archivo y la vía de acceso completa en la que desea almacenar la información de registro. Por ejemplo:

    ```
    schedlogname /vmsched/dsmsched_dm.log
    errorlogname /vmsched/dsmerror_dm.log
    ```

  b. Inicie el servicio aceptador de cliente:

  El programa de instalación crea un script de inicio para el aceptador de cliente (`dsmcad`) en `/etc/init.d`. El aceptador de cliente debe iniciarse antes de que pueda gestionar tareas del programador, o gestionar el cliente web. Como raíz, lleve a cabo los siguientes pasos:

  1) Configure el servicio aceptador de cliente y el servicio de planificador de transportador de datos para que actúe como un Servidor de seguridad vStorage. Debe establecer la variable de entorno `LD_LIBRARY_PATH` en el directorio de instalación del cliente y la

biblioteca compartida de Java libjvm.so. La vía de acceso a libjvm.so también se utiliza para el soporte de descodificación al habilitar la opción de cliente vmtagdatamover en el transportador de datos.

Asegúrese de que el software Java esté instalado y la variable de entorno JAVA_HOME se haya exportado correctamente.

Las siguientes vías de acceso son ejemplos normales de la vía de acceso a libjvm.so:

- Para IBM Java: $JAVA_HOME/jre/bin/classic/libjvm.so
- Para Oracle Java: $JAVA_HOME/jre/lib/amd64/server/libjvm.so

Debe establecer la variable de entorno LD_LIBRARY_PATH en el archivo /etc/init.d/dsmcad. Por ejemplo:

- Para IBM Java, establezca la siguiente variable de entorno:

```
export LD_LIBRARY_PATH=/opt/tivoli/tsm/client/ba/bin:$JAVA_HOME/jre/bin/classic/
```

- Para Oracle Java, establezca la siguiente variable de entorno:

```
export LD_LIBRARY_PATH=/opt/tivoli/tsm/client/ba/bin:$JAVA_HOME/jre/lib/amd64/server/
```

2) Inicie el aceptador de cliente emitiendo el siguiente mandato:

```
service dsmcad start
```

Para habilitar el aceptador de cliente para que se inicie automáticamente después de reiniciar el sistema, añada el servicio de la siguiente forma, en un indicador de shell:

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

Consejo: Si desea ejecutar el mandato **dsmc** directamente desde la línea de mandatos de Linux, deberá también aplicar la variable de entorno LD_LIBRARY_PATH al shell de mandatos.

5. Verifique que el aceptador de cliente y el agente se hayan configurado correctamente:
   a. Inicie una sesión en un sistema remoto.
   b. Utilice un navegador web para conectarse al sistema HOST1 utilizando esta dirección y este puerto:

```
http://HOST1.xyz.yourcompany.com:1581
```

Consejo: Si la dirección IP del sistema en el que está instalado Interfaz gráfica de usuario de Data Protection for VMware vSphere cambia, debe hacer lo siguiente:

a. Defina el aceptador de cliente de nuevo (Paso 3) para que Interfaz gráfica de usuario de Data Protection for VMware vSphere se habilite para llevar a cabo operaciones. De lo contrario, el gestor de plug-ins muestra el estado del Interfaz gráfica de usuario de Data Protection for VMware vSphere como inhabilitado.

Qué hacer a continuación

Para configurar el servicio de aceptador de cliente y servicio de planificador de archivado y copia de seguridad de forma que actúe como servidor de seguridad vStorage, defina la variable de entorno siguiente en el archivo "Configuración de la Interfaz de línea de mandatos de Data Protection for VMware en un entorno de vSphere" en la página 91.

Configuración de la Interfaz de línea de mandatos de Data Protection for VMware en un entorno de vSphere

Actualice el perfil de la Interfaz de línea de mandatos de Data Protection for VMware en el sistema donde se ha instalado el Interfaz gráfica de usuario de Data Protection for VMware vSphere.

Antes de empezar

El perfil (`vmcliprofile`) se encuentra en este directorio en el sistema donde se ha instalado el Interfaz gráfica de usuario de Data Protection for VMware vSphere:

Linux `/opt/tivoli/tsm/tdpvmware/common/scripts`

Windows 64 bits: `C:\Archivos de programa (x86)\Common Files\Tivoli\TDPVMware\VMwarePlugin\scripts`

Acerca de esta tarea

Todos los pasos de este procedimiento se completan en el sistema donde está instalada la Interfaz gráfica de usuario de Data Protection for VMware vSphere.

Consejo: Esta tarea también se puede completar utilizando el asistente de configuración de Interfaz gráfica de usuario de Data Protection for VMware vSphere o cuaderno de configuración. Vaya a la ventana Configuración de Interfaz gráfica de usuario de Data Protection for VMware vSphere y pulse **Ejecutar asistente de configuración** o **Editar configuración**.

Procedimiento

1. Actualice el perfil con estos valores:

   VE_TSMCLI_NODE_NAME
   Especifique el nodo que conecta Interfaz de línea de mandatos de Data Protection for VMware con el servidor de IBM Spectrum Protect y el nodo agente (`MY_VMCLINODE`).

   Restricción: Nodo de VMCLI no soporta el protocolo SSL o autenticación LDAP al comunicarse con el servidor de IBM Spectrum Protect.

   VE_VCENTER_NODE_NAME
   Especifique el nodo virtual que representa un vCenter (`MY_VCNODE`).

   VE_DATACENTER_NAME
   Especifique el nodo virtual que se correlaciona con el centro de datos. A continuación, se muestra la sintaxis correcta:
   `datacenter_name::datacenter_node_name`

   - El valor de `datacenter_name` distingue entre mayúsculas y minúsculas.
   - Asegúrese de establecer este parámetro para cada centro de datos del entorno (`MY_DCNODE`).
   - El Interfaz gráfica de usuario de Data Protection for VMware vSphere no da soporte a los centros de datos con el mismo nombre en el vCenter.

VE_TSM_SERVER_NAME
Especifique el nombre de host o la dirección IP del servidor de IBM Spectrum Protect.

VE_TSM_SERVER_PORT
Especifique el nombre puerto que se utiliza para el servidor de IBM Spectrum Protect. El valor predeterminado es `1500`.

A continuación, se proporciona un perfil de ejemplo con estos valores:

```
VE_TSMCLI_NODE_NAME    MY_VMCLINODE
VE_VCENTER_NODE_NAME   MY_VCNODE
VE_DATACENTER_NAME     MyDatacenter1::MY_DCNODE
VE_TSM_SERVER_NAME     tsmserver.mycompany.xyz.com
VE_TSM_SERVER_PORT     1500
```

2. Establezca la contraseña de Nodo de VMCLI en el archivo `pwd.txt`.
Esta contraseña es para el nodo que conecta la Interfaz de línea de mandatos de Data Protection for VMware al servidor de IBM Spectrum Protect y al nodo de nodo de transportador de datos. Especificado por el parámetro de perfil VE_TSMCLI_NODE_NAME.
   a. Emita el comando `echo` para crear un archivo de texto que contenga la contraseña:

      Linux `echo password1 > pwd.txt`

      Windows `echo password1> pwd.txt`

      Windows No debe existir ningún espacio entre la contraseña (`password1`) y el signo mayor que (>).
   b. Emita este comando vmcli para definir la contraseña de Nodo de VMCLI:
      `vmcli -f set_password -I pwd.txt`

      Importante:

      - Linux Debe emitir el mandato `vmcli -f set_password` como el usuario tdpvmware, no como el usuario root.
      - Linux Windows Si piensa generar informes de protección de aplicación, debe especificar el parámetro **`-type VMGuest`** para identificar que la contraseña se aplica a una VM. Por ejemplo:
        `vmcli -f set_password -type VMGuest -I password.txt`
3. Verifique que Interfaz de línea de mandatos de Data Protection for VMware se está ejecutando:

   Windows Pulse **Inicio** > **Panel de control** > **Herramientas administrativas** > **Servicios** y compruebe que el estado de `Interfaz de línea de mandatos de Data Protection for VMware` sea `Iniciado`.

   Linux Vaya al directorio scripts (`/opt/tivoli/tsm/tdpvmware/common/scripts/`) y emita este mandato:

   `./vmclid status`

   - Si el daemon se está ejecutando, continúe en el paso 4.
   - Si el daemon no se está ejecutando, emita este mandato para iniciar manualmente el daemon:
     `/opt/tivoli/tsm/tdpvmware/common/scripts/vmcli --daemon`

     Estos scripts init también pueden utilizarse para detener e iniciar el daemon:

     ```
     ./vmclid stop
     ./vmclid start
     ```

4. Emita este mandato vmcli para comprobar si la Interfaz de línea de mandatos de Data Protection for VMware reconoce la configuración del nodo de IBM Spectrum Protect:

   ```
   vmcli -f inquire_config -t TSM
   ```

5. Valide los nodos para confirmar que no se han producido errores de configuración:
   a. Inicie el Interfaz gráfica de usuario de Data Protection for VMware vSphere pulsando el icono de la ventana Soluciones y aplicaciones del cliente de vSphere.
   b. Vaya a la ventana Configuración.
   c. Seleccione un nodo de la tabla y pulse **Validar nodo seleccionado**. La información de estado se muestra en el panelDetalles de estado.

Qué hacer a continuación

Linux Windows Tras completar correctamente las tres tareas de configuración manual descritas en esta sección:

1. "Configuración de los nodos de IBM Spectrum Protect en un entorno de vSphere" en la página 84
2. "Configuración de los nodos transportadores de datos en un entorno de vSphere" en la página 85

No es necesario realizar tareas de configuración adicionales para realizar una copia de seguridad de los datos de VM.

Lista de comprobación de configuración de interfaz de línea de mandatos de entorno de vSphere

Utilice este procedimiento para configurar Data Protection for VMware en un entorno de vSphere utilizando sólo una interfaz de línea de mandatos.

Procedimiento

Complete los Pasos 1 y 2 en el servidor de IBM Spectrum Protect.

