Dell EMC PowerStore

Guía de configuración de seguridad

1.x

July 2020
Rev. A02

Notas, precauciones y advertencias

NOTA: Una NOTA indica información importante que le ayuda a hacer un mejor uso de su producto.

PRECAUCIÓN: Una ADVERTENCIA indica un potencial daño al hardware o pérdida de datos y le informa cómo evitar el problema.

AVISO: Una señal de PRECAUCIÓN indica la posibilidad de sufrir daño a la propiedad, heridas personales o la muerte.

Tabla de contenido

Prefacio

Como parte de un esfuerzo por mejorar, se lanzan periódicamente revisiones de software y hardware. Algunas funciones que se describen en este documento no son compatibles con todas las versiones del software o el hardware actualmente en uso. Las notas de la versión del producto proporcionan la información más actualizada acerca de las características del producto. En caso de que un producto no funcione correctamente o no funcione según se describe en este documento, póngase en contacto con un profesional de soporte técnico de .

Dónde obtener ayuda

La información sobre soporte, productos y licenciamiento puede obtenerse de la siguiente manera:

- **Información de productos**

  Para obtener documentación o notas de la versión de productos y funciones, vaya a la página PowerStore Documentation en www.dell.com/powerstoredocs.

- **Solución de problemas**

  Para obtener información sobre productos, actualizaciones de software, licenciamiento y servicio, vaya a www.dell.com/support y busque la página de soporte del producto correspondiente.

- **Soporte técnico**

  Para obtener soporte técnico y realizar solicitudes de servicio, vaya a www.dell.com/support y busque la página **Service Requests**. Para abrir una solicitud de servicio, debe contar con un acuerdo de soporte técnico válido. Póngase en contacto con el representante de ventas para recibir información sobre cómo obtener un acuerdo de soporte técnico válido o para aclarar cualquier tipo de duda en relación con su cuenta.

1

Autenticación y acceso

Este capítulo contiene la siguiente información:

Temas:

Autenticación y administración de cuentas de usuario, funciones y privilegios

La autenticación para acceder al clúster se realiza en función de las credenciales de una cuenta de usuario. Las cuentas de usuario se crean y se administran posteriormente desde la página **Users**, a la que se accede en PowerStore Manager a través de **Settings** > **Users** > **Users**. Las autorizaciones que se aplican dependen de la función asociada con la cuenta de usuario. Cuando el usuario especifica la dirección de red del clúster como la URL en un navegador web, se le muestra una página de inicio de sesión desde la cual puede autenticarse como un usuario local. Las credenciales que el usuario proporciona se autentican y se crea una sesión en el sistema. Posteriormente, el usuario puede monitorear y administrar el clúster dentro de las funcionalidades de la función que tiene asignada.

El clúster autentica a sus usuarios mediante la validación de los nombres de usuario y las contraseñas a través de una conexión segura con el servidor de administración.

Administración predeterminada de fábrica

El dispositivo viene con ajustes de cuenta de usuario predeterminados de fábrica que se usan cuando se accede a él y se configura inicialmente.

NOTA: Con las versiones 1.0.x, se recomienda configurar PowerStore inicialmente mediante la interfaz de usuario de PowerStore Manager en lugar de utilizar las interfaces de API, CLI o scripts de servicio. Esto garantizará el cambio de todas las contraseñas predeterminadas.

Tipo de cuenta	Nombre de usuario	Contraseña	Privilegios
Administración de sistemas	admin	Password123#	Privilegios de administrador para restablecer las contraseñas predeterminadas, configurar los ajustes del dispositivo y administrar cuentas de usuario.
Servicio	Servicio	Servicio	Para realizar operaciones de servicio. **NOTA:** El usuario de servicio existe para el acceso de Secure Shell (SSH). Sin embargo, no

Tipo de cuenta	Nombre de usuario	Contraseña	Privilegios
			puede iniciar sesión en PowerStore Manager con el usuario de servicio.

Reglas de las sesiones

Las sesiones en el clúster tienen las siguientes características:

- El plazo de vencimiento es de una hora.

  NOTA: La sesión del usuario en el clúster se cierra automáticamente después de una inactividad de una hora.
- El tiempo de espera de sesión no es configurable.

Uso de nombres de usuario y contraseñas

Los nombres de usuario de la cuenta del sistema deben cumplir con los siguientes requisitos:

Restricción	Requisito de nombre de usuario
Estructura	Debe comenzar y terminar con un carácter alfanumérico.
Caso	Los nombres de usuario no distinguen mayúsculas de minúsculas
Cantidad mínima de caracteres alfanuméricos	1
Cantidad máxima de caracteres alfanuméricos	64
Caracteres especiales compatibles	. (punto)

Las contraseñas de la cuenta del sistema deben cumplir con los siguientes requisitos:

Restricción	Requisitos de la contraseña
Cantidad mínima de caracteres	8
Cantidad mínima de caracteres en mayúsculas	1
Cantidad mínima de caracteres en minúsculas	1
Cantidad mínima de caracteres numéricos	1
Cantidad mínima de caracteres especiales • Caracteres compatibles: ! @ # $ % ^ * _ ~ ? **NOTA:** La contraseña no puede incluir comillas simples ('), y comercial (&) ni caracteres de espacio.	1
Cantidad máxima de caracteres	40

NOTA: Las últimas cinco contraseñas no se pueden volver a utilizar. Una contraseña anterior se puede reutilizar después de la quinta vez en secuencia.