1. Registre los siguientes nodos en el servidor de IBM Spectrum Protect:
   a. El nodo que representa en VMware vCenter (nodo de vCenter):

      ```
      REGister Node MY_VCNODE <password for MY_VCNODE>
      ```

   b. El nodo que comunica a IBM Spectrum Protect y Interfaz gráfica de usuario de Data Protection for VMware vSphere (Nodo de VMCLI):

      ```
      REGister Node MY_VMCLINODE <password for MY_VMCLINODE>
      ```

   c. El nodo que representa el centro de datos y en el que se van a almacenar los datos de la máquina virtual (datacenter node):

      ```
      REGister Node MY_DCNODE <password for MY_DCNODE>
      ```

   d. El nodo que "mueve datos" de un sistema a otro (nodo transportador de datos):

      ```
      REGister Node MY_DMNODE <password for MY_DMNODE>
      ```

2. Defina las relaciones de proxy de estos nodos:
   a. Otorgue autorización de proxy al nodo de vCenter emitiendo este mandato:

      ```
      GRant PROXynode TArget=MY_VCNODE AGent=MY_DCNODE,MY_VMCLINODE
      ```

Este mandato otorga a MY_DCNODE y MY_VMCLINODE autoridad para copiar y restaurar máquinas virtuales en nombre de MY_VCNODE.

b. Otorgue autorización de proxy al datacenter node emitiendo este mandato:

```
GRant PROXynode TArget=MY_DCNODE AGent=MY_VMCLINODE,MY_DMNODE
```

Este comando otorga a MY_VMCLINODE y MY_DMNODE autoridad para copiar y restaurar máquinas virtuales en nombre de MY_DCNODE.

c. (Opcional) Conceda autoridad proxy a cualquier nodo de datacenter node o transportador de datos adicional de su entorno.

d. Compruebe las relaciones proxy emitiendo el comando IBM Spectrum Protect server Query PROXynode. La salida del comando esperada es:

```
Target Node       Agent Node
--------------    ------------------------------
MY_VCNODE              MY_DCNODE  MY_VMCLINODE
MY_DCNODE            MY_VMCLINODE  MY_DMNODE
```

Complete los Pasos 3 a 9 en el servidor de seguridad vStorage.

3. Defina los valores adecuados para las siguientes opciones del transportador de datos:

   - Windows Especifique estas opciones en el archivo de opciones dsm.opt.
   - Linux Especifique estas opciones en el archivo dsm.sys, en la stanza del nodo de nodo de transportador de datos.

```
NODENAME
PASSWORDACCESS
VMCHOST
VMBACKUPTYPE
MANAGEDSERVICES
TCPSERVERADDRESS
TCPPORT
COMMMETHOD
HTTPPORT
```

Nota: HTTPPORT solo es necesario cuando se utiliza más de un Servicio de aceptador de cliente (CAD). Por ejemplo, si hay dos nodos transportadores de datos (y dos servicios CAD), el archivo de opciones de cada nodo transportador de datos debe especificar un valor HTTPPORT diferente.
A continuación se facilita un ejemplo de archivo dsm.dm.opt con estas opciones:

```
NODename MY_DMNODE
PASSWORDAccess            generate
VMCHost vcenter.storage.usca.example.com
VMBACKUPType FUllvm
MANAGEDServices schedule webclient
TCPServeraddress tsmserver.mycompany.xyz.com
TCPPort                   1500
COMMMethod tcpip
HTTPPORT 1583
```

4. Emita este mandato para verificar la conexión con el servidor de IBM Spectrum Protect:
   `dsmc query session`
5. Emita este comando para definir el usuario y contraseña de VMware vCenter para el nodo transportador de datos:
   `dsmc set password -type=vm vcenter.mycompany.xyz.com <administrator> <password1>`

6. Defina los siguientes servicios de IBM Spectrum Protect:
   - Windows
     a. Instale el servicio del planificador:
        ```
        dsmcutil install scheduler /name:"TSM Central Scheduler Service"
        /node:MY_DMNODE   /password:MY_DMNODEPWD /startnow:no /autostart:no
        ```
     b. Instale el CAD:
        ```
        dsmcutil install cad /name:"TSM CAD - MY_DMNODE" /node:MY_DMNODE
        /password:MY_DMNODEPWD /optfile:c:\tsm\baclient\dsm.dm.opt
        /cadschedname:"TSM Central Scheduler Service" /startnow:no /autostart:yes
        ```
     c. Instale el Servicio de agente de cliente remoto:
        ```
        dsmcutil install remoteagent /name:"TSM AGENT" /node:MY_DMNODE
        /password:MY_DMNODEPWD /optfile:c:\tsm\baclient\dsm.dm.opt
        /partnername:"TSM CAD - MY_DMNODE" /startnow:no
        ```
   - Linux Especifique la opción `managedservices` en el archivo `dsm.sys`, en la stanza para nodo de nodo de transportador de datos:

     Asegúrese de especificar los parámetros `schedule` y`webclient`:

     ```
     managedservices schedule webclient
     ```

     Este valor indica al aceptador de cliente que debe gestionar tanto el cliente web como el planificador.
7. Linux Para configurar el Servicio aceptador de cliente y el Servicio de planificador del transportador de datos de forma que actúen como un Servidor de seguridad vStorage, defina la variable de entorno siguiente en el archivo `/etc/init.d/dsmcad`:

   ```
   export LD_LIBRARY_PATH=/opt/tivoli/tsm/client/ba/bin
   ```
8. Linux Inicie el servicio de aceptador de cliente: El programa de instalación crea un script de inicio para el daemon de aceptador de cliente (`dsmcad`) en `/etc/init.d`. Para poder gestionar tareas del planificador o gestionar el cliente web, debe iniciar el daemon de aceptador de cliente. Como usuario root, utilice el siguiente comando para iniciar el daemon:

   ```
   service dsmcad start
   ```

   Para habilitar el daemon de aceptador de cliente para que se inicie automáticamente tras el reinicio del sistema, agregue el servicio como sigue, cuando se lo indique el shell:

   ```
   # chkconfig --add dsmcad
   ```
9. Compruebe si los servicios de IBM Spectrum Protect se han configurado correctamente:
   a. Inicie una sesión en un sistema remoto.
   b. Utilice un navegador web para conectarse al sistema `HOST1` utilizando esta dirección y este puerto:
      `http://HOST1.xyz.yourcompany.com:1581`

Complete en Paso 10 en el sistema en el que se ha instalado Interfaz gráfica de usuario de Data Protection for VMware vSphere.

10. Establezca los valores apropiados para las opciones siguientes en el perfil de Interfaz de línea de mandatos de Data Protection for VMware (`vmcliprofile`):

    ```
    VE_TSMCLI_NODE_NAME
    VE_VCENTER_NODE_NAME
    VE_DATACENTER_NAME
    VE_TSM_SERVER_NAME
    VE_TSM_SERVER_PORT
    ```

A continuación se facilita un perfil de ejemplo con estas opciones:

```
VE_TSMCLI_NODE_NAME    MY_VMCLINODE
VE_VCENTER_NODE_NAME   MY_VCNODE
VE_DATACENTER_NAME     MyDatacenter1::MY_DCNODE
VE_TSM_SERVER_NAME     tsmserver.mycompany.xyz.com
VE_TSM_SERVER_PORT     1500
```

El perfil se encuentra en los siguientes directorios:

Linux `/opt/tivoli/tsm/tdpvmware/common/scripts`

Windows 64 bits: `C:\Archivos de programa (x86)\Common Files\Tivoli\TDPVMware\VMwarePlugin\scripts`

a. Defina las contraseñas de Nodo de VMCLI:
   1) Emita el comando `echo` para crear un archivo de texto que contenga la contraseña:

      Linux

      ```
      echo password1 > pwd.txt
      ```

      Windows

      ```
      echo password1> pwd.txt
      ```

   2) Emita este comando vmcli para definir la contraseña de Nodo de VMCLI:

      Importante: Linux Debe emitir este comando como usuario tdpvmware, no como usuario root.

      ```
      vmcli -f set_password -I pwd.txt
      ```

b. Verifique que Interfaz de línea de mandatos de Data Protection for VMware se está ejecutando:

   Windows Emita este comando desde un indicador de comandos de Windows:

   ```
   net start
   ```

   Linux Emita este comando:

   ```
   ./vmclid status
   ```

c. Emita este mandato vmcli para comprobar si la Interfaz de línea de mandatos de Data Protection for VMware reconoce la configuración del nodo de IBM Spectrum Protect:

   ```
   vmcli -f inquire_config -t TSM
   ```

Directrices de configuración de cintas

Revise estas directrices antes de intentar realizar operaciones de copia de seguridad en almacenamiento de cinta.

Preparación de la copia de seguridad en cinta

Linux Windows Antes de intentar una copia de seguridad en cinta, deben establecerse estos parámetros en el servidor de IBM Spectrum Protect para las copias de seguridad de cinta:

1. Defina la clase de gestión:

   ```
   define mgmtclass <domain name> <policy set name> <mgmtclass name>
   ```

Por ejemplo:

```
define mgmtclass tape tape DISK
```

2. Defina el grupo de copia:

   ```
   define copygroup <domain name> <policy set name> <mgmtclass name>
   destination=<stgpool name>
   ```

   Por ejemplo:

   ```
   define copygroup tape tape DISK destination=Diskpool
   ```

3. Active el conjunto de políticas:

   ```
   activate policyset <domain name> <policy set name>
   ```

   Por ejemplo:

   ```
   activate policyset tape tape
   ```

Al configurar una copia de seguridad en una cinta física, existen determinados requisitos de configuración adicionales. Debe siempre mantener los metadatos de IBM Spectrum Protect (archivos de control) en el disco y los datos reales de copia de seguridad de la máquina virtual en cinta.

- Utilice la opción VMMC para almacenar las copias de seguridad de VMware (y los archivos de control de VMware) con una clase de gestión distinta a la clase de gestión predeterminada.
- Utilice la opción VMCTLMC para especificar la clase de gestión para utilizar específicamente para los archivos de control de VMware durante las copias de seguridad de VMware. La clase de gestión que especifique altera temporalmente la clase de gestión predeterminada. También altera temporalmente la clase de gestión especificada por la opción VMMC. La clase de gestión VMCTLMC debe especificar una agrupación de almacenamiento de discos, sin ninguna migración a la cinta.
- La opción VMMC siempre se utiliza para controlar la retención en copias de seguridad de máquinas virtuales. Esta opción corresponde tanto a configuraciones de disco como de cinta. VMCTLMC no se utiliza para la retención de archivos de control. Los archivos de control y de datos forman parte del mismo grupo y caducan juntos en función de la política de retención de la opción VMMC. Cuando se definen ambas opciones, VMMC se utiliza para los archivos de datos y VMCTLMC se utiliza para los archivos de control.