Contraseñas de ESXi

La contraseña raíz predeterminada para ESXi en un dispositivo PowerStore X model se encuentra en el siguiente formato: **<*Service_Tag*>_123!**, donde <*Service_Tag*> es la etiqueta de servicio Dell de siete caracteres para el dispositivo.

No cambie la contraseña predeterminada de ESXi hasta que finalice la configuración inicial del clúster. Para obtener más información sobre cómo cambiar una contraseña de ESXi, consulte la documentación de VMware ESXi.

PRECAUCIÓN: Es fundamental que no pierda la contraseña de ESXi. Si ESXi queda inactivo y usted no dispone de la contraseña, el dispositivo se debe reinicializar. Este comportamiento es normal para ESXi; sin embargo, la reinicialización debido a una contraseña perdida puede provocar la pérdida de datos.

PRECAUCIÓN: La contraseña predeterminada de ESXi está configurada de manera exclusiva para cada dispositivo PowerStore X model. La contraseña se utiliza para autenticarse en el host ESXi cuando se agregan los nodos del dispositivo a un clúster de vCenter. Si cambia la contraseña predeterminada antes de que el clúster esté configurado por completo, tendrá que reinicializar el dispositivo.

Funciones y privilegios

Los controles de acceso basado en funciones permiten que los usuarios tengan distintos privilegios. Esto proporciona un medio para segregar las funciones de administración a fin de alinearlas mejor con los conjuntos de habilidades y las responsabilidades.

El sistema admite las siguientes funciones y privilegios:

NOTA: Una marca ✓ en una casilla denota un privilegio admitido para esa función, mientras que una casilla en blanco indica que el privilegio no se admite.

Tarea	Operador	Administrador de VM	Administrador de seguridad	Administrador de almacenamiento	Administrador
Cambiar la contraseña local del sistema	✓	✓	✓	✓	✓
Ver la información de ajustes, estado y rendimiento del sistema	✓		✓	✓	✓
Modificar la configuración del sistema					✓
Crear, modificar, eliminar recursos y políticas de protección, y habilitar/deshabilitar SSH				✓	✓
Conectarse a vCenter		✓		✓	✓
Ver una lista de cuentas locales			✓		✓
Agregar, eliminar o modificar una cuenta local			✓		✓
Ver información del almacenamiento del sistema a través de una instancia de vCenter Server que está conectada al proveedor de VASA del sistema y registrar o volver a registrar el certificado de autoridad de certificación de VMware (VMCA)/CA		✓			✓

Funciones y privilegios relacionados con archivos

El sistema admite las siguientes funciones y privilegios relacionados con archivos:

NOTA: Una marca ✓ en una casilla denota un privilegio admitido para esa función, mientras que una casilla en blanco indica que el privilegio no se admite.

Tarea	Operador	Administrador de VM	Administrador de seguridad	Administrador de almacenamiento	Administrador
Ver lo siguiente: • Alertas del sistema de archivos • Lista de servidores NAS • Lista de sistemas de archivos • Lista de cuotas de usuario de archivo • Lista de rutas de interfaces de archivo • Lista de interfaces de archivo • Lista de recursos compartidos de SMB • Lista de exportaciones de NFS	✓		✓	✓	✓
Ver lo siguiente: • Lista de servidores DNS de archivo o un servidor DNS especificado • Lista de servidores FTP de archivo o un servidor FTP especificado • Lista de interfaces de archivo o interfaz de archivo especificada • Lista de rutas de interfaces de archivo o una ruta de interfaz especificada • Lista de servidores Kerberos de archivo o un servidor Kerberos especificado • Lista de servidores LDAP de archivo o un servidor LDAP especificado • Lista de servidores NDMP de archivo o un servidor NDMP especificado • Lista de servidores NIS de archivo o un servidor NIS especificado • Lista de sistemas de archivos o un sistema de archivos especificado • Lista de cuotas de árbol de archivo o una cuota de árbol de archivo especificada • Lista de cuotas de usuario de archivo o una cuota de usuario especificada • Lista de programas antivirus de archivo o un programa antivirus de archivo especificado • Lista de servidores NAS o un servidor NAS especificado • Lista de exportaciones de NFS o una exportación de NFS especificada • Lista de servidores NFS o un servidor NFS especificado	✓		✓	✓	✓

Tarea	Operador	Administrador de VM	Administrador de seguridad	Administrador de almacenamiento	Administrador
• Lista de servidores SMB o un servidor SMB especificado • Lista de recursos compartidos de SMB o un recurso compartido de SMB especificado					
Agregar, modificar, eliminar o hacer ping a un servidor NAS especificado, o cargar contraseña, hosts o grupos a un servidor NAS especificado				✓	✓
Ver la contraseña o los hosts de un servidor NAS especificado			✓		✓
Agregar un sistema de archivos o modificar o eliminar un sistema de archivos especificado en un servidor NAS existente				✓	✓
Agregar un clon o una instantánea a un sistema de archivos especificado, actualizar o restaurar un sistema de archivos especificado, o actualizar la cuota de un sistema de archivos especificado				✓	✓
Agregar una cuota de árbol de archivo, o modificar, eliminar o actualizar una cuota de árbol de archivo especificada				✓	✓
Agregar una cuota de usuario de archivo, o modificar, eliminar o actualizar una cuota de usuario de archivo especificada				✓	✓
Agregar un programa antivirus de archivo, modificar o eliminar un programa antivirus de archivo especificado o cargar la configuración de un programa antivirus de archivo especificado					✓
Descargar la configuración de un programa antivirus de archivo especificado			✓		✓
Agregar un servidor SMB o NFS, o modificar, eliminar, unirse o desunirse de un servidor SMB o NFS especificado				✓	✓
Agregar un recurso compartido de SMB o modificar o eliminar un recurso compartido de SMB especificado				✓	✓
Agregar una exportación de NFS o modificar o eliminar una exportación de NFS especificada				✓	✓

Tarea	Operador	Administrador de VM	Administrador de seguridad	Administrador de almacenamiento	Administrador
Agregar una interfaz de archivo o modificar o eliminar una interfaz de archivo especificada				✓	✓
Agregar una ruta de interfaz de archivo o modificar o eliminar una ruta de interfaz de archivo especificada				✓	✓
Agregar un servidor DNS de archivo, FTP de archivo, Kerberos de archivo, LDAP de archivo, NDMP de archivo o NIS de archivo, o modificar o eliminar un servidor DNS de archivo, FTP de archivo, Kerberos de archivo, LDAP de archivo, NDMP de archivo o NIS de archivo especificado				✓	✓
Cargar un keytab de Kerberos de archivo					✓
Descargar un keytab de Kerberos de archivo	✓		✓		✓
Cargar una configuración de LDAP o un certificado de LDAP de archivo					✓
Descargar un certificado de LDAP de archivo			✓		✓

Administración de cuentas de usuario basada en privilegios de funciones

Un usuario con una función de administrador o administrador de seguridad puede realizar lo siguiente con respecto a la administración de cuentas de usuario:

- Crear una nueva cuenta de usuario.
- Eliminar cualquier cuenta de usuario, excepto la cuenta de administrador incorporada.

  NOTA: La cuenta de administrador incorporada no se puede eliminar.
- Cambiar otro usuario a cualquier función.
- Restablecer la contraseña de otro usuario.
- Bloquear o desbloquear otra cuenta de usuario.

  NOTA: Los usuarios que iniciaron una sesión con una función de administrador o administrador de seguridad no pueden bloquear su propia cuenta.

Los usuarios que iniciaron una sesión no pueden eliminar su propia cuenta de usuario. Además, con excepción de los usuarios con la función de administrador de seguridad o administrador, los usuarios que iniciaron una sesión pueden cambiar solamente su propia contraseña. Los usuarios deben proporcionar su contraseña anterior para cambiar su contraseña. Los usuarios que iniciaron una sesión no pueden restablecer su propia contraseña, cambiar su propia función ni bloquear o desbloquear sus propias cuentas.

El perfil de cuenta de administrador incorporada (con función de administrador) no se puede editar ni bloquear.

Cuando un administrador de seguridad o un administrador cambian la función o el estado de bloqueo de un usuario, eliminan el usuario o cambian su contraseña, se invalidan todas las sesiones vinculadas a ese usuario.

NOTA: Si un usuario actualiza sus propias contraseñas dentro de la sesión, la sesión permanece activa.

Restablecer las contraseñas de las cuentas de administrador y servicio

El dispositivo se envía con una cuenta de usuario administrador predeterminada que permite realizar la configuración inicial. También se envía con una cuenta de usuario de servicio predeterminado que le permite realizar funciones de servicio especializadas. Se recomienda configurar inicialmente PowerStore mediante la interfaz de usuario de PowerStore Manager en lugar de otro método, como la API REST o la CLI. El uso de la interfaz de usuario de PowerStore Manager garantiza el cambio de todas las contraseñas predeterminadas. Si olvida las contraseñas nuevas, puede restablecerlas a sus valores predeterminados.

El método para restablecer estas contraseñas depende de si el dispositivo es un PowerStore T model o un PowerStore X model. Utilice el método que corresponda al dispositivo para restablecer las contraseñas de administrador, servicio o ambas.

Restablecer las contraseñas de las cuentas de administrador y servicio a sus valores predeterminados en un dispositivo PowerStore T model

Sobre esta tarea

En un dispositivo PowerStore T model, el método primario para restablecer las contraseñas de usuario administrador o de servicio es usar una unidad USB. Entre los sistemas de archivos compatibles se incluyen FAT32 e ISO 9660.

NOTA: Para restablecer la contraseña cuando el dispositivo se encuentra en modo de servicio, utilice los siguientes pasos con una diferencia. Aplique el proceso de restablecimiento mediante USB a cada nodo. Esta acción garantiza que, cuando el sistema regrese al modo normal y después del inicio de sesión en PowerStore Manager, se le solicitará que proporcione una nueva contraseña tanto para el usuario administrador como para el de servicio.

Pasos

1. Si la unidad USB está formateada, continúe con el paso siguiente; de lo contrario, utilice una línea de comandos como `format <d:> /FS:FAT32` para formatearla.

   Donde `d:` es la letra de la unidad USB que insertó en la laptop o la PC.

2. Configure la etiqueta con el comando:

   ```
   label d:
   RSTPWD
   ```

   NOTA: El dispositivo no montará la unidad USB sin la etiqueta `RSTPWD`. Después de etiquetar la unidad USB, inserte un archivo vacío para las contraseñas de la cuenta que desea restablecer. Puede restablecer la contraseña de la cuenta de administrador, servicio o ambas.