Restricción: La restauración de operaciones que utilicen agentes de almacenamiento en configuraciones sin LAN puede restaurar archivos de una agrupación de almacenamiento de copias, aunque también pueden recuperarse datos desde una agrupación de almacenamiento primario. Esto puede ocurrir si la solicitud de restauración se realiza para un archivo específico, o si la solicitud de restauración no utiliza el método de no consulta y la copia primaria del archivo se restaura en una agrupación de almacenamiento a la que no se puede acceder mediante una vía de acceso sin LAN. Ello también puede afectar a situaciones de no restauración como operaciones de copia de seguridad de Data Protection for VMware. En un entorno de Data Protection for VMware, el método preferido para los archivos de control VM es el disco, puesto que no es necesario realizar un montaje para restaurar el archivo durante el proceso de copia de seguridad incremental. Estos archivos de control VM no sólo deben ubicarse en el disco, sino que debe realizarse una copia de los mismos en una agrupación de

almacenamiento de copias que encontrará disponible en una vía de acceso sin LAN. Si realmente existen, se utilizará un montaje de cinta para restaurar los archivos durante la copia de seguridad incremental sin LAN desde un cliente de Data Protection for VMware.

Si un entorno de servidor de IBM Spectrum Protect utiliza migración de disco a cinta, tenga en cuenta las siguientes pautas antes de migrar:

- Establezca la opción MIGDELAY agrupación de almacenamiento de disco en un valor que permita satisfacer la mayoría de solicitudes de montaje del disco. Patrones de uso típicos indican que un elevado porcentaje de recuperaciones de archivos individuales ocurren transcurridos unos pocos días. Por ejemplo, generalmente 3 - 5 días desde que se modificó un archivo por última vez. Por lo tanto, considere mantener los datos en disco durante este breve periodo de tiempo para optimizar las operaciones de recuperación.

  Además, si se está utilizando la optimización del almacenamiento en el cliente con la agrupación de almacenamiento de disco, establezca la opción MIGDELAY con un valor que considere la frecuencia de las copias de seguridad completas de máquinas virtuales. No migre datos desde la agrupación de almacenamiento optimizada a una cinta hasta que se puedan realizar al menos dos copias de seguridad completas de una máquina virtual. Una vez se mueven a una cinta, no es posible optimizar el almacenamiento de los datos. Por ejemplo, si se ejecutan copias de seguridad a la semana, considere establecer MIGDELAY en un valor de al menos 10 días. Este valor garantiza que cada copia de seguridad completa identifique y utilice datos duplicados de la copia de seguridad anterior antes de moverla a cinta.
- Utilice la agrupación de almacenamiento de archivos de clase de dispositivo en lugar de una agrupación de almacenamiento de clase de dispositivo DISK. Un valor típico de un tamaño de volumen, especificado por el parámetro MAXCAPACITY de clase de dispositivo, sería entre 8 GB y 16 GB. Para la agrupación de almacenamiento asociada, considere aplicar la colocación por espacio de archivos. Cada máquina virtual que se copia aparece representada como un espacio de archivos independiente en el servidor de IBM Spectrum Protect. La colocación por espacio de archivos ahorra datos en varias copias de seguridad incrementales en una máquina virtual en el mismo volumen (archivo de disco). Cuando se produce la migración a cinta, la colocación por espacio de archivos ubica varias copias de seguridad incrementales de una máquina virtual determinada en una cinta física.

Utilice el diálogo **Configuración** para configurar el valor de la Modalidad e cinta.

Una operación de copia de seguridad se interrumpe cuando una operación de montaje o restauración instantánea requiere el mismo almacenamiento de cinta que se está utilizando simultáneamente en la operación de copia de seguridad.

Configuración manual de un dispositivo iSCSI en un sistema Linux

Linux

En este procedimiento se describe cómo configurar el sistema Linux que se utiliza durante una operación de montaje iSCSI. La instantánea de máquina virtual se monta desde el almacenamiento de servidor de IBM Spectrum Protect.

Antes de empezar

Durante un montaje de iSCSI, se crear un destino iSCSI en el sistema de Recovery Agent. Microsoft iSCSI Initiator no es necesario en el sistema de Recovery Agent.

Consejo: Open-iSCSI Initiator se facilita con Red Hat Enterprise Linux y SUSE Linux Enterprise Server.

Revise los requisitos siguientes de iSCSI antes de continuar con esta tarea:

- Puede conectarse al destino iSCSI desde cualquier sistema para crear un volumen que contenga los datos de copia de seguridad. Puede montar este volumen desde otro sistema.
- Es necesario un iniciador iSCSI en cualquier sistema que se deba conectar al destino iSCSI.
- Debe instalarse un iniciador iSCSI en el sistema donde se deben restaurar los datos.
- Si un volumen abarca varios discos, debe montar todos los discos necesarios. Cuando se utilizan volúmenes duplicados, monte sólo uno de los discos duplicados. Si se monta un disco, se evitan operaciones de sincronización que necesitan una gran cantidad de tiempo.

Acerca de esta tarea

Realice estos pasos para configurar el sistema Linux utilizado durante una operación de montaje iSCSI:

Procedimiento

1. Registre el nombre del iniciador iSCSI en el sistema en el que se van a restaurar los datos. El nombre del iniciador iSCSI se encuentra en el archivo `/etc/iscsi/initiatorname.iscsi`. Si el valor `InitiatorName=` está vacío, cree un nombre de iniciador con el mandato siguiente:

   ```
   twauslbkpoc01:~ # /sbin/iscsi-iname
   ```

   A continuación se muestra un ejemplo de nombre de iniciador:

   ```
   iqn.2005-03.org.open-iscsi:3f5058b1d0a0
   ```

2. Añada el nombre de iniciador al archivo `/etc/iscsi/initiatorname.iscsi`.
   a. Edite el archivo `/etc/iscsi/initiatorname.iscsi` con el mandato **vi**. Por ejemplo:

      ```
      twauslbkpoc01:~ # vi /etc/iscsi/initiatorname.iscsi
      ```

   b. Actualice el parámetro **InitiatorName=** con el nombre de iniciador. Por ejemplo:

      ```
      InitiatorName=iqn.2005-03.org.open-iscsi:3f5058b1d0a0
      ```

3. Siga estos pasos en el sistema donde está instalado el agente de recuperación (o el destino iSCSI):
   a. Inicie el agente de recuperación. Complete los diálogos `Seleccionar servidor IBM Spectrum Protect` y `Seleccionar instantánea` y pulse **Montar**.
   b. En el diálogo `Seleccionar destino de montaje`, seleccione `Montar un destino iSCSI`.
   c. Cree un nombre de destino. Asegúrese de que sea exclusivo y que pueda identificarlo desde el sistema que ejecuta el lanzador iSCSI. Por ejemplo:

      ```
      iscsi-mount-tsm4ve
      ```

d. Especifique el nombre del iniciador iSCSI registrado en el Paso 1 y pulse **Aceptar**.
e. Verifique que el volumen que acaba de montar aparezca en el campo `Volúmenes montados`.

4. Localice e inicie el programa del iniciador iSCSI en el sistema del iniciador seleccionado en el Paso 1:
   a. Compruebe que el servicio iSCSI se está ejecutando emitiendo este comando:
      Red Hat Enterprise Linux:
      ```
      service iscsi status
      ```
      SUSE Linux Enterprise Server:
      ```
      service open-iscsi status
      ```
      Si el servicio no se está ejecutando, emita este comando para iniciar manualmente el servicio:
      Red Hat Enterprise Linux:
      ```
      service iscsi start
      ```
      SUSE Linux Enterprise Server:
      ```
      service open-iscsi start
      ```
   b. Conéctese con el destino iSCSI emitiendo este comando:
      ```
      iscsiadm -m discovery -t sendtargets -p <IP/nombre host del
      agente de recuperación  system> --login
      ```
   c. Compruebe si hay disponible un nuevo dispositivo en bruto emitiendo este comando:
      ```
      fdisk -l
      ```
5. Monte el sistema de archivos:
   Para un volumen no LVM, emita los mandatos siguientes. En este ejemplo, el dispositivo nuevo es `/dev/sdb1`:
   ```
   mkdir /mountdir
   mount /dev/sdb1 /mountdir
   ```
   Para un volumen LVM, complete las tareas siguientes en el invitado Linux:
   a. Asegúrese de que el script `vgimportclone` esté disponible en el sistema Linux. Este script no se proporciona en el paquete LVM de base (predeterminad). Por ello, quizá deba actualizar el paquete LVM a un nivel que proporcione este script.
   b. Emita el mandato **vgimportclone** e incluya un nombre de grupo de volúmenes base nuevo (`VolGroupSnap01`). Por ejemplo:
      ```
      vgimportclone --basevgname /dev/VolGroupSnap01 /dev/sdb1
      ```
   c. Emita el mandato **lvchange** para marcar el volumen lógico como activo. Por ejemplo:
      ```
      lvchange -a y /dev/VolGroupSnap01/LogVol00
      ```
   d. Emita estos mandatos para montar el volumen:
      ```
      mkdir /mountdir
      mount -o ro /dev/VolGroupSnap01/LogVol00 /mountdir
      ```
6. Una vez completada la operación de restauración de archivo, emita estos mandatos:
   - Para un volumen no LVM, emita los siguientes comandos:
     a. Desmonte el sistema de archivos:

```
umount /dev/sdb1 /mountdir
```

b. Elimine el volumen. Si el volumen forma parte de un grupo de volúmenes, elimine primero el volumen del grupo de volúmenes emitiendo el mandato siguiente:

```
vgreduce <grupo_volúmenes> /dev/sdb1
```

A continuación, emita este mandato para eliminar el volumen:

```
pvremove /dev/sdb1
```

c. Finalice sesión en un destino individual:

```
iscsiadm --mode node --targetname <target_name> --logout
```

d. Finalice sesión en todos los destinos:

```
iscsiadm --mode node --logout
```

- Para un volumen LVM, complete las tareas siguientes en el invitado Linux:
  a. Desmonte el sistema de archivos:

```
unmount /mountdir
```

  b. Elimine el volumen lógico:

```
lvm lvremove LogVol00
```

  c. Elimine el grupo de volúmenes:

```
lvm vgremove VolGroupSnap01
```

  d. Finalice sesión en un destino individual:

```
iscsiadm --mode node --targetname <target_name> --logout
```

  e. Finalice sesión en todos los destinos:

```
iscsiadm --mode node --logout
```

Configuración manual de un dispositivo iSCSI en un sistema Windows

Windows

Este procedimiento describe cómo configurar un sistema Windows que se utiliza durante una operación de montaje iSCSI. La instantánea se monta desde un almacenamiento de servidor de IBM Spectrum Protect.