3. Para crear un archivo vacío en la unidad, utilice uno de los siguientes comandos, o ambos, según sea necesario:

   ```
   copy NUL d:\admin
   copy NUL d:\service
   ```

4. Inserte la unidad USB en el puerto USB de cualquiera de los nodos del dispositivo, espere 10 segundos y, a continuación, extráigala. Ahora, la contraseña de cada cuenta que restablece es el valor predeterminado.
5. Conéctese al clúster a través de un navegador mediante la dirección IP del clúster e inicie sesión como administrador con la contraseña inicial predeterminada, que es **`Password123#`**.
   Debe aparecer una solicitud de restablecimiento de las contraseñas de administrador, servicio o ambas. Si prefiere restablecer la contraseña de servicio mediante Secure Shell (SSH), la contraseña predeterminada inicial para la cuenta de servicio es **`service`**.
6. Cambie la contraseña de administrador del valor predeterminado a una contraseña especificada por el usuario.
7. Si desea configurar la contraseña de la cuenta de servicio de modo que sea diferente a la contraseña de administrador, deseleccione la casilla de verificación relacionada.

Resultados

Si aún no se le solicita restablecer la contraseña en el intento de inicio de sesión después de ejecutar este procedimiento, póngase en contacto con el proveedor de servicio.

Restablecer las contraseñas de las cuentas de administrador y servicio a sus valores predeterminados en un dispositivo PowerStore X model

Requisitos previos

Conozca el nombre del nodo primario del dispositivo primario (por ejemplo, PSTX-44W1BW2-A y PowerStore D6013). Si es necesario, genere el archivo `reset.iso`.

Sobre esta tarea

En el caso de un dispositivo PowerStore X model, utilice una imagen ISO y móntela desde vSphere. Los archivos de imagen creados previamente se pueden descargar desde www.dell.com/support. También puede crear su propia imagen desde un sistema Linux mediante uno de los siguientes comandos touch, o ambos, en función de las contraseñas que se deben restablecer:

```
mkdir iso
touch iso/admin
touch iso/service
mkisofs -V RSTPWD -o reset.iso iso
```

NOTA: La imagen ISO, `reset.iso`, debe residir en un almacén de datos antes de que se pueda montar como un CD virtual desde vSphere.

NOTA: Para restablecer la contraseña cuando el dispositivo se encuentra en modo de servicio, utilice los siguientes pasos con dos diferencias. En primer lugar, debe cargar la imagen ISO en el almacén de datos PRIVATE-C9P42W2.A.INTERNAL de la propia máquina virtual (VM) de la controladora, ya que el almacén de datos público no está disponible. En segundo lugar, cargue y aplique el archivo `reset.iso` a los nodos A y B de la VM de la controladora. Esta acción garantiza que, cuando el sistema regrese al modo normal y el acceso a PowerStore Manager esté disponible, se le solicitará que proporcione una nueva contraseña tanto para el usuario administrador como para el de servicio.

Pasos

1. En vSphere, bajo **Storage**, seleccione el dispositivo PowerStore X model.

   Por ejemplo, **DataCenter-WX-D6013** > **PowerStore D6013**

2. En **Files**, seleccione **ISOs**.
3. Seleccione **Upload** y cargue el archivo `reset.iso`, ya sea el archivo de imagen creado previamente desde www.dell.com/support o un archivo de imagen propio que usted creó en un sistema Linux.
   El archivo `reset.iso` aparece en la carpeta **ISOs**.
4. En vSphere, bajo **Host and Clusters**, seleccione el nodo primario del dispositivo PowerStore X model primario del clúster.

   Por ejemplo, **DataCenter-WX-D6013** > **Cluster WX-D6013** > **PSTX-44W1BW2-A**

5. En **Summary**, haga clic en **CD/DVD drive 1** y seleccione **Connect to datastore ISO file**.
   Aparece la ventana **Choose an ISO image to mount**.
6. En **Datastores**, haga clic en el dispositivo PowerStore X model primario del clúster y seleccione la carpeta **ISOs**.
   El archivo `reset.iso` debe aparecer bajo **Contents**.
7. Seleccione el archivo `reset.iso` y haga clic en **OK**.
   En **Summary**, **CD/DVD drive 1** debe aparecer como **Connected** durante unos 10 segundos y, a continuación, debe cambiar a **Disconnected**. La contraseña del administrador del clúster, la contraseña de servicio o ambas se restablecen ahora a su valor predeterminado.
8. Conéctese al clúster a través de un navegador mediante la dirección IP del clúster e inicie sesión como administrador con la contraseña inicial predeterminada, que es **`Password123#`**.
   Debe aparecer una solicitud de restablecimiento de las contraseñas de administrador, servicio o ambas. Si prefiere restablecer la contraseña de servicio mediante SSH, la contraseña predeterminada inicial para la cuenta de servicio es **`service`**.
9. Cambie la contraseña de administrador del valor predeterminado a una contraseña especificada por el usuario.
10. Si desea configurar la contraseña de la cuenta de servicio de modo que sea diferente a la contraseña de administrador, deseleccione la casilla de verificación relacionada.

Resultados

Si aún no se le solicita restablecer la contraseña en el intento de inicio de sesión después de ejecutar este procedimiento, póngase en contacto con el proveedor de servicio.

Certificados

Los datos en el almacén de certificados de PowerStore son persistentes. El almacén de certificados almacena los siguientes tipos de certificados:

- Certificados de autoridad de certificación (CA)
- Certificados de cliente
- Certificados de servidor

Visualización de certificados

Sobre esta tarea

La siguiente información aparece en PowerStore Manager para cada certificado que se almacena en el dispositivo:

- `Service`
- `Type`
- `Scope`
- `Issued by`
- `Valid`
- `Valid to`
- `Issued to`

NOTA: Utilice la API REST o la CLI para ver información adicional sobre el certificado.

Para ver la información del certificado, realice lo siguiente:

Pasos

1. Inicie PowerStore Manager.
2. Haga clic en **Settings** y, bajo **Security**, haga clic en **Certificates**.
   Aparece información sobre los certificados almacenados en el dispositivo.
3. Para ver la cadena de certificados que componen un certificado e información asociada para un servicio, haga clic en el servicio específico.
   View Certificate Chain aparece y muestra información sobre la cadena de certificados que componen el certificado.