Antes de empezar

Revise los requisitos siguientes de iSCSI antes de continuar con esta tarea:

- Durante un montaje de iSCSI, se crear un destino iSCSI en el sistema de agente de recuperación. Puede conectarse al destino iSCSI desde cualquier sistema para crear un volumen que contenga los datos de seguridad. Además, puede montar a continuación este volumen desde otro sistema.
- El iniciador iSCSI es necesario en cualquier sistema que se deba conectar al destino iSCSI.
- Asegúrese de que haya un iniciador iSCSI instalado en el sistema donde se vayan a restaurar los datos.
- Microsoft iSCSI Initiator no es necesario en el sistema de agente de recuperación.

Revise el disco siguiente y los requisitos de volumen antes de continuar con esta tarea:

- Si un volumen abarca varios discos, debe montar todos los discos necesarios. Cuando se utilizan volúmenes duplicados, monte sólo uno de los discos duplicados. Si se monta un disco, se evitan operaciones de sincronización que necesitan una gran cantidad de tiempo.

- Si se utilizan varios discos dinámicos en el sistema de copia de seguridad, estos discos se asignan al mismo grupo. Como resultado, es posible que el Gestor de discos de Windows considere algunos discos como ausentes y emita un mensaje de error cuando se monta sólo un disco. Ignore este mensaje. Se sigue pudiendo acceder a los datos del disco del que se ha hecho una copia de seguridad, a menos que algunos de los datos se encuentren en el otro disco. Este problema puede resolverse montando todos los discos dinámicos.

Acerca de esta tarea

Realice estas tareas para configurar el sistema Windows que se utiliza durante una operación de montaje iSCSI:

Procedimiento

1. En el sistema de agente de recuperación, abra el puerto `3260` del cortafuegos LAN y el cortafuegos cliente de Windows. Registre el nombre del iniciador iSCSI en el sistema en el que se van a restaurar los datos.

   El nombre del iniciador iSCSI se muestra en la ventana de configuración del iniciador iSCSI del Panel de control. Por ejemplo:

   ```
   iqn.1991-05.com.microsoft:hostname
   ```

2. Realice estas tareas en el sistema donde está instalado agente de recuperación (o el destino iSCSI):
   a. Inicie la GUI de agente de recuperación. Complete los diálogos Seleccionar servidor IBM Spectrum Protect y Seleccionar instantánea y pulse **Montar**.
   b. En el diálogo Seleccionar destino de montaje, seleccione **Montar un destino iSCSI**.
   c. Cree un nombre de destino. Asegúrese de que sea exclusivo y que pueda identificarlo desde el sistema que ejecuta el lanzador iSCSI. Por ejemplo:

      ```
      iscsi-mount-tsm4ve
      ```

   d. Especifique el nombre del iniciador iSCSI registrado en el Paso 1 y pulse **Aceptar**.
   e. Verifique que el volumen que acaba de montar aparezca en el campo Volúmenes montados.
   f. Cuando utilice el Recovery Agent en una red iSCSI, y el Recovery Agent no utilice un transportador de datos, vaya al archivo `C:\ProgramData\Tivoli\TSM\RecoveryAgent\mount\RecoveryAgent.conf` y especifique el código `[IMOUNT]` y el parámetro **`Target IP`**:

      ```
      [IMOUNT config]
      Target IP=<dirección IP de la tarjeta de red del sistema
      que expone los destinos de iSCSI.>
      ```

      Por ejemplo:

      ```
      [General config]
      param1
      param2
      ...
      [IMount config]
      Target IP=9.11.153.39
      ```

      Después de añadir o modificar el parámetro Target IP, reinicie el servicio la GUI de agente de recuperación o la CLI de agente de recuperación.
3. Localice e inicie el programa del iniciador iSCSI en el sistema del iniciador seleccionado en el Paso 1:
   a. Conéctese con el destino iSCSI:

1) En el separador Destinos, especifique la dirección TCP/IP del agente de recuperación (destino iSCSI) utilizado en el paso 2 en el diálogo Destino:. Pulse **Conexión rápida**.
2) El diálogo Conexión rápida muestra un destino que coincide con el nombre de destino especificado en el Paso 2c. Si no está ya conectado, seleccione este destino y pulse **Conectar**.

b. En el sistema del lanzador, vaya a **Panel de control** > **Herramientas administrativas** > **Gestión de sistemas** > **Almacenamiento** > **Gestión de discos**.
1) Si el destino iSCSI montado aparece como Tipo=Foráneo, pulse con el botón derecho del ratón sobre **Disco foráneo** y seleccione **Importar discos foráneos**. Se selecciona el Grupo de discos foráneos. Haga clic en **Aceptar**.
2) La siguiente pantalla muestra el tipo, la condición y el tamaño del disco foráneo. Pulse **Aceptar** y espere a que se importe el disco.
3) Cuando finalice la importación del disco, pulse **F5** (renovar). La instantánea iSCSI montada aparece visible y contiene una letra de unidad asignada. Si las letras de unidad no se asignan automáticamente, pulse con el botón derecho del ratón sobre la partición necesaria y seleccione **Cambiar letras de unidad o vías de acceso**. Pulse **Añadir** y seleccione una letra de unidad.

4. Abra Windows Explorer (u otro programa de utilidad) y desplácese a la instantánea montada para una operación de restauración de archivos.
5. Después de que se haya restaurado el archivo, realice estas tareas:
   a. Desconecte cada destino iSCSI utilizando el diálogo Propiedades de iniciador iSCSI.
   b. Desmonte el volumen del paso 2 seleccionando el volumen en la GUI de agente de recuperación y pulsando **Desmontar**.

Configuración manual de los nodos de proxy de montaje en un sistema Linux

Linux

Realice esta tarea para añadir un nodo de proxy de montaje a un sistema Linux remoto.

Antes de empezar

En un entorno de Interfaz gráfica de usuario de Data Protection for VMware vSphere estándar, se utiliza una stanza del archivo `dsm.sys` independiente para cada nodo de proxy de montaje. Todos los pasos de este procedimiento se completan utilizando el transportador de datos instalado en el servidor de seguridad.

Acerca de esta tarea

Esta tarea configura los nodos de proxy de montaje actualizando las opciones del transportador de datos y verificando la conectividad con el servidor de IBM Spectrum Protect.

Procedimiento

1. Especifique estas opciones en el archivo `dsm.sys`, en la stanza del nodo de proxy de montaje.

   NODENAME
   Especifique el nombre de un nodo de proxy de montaje definido anteriormente. Las planificaciones de IBM Spectrum Protect están asociadas con este nodo.

   PASSWORDACCESS
   Especifique GENERATE para que se genere automáticamente la contraseña (en lugar de un indicador de usuario).

   MANAGEDSERVICES
   Especifique esta opción para dirigir el aceptador de cliente para gestionar tanto el cliente web como el planificador (`schedule webclient`).

   TCPSERVERADDRESS
   Especifique la dirección TCP/IP para el servidor de IBM Spectrum Protect.

   TCPPORT
   Especifique la dirección de puerto TCP/IP para el servidor de IBM Spectrum Protect.

   COMMMETHOD
   Especifique el método de comunicación que va a utilizar el servidor de IBM Spectrum Protect. Para los nodos de proxy de montaje, debe especificar TCP/IP como método de comunicación. Si especifica otro método, fallarán las operaciones.

   HTTPPORT
   Esta opción especifica una dirección de puerto TCP/IP y sólo debe especificarse cuando se utiliza más de un Servicio aceptador de cliente (CAD). Por ejemplo, si existen dos nodos de proxy de montaje (y dos servicios CAD), el archivo de opciones de cada uno de los nodo de proxy de montaje debe especificar un valor de `HTTPPORT` distinto.

   Restricción: No habilite la opción libre de LAN (`ENABLELANFREE YES`) en el archivo `dsm.sys`. Esta opción no tiene soporte para nodos proxy de montaje. A continuación, se proporciona un archivo dsm.sys de ejemplo con estos valores:

```
Servername     tsm_server1
  NODename datacenter1_MP_LNX
  PASSWORDAccess            generate
  MANAGEDServices schedule webclient
  TCPServeraddress tsmserver.myco.com
  TCPPort                   1500
  COMMMethod tcpip
  HTTPPORT 1583
```

2. Emita este mandato para definir el usuario y la contraseña de VMware vCenter para el nodo de proxy de montaje:
   `dsmc set password -type=vm vcenter.mycompany.xyz.com <administrator> <password1>`
3. Inicie una sesión de línea de mandatos del transportador de datos con los parámetros de línea de mandatos `-asnodename` y `-optfile`:
   `dsmc -asnodename=vctr1_datacenter1 -optfile=dsm_MP_LNX.sys`
   Asegúrese de que después del inicio de sesión inicial, no se le solicita la contraseña.

Atención: Para evitar que falle el planificador de IBM Spectrum Protect, asegúrese de que la opción `asnodename` no está definida en la stanza del archivo `dsm.sys` (Linux). El planificador consulta el servidor de IBM Spectrum Protect para ver las planificaciones asociadas con `nodename` (nodo de proxy de montaje), y no `asnodename` (datacenter node). Si `asnodename` está definido en `dsm.sys`, se consultan las planificaciones asociadas con `asnodename` (y no `nodename`). Como resultado, fallan las operaciones de planificación.