Comunicación segura entre los dispositivos PowerStore dentro de un clúster

Durante la creación del clúster, el nodo primario del dispositivo maestro del clúster crea un certificado de autoridad de certificación (CA), también conocido como la CA del clúster. El dispositivo maestro transmite el certificado de CA del clúster a los dispositivos que se unen al clúster.

Cada dispositivo PowerStore en un clúster genera su propio certificado de IPsec único firmado por el certificado de CA del clúster. IPsec y TLS protegen la información confidencial que transmiten los dispositivos PowerStore a través de su red de clúster, lo que permite conservar la seguridad y la integridad de los datos.

Comunicación segura para la replicación y la importación de datos

La infraestructura de certificados y credenciales de PowerStore permite el intercambio de certificados de servidor y cliente, así como de la información de identificación. Este proceso incluye lo siguiente:

- Recuperación y validación del certificado del servidor durante el protocolo de enlace de TLS
- Adición del certificado de CA de confianza desde el sistema remoto al almacén de credenciales
- Adición del certificado de servidor/cliente de confianza al almacén de credenciales
- Apoyo para el establecimiento de conexiones seguras una vez que se establece la confianza

PowerStore es compatible con la siguiente funcionalidad de administración de certificados:

- Para la replicación, se intercambia un certificado entre dos clústeres de PowerStore con el fin de establecer la comunicación de administración de confianza. Para facilitar la replicación entre clústeres de PowerStore, se debe establecer una confianza bidireccional entre los clústeres que permita la autenticación de TLS mutua cuando se emiten solicitudes de control REST de replicación.
- Para la importación de datos, se intercambian un certificado y las credenciales con persistencia con el fin de establecer una conexión segura entre un sistema de almacenamiento Dell EMC (un sistema VNX, Unity, Storage Center [SC] o Peer Storage [PS]) y un clúster de PowerStore.

Compatibilidad con vSphere Storage API for Storage Awareness

vSphere Storage API for Storage Awareness (VASA) es una API independiente del proveedor definida por VMware para el reconocimiento del almacenamiento. Un proveedor de VASA consta de varios componentes que trabajan en cooperación para gestionar las solicitudes entrantes de la API de VASA. El gateway de la API de VASA, que recibe todas las API entrantes de VASA, se implementa en el dispositivo primario (el que posee la IP de administración flotante) en un clúster de PowerStore. Los hosts ESXi y vCenter Server se conectan al proveedor de VASA y obtienen información sobre el estado, las funcionalidades y la topología del almacenamiento disponibles. Posteriormente, vCenter Server proporciona esta información a los clientes de vSphere. Los clientes de VMware y no los de PowerStore Manager utilizan VASA.

El usuario de vSphere debe configurar la instancia del proveedor de VASA como el proveedor de información de VASA para el clúster. En caso de que el dispositivo principal quede inactivo, el proceso relacionado se reiniciará en el dispositivo que se convierte en el primario siguiente, junto con el proveedor de VASA. La conmutación por error de la dirección IP se realiza automáticamente. Internamente, el protocolo verá una falla cuando obtenga eventos de cambio en la configuración desde el proveedor de VASA recientemente activo, pero esto generará una resincronización automática de los objetos de VASA sin intervención del usuario.

PowerStore proporciona interfaces VASA 3.0 para vSphere 6.5 y 6.7.

VASA 3.0 es compatible con Virtual Volumes (VVols). VASA 3.0 es compatible con interfaces para consultar abstracciones de almacenamiento como VVols y contenedores de almacenamiento. Esta información facilita a la administración basada en políticas del almacenamiento (SPBM) la toma de decisiones con respecto al cumplimiento y la ubicación de unidades virtuales. VASA 3.0 también es compatible con interfaces para aprovisionar y administrar el ciclo de vida útil de VVols que se utilizan para respaldar unidades virtuales. Estas interfaces las invocan directamente los hosts ESXi.

Para obtener más información relacionada con VASA, vSphere y VVols, consulte la documentación de VMware y la ayuda en línea de PowerStore Manager.

Autenticación relacionada con VASA

Para iniciar una conexión desde vCenter al proveedor de VASA de PowerStore Manager, utilice el vSphere Client a fin de ingresar la siguiente información:

- Dirección URL del proveedor de VASA con el siguiente formato para VASA 3.0: https://<Management IP address>:8443/version.xml.
- Nombre de un usuario de PowerStore Manager (la función debe ser administrador de VM o administrador).

  NOTA: La función del administrador de VM se utiliza en exclusiva como medio para registrar los certificados.
- Contraseña asociada con este usuario.

Las credenciales de PowerStore Manager utilizadas aquí se emplean solamente durante este paso inicial de la conexión. Si las credenciales de PowerStore Manager son válidas para el clúster de destino, el certificado de vCenter Server se registra automáticamente con el clúster. Este certificado se usa para autenticar todas las solicitudes subsiguientes desde vCenter. No se requieren pasos manuales para instalar o cargar este certificado en el proveedor de VASA. Si el certificado venció, vCenter debe registrar uno nuevo para permitir una nueva sesión. Si el usuario revocó el certificado, la sesión pierde su validez y la conexión se interrumpe.

Sesión de vCenter, conexión segura y credenciales

Una sesión de vCenter comienza cuando un administrador de vSphere usa vSphere Client para proporcionar a vCenter Server la URL del proveedor de VASA y las credenciales de inicio de sesión. vCenter Server usa la URL, las credenciales y el certificado SSL del proveedor de VASA para establecer una conexión segura con el proveedor de VASA. La sesión de vCenter finaliza cuando se produce uno de los eventos siguientes:

- Un administrador usa vSphere Client para quitar el proveedor de VASA de la configuración de vCenter y vCenter Server finaliza la conexión.
- Falla vCenter Server o un servicio de vCenter Server, lo cual finaliza la conexión. Si vCenter o el servicio vCenter Server no pueden restablecer la conexión SSL, se iniciará una nueva.
- Falla el proveedor de VASA, lo cual finaliza la conexión. Cuando se inicia el proveedor de VASA, puede responder a la comunicación proveniente de vCenter Server para restablecer la conexión SSL y la sesión de VASA.

Una sesión de vCenter se basa en la comunicación HTTPS segura entre vCenter Server y un proveedor de VASA. En VASA 3.0, vCenter Server actúa como autoridad de certificación de VMware (VMCA). El proveedor de VASA transmite un certificado autofirmado a petición, una vez que se autoriza la solicitud. Agrega el certificado de VMCA a su almacén de confianza y, a continuación, emite una solicitud de firma de certificado y reemplaza su certificado autofirmado por el certificado firmado de VMCA. El proveedor de VASA autenticará las conexiones futuras mediante el certificado del servicio de monitoreo del almacenamiento (SMS) del cliente validado en función del certificado de firma raíz antes registrado. Un proveedor de VASA genera identificadores únicos para los objetos de entidad de almacenamiento, los cuales utiliza vCenter Server para solicitar los datos de una entidad específica.

El proveedor de VASA utiliza certificados SSL y el identificador de sesión de VASA para validar las sesiones de VASA. Después de establecer la sesión, un proveedor de VASA debe validar tanto el certificado SSL como el identificador de sesión de VASA asociado a cada llamada de función desde vCenter Server. El proveedor de VASA usa el certificado de VMCA almacenado en su almacén de confianza para validar el certificado asociado a las llamadas de función desde el SMS de vCenter. Las sesiones de VASA son persistentes en distintas conexiones SSL. Si se interrumpe una conexión SSL, vCenter Server ejecutará un protocolo de enlace de SSL con el proveedor de VASA para restablecer la conexión SSL en el contexto de la misma sesión de VASA. Si vence el certificado SSL, el administrador de vSphere debe generar un certificado nuevo. vCenter Server establecerá una conexión SSL nueva y registrará el certificado nuevo con el proveedor de VASA.

PRECAUCIÓN: SMS no llama a la función `unregisterVASACertificate` frente a un proveedor de VASA 3.0. Por lo tanto, incluso después de la anulación del registro, el proveedor de VASA puede continuar utilizando su certificado firmado de VMCA obtenido de SMS.

autenticación CHAP

El protocolo de autenticación por desafío mutuo (CHAP) es un método de autenticación de iniciadores iSCSI (hosts) y destinos (volúmenes e instantáneas). CHAP expone el almacenamiento iSCSI y garantiza un protocolo de almacenamiento estándar seguro. La autenticación depende de una seña secreta, similar a una contraseña, conocida tanto para el autenticador como para el par. El protocolo CHAP tiene dos variantes:

- La autenticación CHAP único permite que el destino iSCSI autentique al iniciador. Cuando un iniciador intenta conectarse a un destino (modo normal o a través del modo de descubrimiento), le proporciona a este un nombre de usuario y una contraseña.
- La autenticación CHAP mutuo se aplica además de CHAP único. CHAP mutuo permite que el destino iSCSI y el iniciador se autentiquen entre sí. El iniciador iSCSI autentica a cada destino iSCSI que presenta el grupo. Cuando un iniciador intenta conectarse a un destino, proporciona al iniciador un nombre de usuario y una contraseña. El iniciador compara el nombre de usuario y la contraseña proporcionados con la información que posee. Si coinciden, el iniciador puede conectarse al destino.

NOTA: Si se utilizará CHAP en el entorno, se recomienda configurar y habilitar la autenticación CHAP antes de preparar los volúmenes para recibir datos. Si prepara las unidades para recibir datos antes de configurar y habilitar la autenticación CHAP, podría perder el acceso a los volúmenes.

PowerStore no es compatible con el modo de descubrimiento de CHAP de iSCSI. En la siguiente tabla se muestran las limitaciones de PowerStore en relación con el modo de descubrimiento de CHAP de iSCSI.

Tabla 1. Limitaciones del modo de descubrimiento de CHAP de iSCSI

Modo de CHAP	Modo único (iniciador habilitado)	Modo mutuo (iniciador y destino habilitados)
Descubrimiento	PowerStore no autenticará (reto) al host. La autenticación no se puede usar para impedir el descubrimiento de destinos. Esto	PowerStore no responderá a una solicitud de autenticación (reto) desde un host y el

Tabla 1. Limitaciones del modo de descubrimiento de CHAP de iSCSI (continuación)

Modo de CHAP	Modo único (iniciador habilitado)	Modo mutuo (iniciador y destino habilitados)
	no da lugar a un acceso no deseado a los datos de usuario.	descubrimiento fallará si el host desafía a PowerStore.
Normal	Funciona según lo previsto. PowerStore prueba las credenciales.	Funciona según lo previsto. PowerStore transfiere las credenciales.

Para la replicación remota entre un dispositivo de origen y destino, el proceso de verificación y actualización detecta cambios en los sistemas locales y remotos, restablece las conexiones de datos y, a la vez, toma en cuenta los ajustes de CHAP.