4. Emita este mandato para verificar la conexión con el servidor de IBM Spectrum Protect:
   ```
   dsmc query session
   ```
   Este mandato muestra información acerca de la sesión como, por ejemplo, el nombre de nodo actual, cuándo se ha establecido la sesión, información del servidor e información de conexión del servidor.
5. Configure el Servicio de aceptador de cliente (CAD) y el Servicio de planificador del transportador de datos llevando a cabo las tareas siguientes:
   - Especifique estas opciones en el archivo `dsm.sys`, en la stanza del nodo de proxy de montaje:
     - Especifique la opción `managedservices` con estos dos parámetros:
       ```
       managedservices schedule webclient
       ```
       Este valor indica al aceptador de cliente que debe gestionar tanto el cliente web como el planificador.
     - Si desea dirigir información de error y planificación a otros archivos de registro distintos de los predeterminados, especifique las opciones `schedlogname` y `errorlogname`. Cada opción debe contener la vía de acceso completa y el nombre de archivo en que se debe almacenar la información de registro. Por ejemplo:
       ```
       schedlogname /vmsched/dsmsched_mp_lnx.log
       errorlogname /vmsched/dsmerror_mp_lnx.log
       ```
   - Para configurar el Servicio de aceptador de cliente y el Servicio de planificador del transportador de datos de forma que actúen como servidor de seguridad, defina la variable de entorno siguiente en el archivo `/etc/init.d/dsmcad`:
     ```
     export LD_LIBRARY_PATH=/opt/tivoli/tsm/client/ba/bin
     ```
   - Inicie el servicio de aceptador de cliente:

     El programa de instalación crea un script de inicio para el daemon de aceptador de cliente (`dsmcad`) en `/etc/init.d`. Para poder gestionar tareas del planificador o gestionar el cliente web, debe iniciar el daemon de aceptador de cliente. Como usuario root, utilice el siguiente comando para iniciar el daemon:
     ```
     export LD_LIBRARY_PATH=/opt/tivoli/tsm/client/ba/bin
     service dsmcad start
     ```
     Para habilitar el daemon de aceptador de cliente para que se inicie automáticamente tras el reinicio del sistema, agregue el servicio como sigue, cuando se lo indique el shell:
     ```
     # chkconfig --add dsmcad
     ```
6. Verifique que el aceptador de cliente y el agente se hayan configurado correctamente:
   a. Inicie una sesión en un sistema remoto.
   b. Utilice un navegador web para conectarse al sistema `HOST1` utilizando esta dirección y este puerto:

http://HOST1.xyz.yourcompany.com:1581

Configuración manual de los nodos de proxy de montaje en un sistema Windows remoto

Windows

Realice esta tarea para añadir un nodo de proxy de montaje a un sistema Windows remoto. Esta tarea es obligatoria si desea añadir un segundo nodo proxy de montaje de Windows en su entorno.

Antes de empezar

Antes de seguir con esta tarea, asegúrese de que el nodo de proxy de montaje primario de Windows está configurado.

Acerca de esta tarea

Realice estos pasos en el sistema proxy de montaje de Windows remoto:

Procedimiento

1. Instale los productos siguientes en el sistema proxy de montaje de Windows remoto:
   - agente de recuperación
   - Transportador de datos de IBM Spectrum Protect

   Acceda a ambos productos en la imagen de descarga de IBM Spectrum Protect for Virtual Environments. Las instrucciones de instalación paso a paso están disponibles en IBM Knowledge Center en
   "Instalación de los componentes de Data Protection for VMware en sistemas Windows" en la página 21
2. Recupere el contenido del archivo de opciones de ejemplo del nodo proxy de montaje de Windows y añádalo al archivo de opciones del sistema proxy de montaje de Windows remoto:
   a. En el sistema proxy de montaje de Windows remoto, vaya a la ventana Configuración de la Interfaz gráfica de usuario de Data Protection for VMware vSphere.
   b. Pulse **Editar configuración de TSM** en la lista Tareas. Es posible que el cuaderno de configuración tarde un poco en cargarse.
   c. Vaya a la página Pares de nodos proxy de montaje.
   d. En la columna Nodo primario de la tabla, acceda al nodo proxy de montaje de Windows con la ubicación pendiente y pulse **Ver valores**.
   e. Copie el contenido del archivo de ejemplo `dsm.opt` que se muestra en el diálogo **Valores de proxy de montaje**.
   f. Pegue (o añada) el contenido del archivo `dsm.opt` de ejemplo en el archivo de opciones del sistema proxy de montaje de Windows remoto. Nombre el archivo de opciones con un convenio que identifique su rol como un nodo de proxy de montaje remoto.
   Por ejemplo: `dsm.REMOTE1_MP_WIN.opt`.

   Restricción: No habilite la opción libre de LAN (`ENABLELANFREE YES`) en el archivo de opciones. Esta opción no tiene soporte para nodos proxy de montaje.

3. Emita este mandato del transportador de datos para definir el usuario y la contraseña de VMware vCenter para el nodo de proxy de montaje:

   Consejo: Para iniciar la línea de mandatos de dsmc, abra el menú **Inicio de Windows** y seleccione **Programas→ IBM Spectrum Protect → Línea de mandatos del cliente de copia de seguridad**.

   ```
   dsmc set password -type=vm vcenter.mycompany.xyz.com <administrator> <password1>
   -optfile=dsm.REMOTE1_MP_WIN.opt
   ```

4. Emita este mandato para verificar la conexión con el servidor de IBM Spectrum Protect:

   ```
   dsmc query session -optfile=dsm.REMOTE1_MP_WIN.opt
   ```

   Este mandato muestra información acerca de la sesión como, por ejemplo, el nombre de nodo actual, cuándo se ha establecido la sesión, información del servidor e información de conexión del servidor.

5. Configure el Servicio de aceptador de cliente (CAD) y el Servicio de planificador del transportador de datos llevando a cabo los pasos siguientes: Este paso utiliza el asistente de configuración de la GUI de cliente IBM Spectrum Protect para establecer el servicio de planificador y CAD. De forma predeterminada, el Servicio de agente de cliente remoto también se configura a través de este asistente. Utiliza el programa de utilidad de configuración del servicio de cliente IBM Spectrum Protect (`dsmcutil`) para esta tarea, asegúrese de que también instala el servicio de agente de cliente remoto.
   Inicie el asistente Configuración de cliente IBM Spectrum Protect desde el menú de archivos, a través de **Programas de utilidad >Asistente de configuración**:
   a. Seleccione `Obtener ayuda para configurar el cliente web de TSM`. Especifique la información que se le solicite.
      1) En la opción `¿Cuándo desea que se inicie el servicio?` , seleccione `Automáticamente al arrancar Windows`.
      2) En la opción `¿Desea iniciar el servicio al completar este asistente?`, seleccione `Sí`.

      Una vez que la operación se haya realizado correctamente, vuelva a la página de bienvenida del asistente y vaya al paso b.

      Consejo: Cuando configure más de un nodo de proxy de montaje en el mismo sistema, debe especificar un valor de puerto distinto para cada instancia de aceptador de cliente.

   b. Seleccione `Obtener ayuda para configurar el planificador cliente de TSM`. Especifique la información que se le solicite.
      1) Al especificar el nombre del planificador, asegúrese de seleccionar la opción `Utilizar el daemon de aceptador de cliente (CAD) para gestionar el planificador`.
      2) En la opción `¿Cuándo desea que se inicie el servicio?` , seleccione `Automáticamente al arrancar Windows`.
      3) En la opción `¿Desea iniciar el servicio al completar este asistente?`, seleccione `Sí`.

6. Verifique que el aceptador de cliente y el agente se hayan configurado correctamente. Utilice un navegador web para conectarse al sistema `HOST1` utilizando esta dirección y este puerto:

   `http://HOST1.xyz.yourcompany.com:1581`

Configuración manual de varios servicios aceptadores de cliente en un sistema Linux

Bajo ciertas circunstancias, puede ser beneficioso utilizar varios servicios dsmcad en un único host de cliente de Linux.

Acerca de esta tarea

Esta tarea configura varias instancias dsmcad para que se ejecuten e inicien automáticamente cuando se inicia el sistema:

Procedimiento

1. Cree dos stanzas de nodo exclusivas en el archivo dsm.sys (de forma predeterminada, este archivo se encuentra en `/opt/tivoli/tsm/client/ba/bin/`):

```
# cat /opt/tivoli/tsm/client/ba/bin/dsm.sys
SErvername node1
  COMMMethod               TCPip
  TCPPort                  1500
  TCPServeraddress   localhost
  nodename           node1
  errorlogname       /opt/tivoli/tsm/client/ba/bin/dsmerror-node1.log
  schedlogname       /opt/tivoli/tsm/client/ba/bin/dsmsched-node1.log
  managedservices    webclient sched
  httpport           1581
  passwordaccess     generate

SErvername node2
  COMMMethod               TCPip
  TCPPort                  1500
  TCPServeraddress   localhost
  nodename           node2
  errorlogname       /opt/tivoli/tsm/client/ba/bin/dsmerror-node2.log
  schedlogname       /opt/tivoli/tsm/client/ba/bin/dsmsched-node2.log
  managedservices    webclient sched
  httpport           1582
  passwordaccess     generate
```

   Consejo: Es posible que sea útil incluir ciertas opciones includes/exclude para diferencias estos nodos. De lo contrario, es posible que se realice una copia de seguridad de los mismos datos utilizando los dos nombres de nodo.

2. Cree dos archivos dsm.opt, uno para cada nodo (de forma predeterminada, estos archivos están en `/opt/tivoli/tsm/client/ba/bin`):

```
# cat /opt/tivoli/tsm/client/ba/bin/dsm-node1.opt
servername node1
# cat /opt/tivoli/tsm/client/ba/bin/dsm-node2.opt
servername node2
```

3. Habilite `passwordaccess generate` iniciando sesión con las credenciales en ambos nodos:

```
# cat /opt/tivoli/tsm/client/ba/bin/dsm-node1.opt
servername node1
# cat /opt/tivoli/tsm/client/ba/bin/dsm-node2.opt
servername node2
```

4. Realice dos copias del script init predeterminado `rc.dsmcad` (de forma predeterminada, este script se encuentra en `/opt/tivoli/tsm/client/ba/bin`):

```
# cp /opt/tivoli/tsm/client/ba/bin/rc.dsmcad /opt/tivoli/tsm/client/ba/bin/rc.dsmcad-node1
# cp /opt/tivoli/tsm/client/ba/bin/rc.dsmcad /opt/tivoli/tsm/client/ba/bin/rc.dsmcad-node2
```

5. Edite rc.dsmcad-node1:
   a. Modifique esta línea para distribuciones de Red Hat Enterprise Linux:

      ```
      daemon $DSMCAD_BIN
      ```

      Por esta línea:

      ```
      daemon $DSMCAD_BIN -optfile=/opt/tivoli/tsm/client/ba/bin/dsm-node1.opt
      ```

   b. Cambie esta línea para distribuciones SUSE Linux Enterprise Server:

      ```
      startproc $DSMCAD_BIN
      ```

      Por esta línea:

      ```
      startproc $DSMCAD_BIN -optfile=/opt/tivoli/tsm/client/ba/bin/dsm-node1.opt
      ```

6. Edite rc.dsmcad-node2:
   a. Cambie esta línea para distribuciones de Red Hat Enterprise Linux:

      ```
      daemon $DSMCAD_BIN
      ```

      Por esta línea:

      ```
      daemon $DSMCAD_BIN -optfile=/opt/tivoli/tsm/client/ba/bin/dsm-node2.opt
      ```

   b. Cambie esta línea para distribuciones SUSE Linux Enterprise Server:

      ```
      startproc $DSMCAD_BIN
      ```

      Por esta línea:

      ```
      startproc $DSMCAD_BIN -optfile=/opt/tivoli/tsm/client/ba/bin/dsm-node2.opt
      ```

7. Cree nuevos enlaces en `/etc/init.d/` para hacer referencia a los dos nuevos scripts ini rc.dsmcad. Estos enlaces permiten que el servicio init de Linux inicie los servicios dsmcad en el inicio del sistema:

   ```
   # ln -s /opt/tivoli/tsm/client/ba/bin/rc.dsmcad-node2 dsmcad-node2
   # ln -s /opt/tivoli/tsm/client/ba/bin/rc.dsmcad-node1 dsmcad-node1
   # ls -la dsm*
   lrwxrwxrwx. 1 root root 45 Aug  2 08:04 dsmcad-node1 -> /opt/tivoli/tsm/client/ba/bin/rc.dsmcad-node1
   lrwxrwxrwx. 1 root root 45 Aug  2 08:04 dsmcad-node2 -> /opt/tivoli/tsm/client/ba/bin/rc.dsmcad-node2
   ```

8. Registre los dos nuevos scripts rc con **`chkconfig`**:

   ```
   # chkconfig --add dsmcad-node1
   # chkconfig --add dsmcad-node2
   ```

9. Pruebe la configuración con el mandato **`service dsmcad start`** para asegurarse de que los scripts se cargan y se inician sin problemas:

```
# service dsmcad-node1 start
Starting dsmcad-node1:                                     [  OK  ]
# service dsmcad-node2 start
Starting dsmcad-node2:                                     [  OK  ]
# ps -ef | grep dsmcad
root 2689 1 0 09:04 ? 00:00:00 /opt/tivoli/tsm/client/ba/bin/dsmcad
-optfile=/opt/tivoli/tsm/client/ba/bin/dsm-node1.opt
root 2719 1 0 09:04 ? 00:00:00 /opt/tivoli/tsm/client/ba/bin/dsmcad
-optfile=/opt/tivoli/tsm/client/ba/bin/dsm-node2.opt
```

El texto del mandato se coloca en dos líneas en este ejemplo para acomodarlo al formato de la página.

10. Reinicie y confirme que las dos instancias de dsmcad se han iniciado automáticamente:

```
# ps -ef | grep dsmcad
root 1830 1 0 09:14 ? 00:00:00 /opt/tivoli/tsm/client/ba/bin/dsmcad
-optfile=/opt/tivoli/tsm/client/ba/bin/dsm-node1.opt
root 1856 1 0 09:14 ? 00:00:00 /opt/tivoli/tsm/client/ba/bin/dsmcad
-optfile=/opt/tivoli/tsm/client/ba/bin/dsm-node2.opt
```

El texto del mandato se coloca en dos líneas en este ejemplo para acomodarlo al formato de la página.

Modificación del archivo de configuración de VMCLI

El archivo de configuración de VMCLI (`vmcliConfiguration.xml`) contiene valores para el Interfaz gráfica de usuario de Data Protection for VMware vSphere.

El proceso de instalación de Data Protection for VMware necesita que un usuario especifique una dirección IP de servidor vCenter o vCloud y si se debe habilitar el acceso a la GUI mediante un navegador web. Sin embargo, después de la instalación, el instalador no puede modificar la dirección IP de servidor y el método de acceso a GUI.

Para actualizar estos valores, puede editar manualmente el archivo de configuración de VMCLI (`vmcliConfiguration.xml`). Este archivo se crea durante la instalación en las siguientes ubicaciones:
En sistemas Windows:
`C:\IBM\tivoli\tsm\tdpvmware\webserver\usr\servers\veProfile\tsmVmGUI`
En sistemas Linux:
`/opt/tivoli/tsm/tdpvmware/common/webserver/usr/servers/veProfile/tsmVmGUI/`

Para modificar si se debe habilitar el acceso a la GUI mediante un navegador web, entre uno de los valores siguientes en el parámetro **<enable_direct_start></enable_direct_start>**:

- *yes* Se puede acceder directamente a la GUI mediante un navegador web. Por ejemplo:

```
<enable_direct_start>yes</enable_direct_start>
```

- *no* No se puede acceder directamente a la GUI mediante un navegador web. Por ejemplo:

```
<enable_direct_start>no</enable_direct_start>
```

Para utilizar la protección de GUI for vSphere, especifique el valor siguiente en el parámetro **<mode></mode>**:

- *vcenter* Se utiliza la GUI para la protección de vSphere. Por ejemplo:

```
<mode>vcenter</mode>
```

Para modificar la dirección IP de servidor vCenter, asegúrese de que se ha establecido **<mode>vcenter</mode>** y, a continuación, especifique la dirección IP en el parámetro **<vcenter_url></vcenter_url>**. Por ejemplo:

```
<vcenter_url>https://vcenter.myco.com/sdk</vcenter_url>
```

Es necesario que el valor `https://` esté al principio de la dirección IP de servidor vCenter. Es necesario que el valor `/sdk` esté al final de la dirección IP de servidor vCenter.

Archivos de ejemplo `vmcliConfiguration.xml`

El archivo `vmcliConfiguration.xml` siguiente se ha configurado para la protección de vSphere y el acceso de navegador web se ha habilitado para la GUI:

```
<?xml version="1.0" encoding="UTF-8"?>
<vmcliAdaptor>
 <VMCLIPath>C:\Archivos de programa (x86)\Common Files\Tivoli\TDPVMware\
VMwarePlugin\scripts\
</VMCLIPath>
 <interruptDelay>900000</interruptDelay>
 <mode>vcenter</mode>
 <vcenter_url>https://vcenter.myco.com/sdk</vcenter_url>
 <enable_direct_start>yes</enable_direct_start>
</vmcliAdaptor>
```

Apéndice B. Migración a una estrategia de copia de seguridad incremental constante

Utilice este procedimiento para migrar planificaciones de copia de seguridad, políticas ynodo de nodo de transportador de datoss existentes para su uso en una estrategia de copia de seguridad incremental para siempre.

Antes de empezar

Puede utilizar la estrategia de copia de seguridad completa constante que se ha implementado en Data Protection for VMware versión 6.2 y 6.3. Si desea continuar utilizando la estrategia de copia de seguridad completa constante, no es necesario que cambie su política o planificaciones. Debe asegurarse de que sólo actualiza los nodos transportadores de datos a la versión 6.4 (o posterior), como se documenta en el procedimiento siguiente. No obstante, si desea utilizar la estrategia de copia de seguridad incremental constante, además de actualizar los nodos transportadores de datos a la versión 6.4 (o posterior), también debe actualizar las planificaciones y la política para esos nodos transportadores de datos que se transfieren a esta estrategia de copia de seguridad incremental constante.

Para migrar planificaciones existentes de Data Protection for VMware a una estrategia de copia de seguridad incremental constante, debe completar las tareas incluidas en este procedimiento.

Importante:

- Aunque algunas tareas son discretas, se deben actualizar todas las aplicaciones y componentes para beneficiarse totalmente de la estrategia incremental constante. Esta publicación proporciona toda la información necesaria para guiarle a través de cada tarea.
- Existen diversos métodos disponibles para completar todo el proceso de migración. No obstante, los métodos documentados en esta publicación se consideran eficaces para entornos deData Protection for VMware típicos.
- La planificación migrar en este procedimiento es una planificación creada con el asistente de configuración de Interfaz gráfica de usuario de Data Protection for VMware vSphere. Si la planificación que se va a migrar se ha creado de manera manual, las actualizaciones de la planificación identificadas en este procedimiento también deben hacerse manualmente.

Acerca de esta tarea

Procedimiento

1. Actualice todos los servidores de seguridad vStorage que protegen un vCenter. Asegúrese de que esta actualización se completa a la vez para todos los nodos transportadores de datos.
   - Esta actualización necesita que se instale la versión 6.4 (o posterior) del Transportador de datos de IBM Spectrum Protect en el Servidor de seguridad vStorage.
   - Como tarea discreta, no es necesario completar el Paso 2 o el Paso 3 inmediatamente después del paso 1. Tras actualizar los nodos

transportadores de datos, puede continuar realizando copias de seguridad de sus máquinas virtuales en su entorno existente. Puede completar el Paso 2 y Paso 3 cuando más le convenga.

Consejo: Si su entorno utiliza varios servidores de seguridad vStorage, considere la actualización de solo uno de los servidores. A continuación, compruebe si su servidor opera correctamente antes de actualizar el resto de servidores de seguridad vStorage.

2. Actualice la política y planificaciones de copia de seguridad para implementar copias de seguridad incrementales constantes:
   Complete las siguientes tareas de política de copia de seguridad en el servidor de IBM Spectrum Protect emitiendo los comandos en el cliente de línea de comandos administrativos (`dsmadmc`):
   a. Cree una clase de gestión para el dominio y conjunto de políticas adecuado para sus copias de seguridad incrementales constantes. Este ejemplo crear la clase de gestión `mgmt_ifincr28` para el dominio `domain1` y el conjunto de políticas `prodbackups`. El nombre de la clase de gestión se utiliza para describir una estrategia de copia de seguridad incremental constante que retiene 28 versiones de copias de seguridad:

      ```
      define mgmtclass domain1 prodbackups mgmt_ifincr28
      description="Retain 28 backup versions"
      ```

   b. Cree un grupo de copias de seguridad para sus copias de seguridad incrementales constantes. Este ejemplo crea un grupo de copias de seguridad estándar para el dominio `domain1`, el conjunto de políticas `prodbackups` y la clase de gestión `mgmt_ifincr28`:

      ```
      define copygroup domain1 prodbackups mgmt_ifincr28 standard type=backup
      ```

      Las entradas `standard type=backup` son valores predeterminados, por lo que no es necesario especificarlas. Se incluyen en este ejemplo para mostrar que el nombre del grupo de copias es `STANDARD` y el tipo de grupo de copias es `backup` (en vez de `archive`).

   c. Actualice el grupo de copias de seguridad con los valores de versión, retención y caducidad adecuados:

      Recuerde: En Data Protection for VMware versión 6.2 y 6.3, la versión de copia de seguridad, la retención y la caducidad se basan en un nivel de granularidad de cadena de copia de seguridad. Este método significa que aunque se realicen copias de seguridad completas e incrementales constantes (como parte de la estrategia de copia de seguridad completa constante 6.2 y 6.3), la caducidad de versión sólo cuenta copias de seguridad completas. En Data Protection for VMware versión 6.4 (o posterior), la versión de copia de seguridad, la retención y la caducidad se basan en un nivel de granularidad de una sola copia de seguridad. Es decir, se tiene en cuenta la caducidad de la versión tanto de copias de seguridad incrementales completas constantes como incrementales constantes.

      El parámetro `verexists` especifica el número máximo de versiones de copia de seguridad de máquina virtual que se retienen en el servidor. Si una operación de copia de seguridad incremental constante hace que se supere este número, el servidor hace caducar la versión de copia de seguridad más antigua del almacenamiento del servidor. Este ejemplo especifica `verexists=28`. Este valor indica que en el servidor se retienen un máximo de 28 versiones de copia de seguridad de máquina virtual.

      El parámetro `retextra` especifica el número de días que se retiene una versión de copia de seguridad de máquina virtual una vez que la versión

pasa a estar inactiva. Este ejemplo especifica `retextra=nolimit`. Este valor indica que el número máximo de versiones de copia de seguridad de máquina virtual inactivas se retiene de manera indefinida. No obstante, cuando se especifica `verexists`, el valor `nolimit` se reemplaza por el valor `verexists`. Como resultado, en este ejemplo se retienen en el servidor un máximo de 28 versiones de copia de seguridad de máquina virtual inactivas.

De acuerdo con los valores descritos en este paso, el grupo de copias de seguridad se actualiza del siguiente modo:

```
update copygroup domain1 prodbackups mgmt_ifincr28 verexists=28
retextra=nolimit
```

En este ejemplo, el entorno de Data Protection for VMware versión 6.3 existente está formado por los siguientes hosts y planificaciones:

- Un clúster ESX (`esxcluster`) que contiene dos hosts ESX (`esxhost1`, `esxhost2`).
- La planificación `bup_esxcluster_full` ejecuta una copia de seguridad completa constante semanal de cada host ESX con el nodo de transportador de datos `dm1`.
- La planificación `bup_esxcluster_incr` ejecuta una copia de seguridad incremental constante diaria de cada host ESX con el nodo de transportador de datos `dm2`.

Complete las siguientes tareas de planificación de copia de seguridad en Interfaz gráfica de usuario de Data Protection for VMware vSphere:

a. Inicie el Interfaz gráfica de usuario de Data Protection for VMware vSphere pulsando el icono de la ventana Soluciones y aplicaciones del cliente de vSphere.
b. En la ventana Cómo empezar, pulse la pestaña **Copia de seguridad** para abrir la ventanaGestión de planificaciones de copia de seguridad.
c. Ubique la planificación de copia de seguridad (utilizada para copias de seguridad completas constantes o incrementales) que desea actualizar. En este procedimiento, se utiliza la planificación `bup_esxcluster_full` completa constante.
d. Pulse con el botón derecho la planificación y seleccione **Propiedades**.
e. Vaya a la página Planificación y especifique **Incremental** en la lista desplegable **Estrategia de copia de seguridad**.
f. Pulse **Aceptar** para guardar la actualización.
g. Ubique la planificación de copia de seguridad utilizada para las copias de seguridad incrementales constantes. Pulse con el botón derecho la planificación y seleccione **Suprimir**. Dado que la planificación `bup_esxcluster_full` completa incremental constante se ha actualizado a incremental constante, esta planificación incremental constante ya no es necesaria.

3. Ahora que tiene una planificación de copia de seguridad incremental constante, puede reducir el número de nodos transportadores de datos mediante su consolidación:
   Este ejemplo consolida dos nodos transportadores de datos en uno solo.
   a. En el servidor de seguridad vStorage, abra un indicador de comandos y vaya al directorio en el que se ubica el archivo de opciones para`dm1`.
   b. Mediante un editor de texto (como Notepad), actualice este archivo con las siguientes opciones:

1) Especifique `vmmaxparallel` para controlar el número de máquinas virtuales copiadas a la vez por `dm1`:

   ```
   vmmaxparallel=2
   ```

   El valor predeterminado y valor mínimo es 1. El valor máximo es 50.

   Consejo: Por cada nodo transportador de datos que elimine, aumente el valor de `vmmaxparallel` en 1.

   De forma alternativa, puede especificar `vmlimitperhost` para controlar el número de máquinas virtuales copiadas a la vez por `dm1` desde el host ESX:

   ```
   vmlimitperhost=1
   ```

   Esta opción es útil si desea evitar la sobrecarga de un host. El valor por omisión es 0 (sin límite). El valor mínimo es 1. El valor máximo es 50.

c. Inicie sesión en el servidor de IBM Spectrum Protect. Utilice el cliente de línea de comandos administrativo (`dsmadmc`) para especificar el número máximo de sesiones de copia de seguridad de máquina virtual simultáneas que se pueden conectar al servidor. Por ejemplo:

   ```
   maxsessions=4
   ```

   El valor predeterminado es 25. El valor mínimo es 2.

4. Compruebe si los nodos transportadores de datos actualizados funcionan correctamente:
   a. Inicie el Interfaz gráfica de usuario de Data Protection for VMware vSphere pulsando el icono de la ventana Soluciones y aplicaciones del cliente de vSphere.
   b. En la ventana Cómo empezar, pulse la pestaña Configuración para abrir la página Estado de configuración.
   c. En la página Estado de configuración, seleccione el vCenter protegido en el Paso 1. Pulse un nodo transportador de datos para ver su información es estado en el panel Detalles de estado. Si un nodo muestra un aviso o un error, pulse en ese nodo y utilice la información del panel Detalles del estado para resolver el problema. Luego seleccione el nodo y pulse en **Validar nodo seleccionado** para verificar si se ha resuelto el problema. Pulse Renovar para volver a comprobar todos los nodos.

Resultados

Tras finalizar correctamente esta tarea, el entorno está listo para su uso en una estrategia de copia de seguridad incremental constante.

Restricciones: Tras migrar planificaciones de tipos de copia de seguridad completa constantes a tipos de copia de seguridad incrementales constantes, tenga en cuenta las siguientes restricciones:

- El cambio de planificaciones migradas a tipos de copia de seguridad completa constante de nuevo por máquina virtual (espacio de archivos) no se soporta.
- No se puede utilizar una versión anterior del transportador de datos de IBM Spectrum Protect en un espacio de archivos migrado.
- Cuando un espacio de archivos contiene una (o varias) copias de seguridad incrementales constantes, no se soportan copias de seguridad completas constantes.

Ejemplo de control de versión con el parámetro `verexists`

En este ejemplo de migración de planificación, Data Protection for VMware versión 6.3 utiliza las dos planificaciones de copia de seguridad siguientes:

- `-mode=full`: Se planifica una copia de seguridad completa constante semanal (domingos) y el número máximo de versiones de copia de seguridad de máquinas virtuales que se retienen en el servidor es cuatro (`verexists=4`).
- `-mode=incr`: Se planifica una copia de seguridad incremental constante entre semana (lunes a sábado).

El número de copias de seguridad realizadas durante un periodo de cuatro semanas es de 28:

- Cuatro copias de seguridad completas constantes (una copia completa semanal multiplicada por cuatro semanas)
- 24 copias de seguridad incrementales constantes (seis copias incrementales entre semana multiplicadas por cuatro semanas)

Dado que Data Protection for VMware versión 6.3 solo cuenta las copias de seguridad completas, el valor `verexists=4` recoge las 28 copias de seguridad.

Para proporcionar el mismo nivel de protección con Data Protection for VMware versión 6.4 (o posterior) y la estrategia de copia de seguridad incremental constante, cree la planificación siguiente:
`-mode=iffull`: Se planifica una copia de seguridad completa constante diaria y el parámetro `verexists` se define en 28.
El número de copias de seguridad realizadas durante un periodo de cuatro semanas es de 28:

- Una copia de seguridad completa constante (copia inicial multiplicada por un día)
- 27 copias incrementales constantes (copias incrementales para siempre diarias multiplicadas por 27 días)

Dado que Data Protection for VMware versión 6.4 (o posterior) cuenta las copias de seguridad completas constantes e incrementales constantes, el valor `verexists=28` conserva las 28 copias de seguridad.

Apéndice C. 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.

Software de otros proveedores

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.

IBM puede no ofrecer los productos, servicios o funcionalidades tratados en este documento en otros países. Póngase en contacto con su representante local de IBM para obtener más información sobre los productos y servicios que actualmente están disponibles en su país. Las referencias a programas, productos o servicios de IBM no pretenden establecer ni implicar que sólo puedan utilizarse dichos productos, programas o servicios de IBM. En su lugar, se puede utilizar cualquier producto, programa o servicio funcionalmente equivalente que no infrinja ninguno de 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 de aprobación que cubran alguno de los temas tratados en este documento. El presente documento no le confiere ningún derecho sobre estas patentes. Si lo desea, puede realizar consultas sobre licencias, por escrito, dirigiéndose a:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
EE.UU.

Si desea realizar consultas acerca de la información de juegos de caracteres de doble byte (DBCS), puede ponerse en contacto con el Departamento de Propiedad Intelectual de IBM de su país o bien enviar las consultas por escrito a:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokio 103-8510, Japón

INTERNATIONAL BUSINESS MACHINES CORPORATION PROPORCIONA ESTA PUBLICACIÓN "TAL CUAL" SIN GARANTÍA DE NINGUNA CLASE, NI 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 puede contener imprecisiones técnicas o errores tipográficos. Periódicamente se efectúan cambios en la información aquí contenida; estos cambios se incorporarán en nuevas ediciones de la publicación. IBM puede realizar mejoras y/o cambios en los productos o programas descritos en esta publicación 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 suministrada por los usuarios del modo en que considere oportuno, sin incurrir por ello en ninguna obligación para con ellos.

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 bajo licencia que se describe en este documento y todo el material bajo licencia disponible los proporciona IBM bajo los términos de las Condiciones Generales de IBM, Acuerdo Internacional de Programas Bajo Licencia de IBM o cualquier acuerdo equivalente entre las 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 comerciales cotidianas. Para ilustrarlos de la forma más completa posible, se han utilizado nombres de personas, empresas, marcas y productos. Todos estos nombres son ficticios y cualquier parecido con nombres y direcciones de una empresa real es pura coincidencia.

LICENCIA DE COPYRIGHT:

Esta información contiene programas de aplicación de ejemplo en código fuente, que ilustran técnicas de programación en diferentes plataformas operativas. Puede copiar, modificar y distribuir estos programas de ejemplo de cualquier manera sin realizar pago alguno a IBM, con el fin de desarrollar, utilizar, comercializar o distribuir programas de aplicación en conformidad con la interfaz de programación de aplicaciones para la plataforma operativa para los que se han escrito los programas de ejemplo. Estos ejemplos no se han probado exhaustivamente bajo todas las condiciones. Por consiguiente, IBM no puede garantizar o dar por implícita la fiabilidad, la capacidad de servicio o la función de estos programas.