Configuración de CHAP

En un clúster de PowerStore se puede habilitar la autenticación CHAP único (iniciador habilitado) o mutuo (iniciador y destino). CHAP se puede habilitar para la implementación de un clúster de un dispositivo o de varios dispositivos PowerStore y hosts externos.

Cuando se habilita la autenticación única, se requiere que el nombre de usuario y la contraseña de cada iniciador se ingresen en el momento en que se agregan hosts externos. Cuando se habilita la autenticación mutua, también es necesario ingresar el nombre de usuario y la contraseña del clúster. Cuando se agrega un host y se agregan iniciadores con CHAP habilitado, la contraseña del iniciador debe ser única; no se puede usar la misma contraseña en los iniciadores de un host. Los detalles específicos sobre cómo establecer la configuración de CHAP de un host externo varían. Para usar esta funcionalidad, debe estar familiarizado con el sistema operativo del host y la manera de configurarlo.

NOTA: La habilitación de CHAP una vez que los hosts están configurados en el sistema es una acción disruptiva para los hosts externos. Causa interrupción de I/O hasta que las configuraciones se establecen tanto en el host externo como en el dispositivo. Se recomienda que, antes de agregar hosts externos al dispositivo, decida qué tipo de configuración de CHAP desea implementar, si la hubiera.

Si habilita CHAP después de la adición de los hosts, actualice los iniciadores de cada host. Si CHAP está habilitado, no puede agregar un host a un grupo de hosts que no tenga credenciales de CHAP. Cuando CHAP esté habilitado y se agregue un host con posterioridad, regístrelo manualmente en PowerStore Manager. Para esto, en **Compute** seleccione **Hosts & Host Groups**. Debe ingresar credenciales en el nivel de iSCSI para uso de la autenticación. En este caso, copie el IQN desde el host y, a continuación, agregue las credenciales de CHAP relacionadas para cada iniciador.

Configure CHAP para un clúster a través de cualquiera de los siguientes medios:

- **CHAP**: una página de ajustes de CHAP a la que puede acceder desde PowerStore Manager (haga clic en **Settings** y, bajo **Security**, seleccione **CHAP**).
- Servidor de API REST: interfaz de aplicaciones que puede recibir solicitudes de la API REST para configurar los ajustes de CHAP. Para obtener más información sobre la API REST, consulte *PowerStore REST API Reference Guide*.

Para determinar el estado de CHAP, en PowerStore Manager, haga clic en **Settings** y, bajo **Security**, seleccione **CHAP**.

Acceso mediante SSH externo

Cada dispositivo puede habilitar de manera opcional el acceso de Secure Shell (SSH) externo al puerto SSH de la dirección IP del dispositivo, lo que lleva al usuario a la función de servicio en el nodo primario de un dispositivo. La dirección IP del dispositivo flota entre los dos nodos del dispositivo a medida que cambia la designación del nodo primario. Si SSH externo está deshabilitado, el acceso mediante SSH no se permite.

Cuando un dispositivo se enciende por primera vez y no está configurado, SSH se habilita de manera predeterminada de modo que el dispositivo pueda recibir servicio si se encuentran problemas antes de su adición a un clúster. Cuando se crea un nuevo clúster o para una operación de unión de un clúster, todos los dispositivos deben tener SSH configurado inicialmente como deshabilitado.

Configuración del acceso mediante SSH externo

Configure el acceso mediante SSH externo a los dispositivos de un clúster utilizando cualquiera de los siguientes medios:

- **SSH Management**: página de ajustes de SSH a la que puede acceder desde PowerStore Manager (haga clic en **Settings** y, bajo **Security**, seleccione **SSH Management**).

- Servidor de API REST: interfaz de aplicaciones que puede recibir solicitudes de la API REST para configurar los ajustes de SSH. Para obtener más información sobre la API REST, consulte *PowerStore REST API Reference Guide*.
- `svc_service_config` : un comando de servicio que puede ingresar directamente como el usuario de servicio en el dispositivo. Para obtener más información sobre este comando, consulte *PowerStore Service Scripts Guide*.

Para determinar el estado de SSH en los dispositivos de un clúster, en PowerStore Manager, haga clic en **Settings** y, bajo **Security**, seleccione **SSH Management**. También puede habilitar o deshabilitar SSH en uno o más dispositivos seleccionados.

Una vez que el servicio SSH se haya habilitado correctamente, utilice cualquier cliente SSH para iniciar sesión en la dirección IP del dispositivo. El acceso al dispositivo requiere información de identificación del servicio.

La cuenta de servicio les permite a los usuarios realizar las siguientes funciones:

- Ejecutar scripts de servicio del dispositivo especializados para monitorear y solucionar problemas de los ajustes y las operaciones del sistema del dispositivo.
- Operar solo un conjunto limitado de comandos que se asignan como un miembro de una cuenta de usuario de Linux sin privilegios en el modo de shell restringido. Esta cuenta no tiene acceso a los datos de usuarios o clientes, los archivos de configuración o los archivos de sistema patentados.

Para contar con un máximo nivel de seguridad del dispositivo, se recomienda dejar la interfaz de servicio de SSH externo deshabilitada en todo momento, a menos que se necesite específicamente para realizar operaciones de servicio en el dispositivo. Después de realizar las operaciones de servicio necesarias, deshabilite la interfaz de SSH para asegurarse de que el dispositivo permanezca seguro.

Sesiones de SSH

Las sesiones de la interfaz de servicio de SSH de PowerStore se mantienen conforme a los ajustes que establece el cliente SSH. Las características de las sesiones son determinadas por los parámetros de configuración del cliente SSH.