Los programas de ejemplo se proporcionan "TAL CUAL" y sin garantía de ninguna clase. IBM no será responsable de ningún daño producido por el uso de los programas de ejemplo.

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 y ibm.com son marcas registradas de International Business Machines Corp., que se encuentran registradas en un gran número de jurisdicciones en todo el mundo. Otros nombres de productos o servicios pueden ser marcas registradas de IBM o de otras empresas. 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 comercial 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 Estados Unidos y en otros países.

Intel e Itanium son marcas registradas de Intel Corporation o sus filiales en Estados Unidos y/o en otros países.

Linux es una marca registrada de Linus Torvalds en Estados Unidos o en otros países.

Microsoft, Windows y Windows NT son marcas registradas de Microsoft Corporation en Estados Unidos y/o en otros países.

Java y todas las marcas registradas y 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 de la documentación del producto

Los permisos para la utilización de estas publicaciones se otorgan sujetos a los siguientes términos y condiciones.

Validez

Estos términos y condiciones completan los términos y condiciones de uso del sitio web de IBM.

Uso personal

Puede reproducir estas publicaciones para su uso personal, no comercial, siempre y cuando se conserven todos los avisos de propiedad. No puede distribuir ni exponer estas publicaciones ni ninguna de sus partes, como tampoco elaborar trabajos que se deriven de ellas, sin el consentimiento explícito de IBM.

Uso comercial

Puede reproducir, distribuir y mostrar estas publicaciones únicamente dentro de su empresa, siempre que se conserven todos los avisos sobre derechos de propiedad. No podrá crear trabajo derivado de estas publicaciones, ni reproducir, distribuir ni visualizar estas publicaciones o cualquier parte de éstas sin el consentimiento expreso de IBM.

Derechos

Si no se indica lo contrario en este permiso, no se otorgan otros permisos, licencias o derechos, ya sea de forma expresa o implícita, a las publicaciones u otra información, datos, software u otra propiedad intelectual que contenga este documento.

IBM se reserva el derecho de retirar las autorizaciones otorgadas por el presente documento siempre que, a su juicio, el uso de las publicaciones perjudique sus intereses o, según lo determinado por IBM, no se estén siguiendo correctamente las instrucciones indicadas anteriormente.

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 EFECTÚA NINGÚN TIPO DE GARANTÍA SOBRE EL CONTENIDO DE ESTAS PUBLICACIONES. LAS PUBLICACIONES SE SUMINISTRAN "TAL CUAL", SIN GARANTÍAS DE NINGÚN TIPO, NI EXPLÍCITAS NI IMPLÍCITAS, INCLUIDAS 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, incluido el software como soluciones de servicio, (“Ofertas de software”) podrían utilizar cookies u otras tecnologías para recopilar información del uso del producto para ayudar a mejorar la experiencia del usuario final, para adaptar las interacciones con el usuario final o para otros fines. En muchos casos, las Ofertas de software no recopilan información de identificación personal. Algunas de nuestras ofertas de software pueden ayudarle a recopilar información de identificación personal. Si esta oferta de software utiliza cookies para recopilar información de identificación personal, la información específica sobre la utilización de cookies de esta oferta se expone más adelante.

Esta oferta de software no utiliza cookies u otras tecnologías para recopilar información de identificación personal.

Si las configuraciones desplegadas para esta Oferta de software le ofrecen como cliente la posibilidad de recopilar información de identificación personal de los usuarios finales mediante cookies y otras tecnologías, debe buscar asesoramiento legal sobre las leyes aplicables a dicha recopilación de datos, incluidos los requisitos de aviso y consentimiento.

Para obtener más información sobre el uso de las distintas tecnologías, incluidas las cookies, para estos fines, consulte la Política de privacidad de IBM en http://www.ibm.com/privacy y la 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

Hay un glosario disponible 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 IBM, consulte Terminología de IBM.

Índice

A

acceso al almacén de claves
  certificado de terceros 56
actualización
  desde V6.x
    estándar 33
  Linux
    silenciosa 35
  visión general 32
  Windows de 64 bits
    silenciosa 34
actualización silenciosa
  Linux 35
  Windows de 64 bits 34
agente de recuperación 6
almacenamiento en cinta
  configurar 96
archivo de configuración de VMCLI
  modificar 110
  vmcliConfiguration.xml 110
asistente de configuración 41
asistente de instalación
  Linux
    utilizar el asistente de instalación 22
  Windows
    utilizar el asistente de instalación 21
autorización
  permisos 12

C

características de accesibilidad 119
certificado de terceros
  acceso al almacén de claves 56
  configurar TLS 56
  crear una solicitud de firma de certificado 58
  enviar la solicitud de firma de certificado 59
  recibir el certificado firmado 59
clave de registro 19, 68
Client Acceptor
  configurar 108
componentes 1
  agente de recuperación 6
  componentes instalables 19
  Extensión de IBM Spectrum Protect 7
  GUI de Restauración de archivo 8
  Interfaz de línea de mandatos de Data Protection for VMware 7
  Interfaz gráfica de usuario de Data Protection for VMware vSphere 3
  transportador de datos 8
componentes instalables 1
  agente de recuperación 6
  Extensión de IBM Spectrum Protect 7
  GUI de Restauración de archivo 8
  Interfaz de línea de mandatos de Data Protection for VMware 7
  Interfaz gráfica de usuario de Data Protection for VMware vSphere 3
  transportador de datos 8
comunicación TLS
  configurar 56
configurar
  almacenamiento en cinta 96
  archivo de configuración de VMCLI 110
  Client Acceptor 108
  comunicación de navegador web 56
  comunicación TLS 56
  configuración existente 42
  configuración inicial 41
  entorno de vSphere
    lista de comprobación de línea de mandatos 93
  habilitar la restauración de archivos 43
  habilitar soporte de descodificación 49
  hoja de trabajo para Data Protection for VMware 31
  interfaz gráfica de usuario de agente de recuperación 69
  montaje de iSCSI 99, 101
  Nodos de IBM Spectrum Protect
    entorno de vSphere 84
  nodos de proxy de montaje
    Linux 103
    Windows 106
  nodos transportadores de datos
    entorno de vSphere 85
  restauración de archivos
    opciones 46
  SSL 56
  tareas avanzadas 83
  valores de entorno local 78
  visión general 41
  VMCLI
    entorno de vSphere 91
configurar TLS
  certificado de terceros 56
  entidad emisora de certificados 56
  habilitar comunicación segura con el servidor 60, 74, 75, 76
crear una solicitud de firma de certificado
  certificado de terceros 58
credenciales
  permisos 12
cuaderno de configuración 42

D

Data Protection for VMware
  componentes instalables 1
  descargar el paquete 20
  planificar 9
Desinstalación
  Linux
    modalidad silenciosa 39
    típica 36
  Windows de 64 bits
    modalidad silenciosa 38
    típica 36
desinstalación silenciosa
  Linux
    modalidad silenciosa 39
  Windows de 64 bits
    modalidad silenciosa 38

discapacidad 119

E

entorno local
  valores 78
enviar la solicitud de firma de certificado
  certificado de terceros 59
Extensión de IBM Spectrum Protect 7

G

GUI
  Interfaz gráfica de usuario de Data Protection for VMware vSphere 32
GUI de Restauración de archivo 8
GUI de vSphere 32

H

habilitar comunicación segura con el servidor
  configurar TLS 60, 74, 75, 76

I

IBM Knowledge Center v
instalación
  componentes 19
  componentes instalables 1
  Data Protection for VMware 1
  descargar el paquete 20
  hoja de ruta 9
  Linux
    utilizar el asistente de instalación 22
  obtener el paquete 20
  permisos de usuario 12
  puertos de comunicación necesarios 13
  requisitos de hardware 11
  requisitos de software 11
  requisitos del sistema 11
  Windows
    utilizar el asistente de instalación 21
instalación silenciosa
  Linux 28
  Windows de 64 bits
    instalador silencioso de Suite 24
Interfaz de línea de mandatos de Data Protection for VMware 7
interfaz gráfica de usuario de agente de recuperación
  configurar 69
  opciones 69
Interfaz gráfica de usuario de Data Protection for VMware vSphere 3, 32
  permisos
    operaciones 65

K

Knowledge Center v

L

Linux
  actualización
    silenciosa 35
  Desinstalación
    modalidad silenciosa 39
    típica 36
  procedimiento de instalación
    limpia 23
    silenciosa 28

M

migración
  planificaciones 113
montaje de iSCSI
  configurar 99, 101

N

Nodos de IBM Spectrum Protect
  configurar
    entorno de vSphere 84
Novedades en Data Protection for VMware versión 7.1.6 vii

P

permisos
  instalación 12
  Interfaz gráfica de usuario de Data Protection for VMware vSphere
    operaciones 65
planificación
  hoja de ruta 9
  requisitos del sistema 11
planificar
  permisos 12
  puertos de comunicación necesarios 13
  visión general 9
privilegio de administrador
  Interfaz gráfica de usuario de Data Protection for VMware vSphere 65
procedimiento de instalación
  Linux
    limpia 23
    silenciosa 28
  Windows de 64 bits
    instalador silencioso de Suite 24
publicaciones v
puertos
  instalación 13
puertos de comunicación
  instalación 13

R

recibir el certificado firmado
  certificado de terceros 59
registro
  restauración de archivos 47
requisitos de hardware 11
requisitos de software 11
requisitos del sistema 11
restauración
  archivo 46, 47

restauración *(continuación)*
configuración de opciones 46
configurar registro 47
opciones 46
restauración de archivos
configuración de opciones 46
configurar registro 47
entorno de Linux 44
habilitar 43
opciones 46, 48
restaurar
agente de recuperación 6
archivo 48
opciones 48

S

servicios 81
soporte de etiquetado
habilitar 49
SSL
configurar 56, 60, 74, 75, 76

T

teclado 119
transportador de datos 8
nodos
configurar en entorno de vSphere 85

U

usuario
permisos 12

V

VMCLI
configurar en entorno de vSphere 91

W

Windows de 64 bits
actualización
silenciosa 34
Desinstalación
modalidad silenciosa 38
típica 36
procedimiento de instalación
instalador silencioso de Suite 24

Número de Programa: 5725-X00

Impreso en España