Contraseña de la cuenta de servicio

La cuenta de servicio es una cuenta que el personal de servicio puede usar para ejecutar comandos de Linux básicos.

Durante la configuración inicial del dispositivo, debe cambiar la contraseña de servicio predeterminada. Las restricciones de la contraseña de servicio son las mismas que se aplican a las cuentas de administración del sistema (consulte Uso de nombres de usuario y contraseñas en la página 7).

Autorización de SSH

La autorización de la cuenta de servicio se basa en lo siguiente:

- Aislamiento de aplicaciones: el software PowerStore utiliza tecnología de contenedor que proporciona aislamiento de aplicaciones. El contenedor de servicios proporciona acceso de servicio al dispositivo; están disponibles solamente un conjunto de scripts de servicio y un conjunto de comandos de Linux. La cuenta de servicio no tiene la capacidad de acceder a otros contenedores que gestionan el sistema de archivos y bloquean la I/O para los usuarios.
- Permisos del sistema de archivos Linux: la mayoría de las herramientas y las utilidades de Linux que modifican de alguna manera el funcionamiento del sistema no está disponible para el usuario de servicio; requieren privilegios de cuenta de superusuario. Dado que la cuenta de servicio no tiene tales derechos de acceso, no puede usar herramientas ni utilidades de Linux para las cuales no tiene permisos de ejecución ni puede editar archivos de configuración que requieren acceso de raíz para leer, modificar o ambos.
- Controles de acceso: además del aislamiento de aplicaciones que proporciona la tecnología de contenedores, el mecanismo de lista de control de acceso (ACL) en el dispositivo utiliza una lista de reglas muy específicas para conceder o rechazar explícitamente el acceso de la cuenta de servicio a los recursos del sistema. Estas reglas especifican los permisos de la cuenta de servicio a otras áreas del dispositivo que no definen de otro modo en los permisos estándares del sistema de archivos de Linux.

Scripts de servicio del dispositivo

Un conjunto de scripts de diagnóstico de problemas y configuración y recuperación del sistema está instalado en la versión de software del dispositivo. Estos scripts proporcionan información detallada y un nivel más bajo de control del sistema que el disponible a través de PowerStore Manager. En *PowerStore Service Scripts Guide* se describen estos scripts y sus casos de uso comunes.

Puerto de servicio Ethernet del nodo de un dispositivo y IPMItool

El dispositivo proporciona acceso a la consola por medio de un puerto de servicio Ethernet presente en cada nodo. Este acceso requiere el uso de IPMItool. IPMItool es una herramienta de red similar a SSH o Telnet, que se conecta a cada nodo a través de una conexión Ethernet mediante el protocolo IPMI. IPMItool es una utilidad de Windows que negocia un canal de comunicación seguro para acceder a la consola del nodo de un dispositivo. Esta utilidad requiere acceso físico para activar la consola.

La interfaz del puerto de servicio Ethernet del nodo proporciona las mismas funciones y características que la interfaz de SSH de servicio (interfaz de LAN de servicio) y también está sujeta a las mismas restricciones. Sin embargo, los usuarios acceden a la interfaz a través de una conexión a un puerto Ethernet en lugar de hacerlo mediante un cliente SSH. Esta interfaz está diseñada para el personal de servicio de campo que se puede conectar al dispositivo sin necesidad de alterar la red. No es necesaria una consola de administración dedicada.

Esta interfaz proporciona una conexión directa de punto a punto que no enrutable. El personal de servicio puede usar la interfaz de LAN de servicio para la salida de la consola, el acceso mediante SSH al contenedor de servicios de PowerStore y PowerStore Manager, incluido ICW (Initial Configuration Wizard). El acceso mediante SSH al contenedor de servicios a través de la interfaz de LAN de servicio está siempre habilitado y no se puede deshabilitar; sin embargo, usted administra la credencial de la cuenta de servicio.

Para obtener una lista de scripts de servicio, consulte *PowerStore Service Scripts Guide*.

NFS seguro

NFS seguro consiste en usar Kerberos para autenticar los usuarios con NFSv3 y NFSv4. Kerberos proporciona integridad (firma) y privacidad (cifrado). No es preciso habilitar la integridad ni la privacidad, sino que son opciones de exportación de NFS.

Sin Kerberos, el servidor depende por completo del cliente para autenticar los usuarios: el servidor confía en el cliente. No ocurre lo mismo con Kerberos, en cuyo caso el servidor confía en el centro de distribución de claves (KDC). El KDC se ocupa de manejar la autenticación y de administrar tanto las cuentas (entidades de seguridad) como las contraseñas. Es más, no se envía por vía electrónica ninguna contraseña de ninguna manera.

Sin Kerberos, la credencial del usuario se envía sin cifrar por vía electrónica y, por lo tanto, puede suplantarse con facilidad. Con Kerberos, la identidad (principal) del usuario se incluye en el vale cifrado de Kerberos, el cual pueden leer solo el servidor de destino y el KDC. Son los únicos que conocen la clave de cifrado.

En combinación con el NFS seguro, son compatibles los cifrados AES128 y AES256 en Kerberos. Junto con el NFS seguro, eso también repercute en SMB y LDAP. Estos cifrados ya son compatibles en forma predeterminada con Windows y Linux. Estos nuevos cifrados son mucho más seguros, pero su uso queda a discreción del cliente. A partir de esa entidad de seguridad de usuario, el servidor crea la credencial de dicho usuario realizando una consulta al servicio de directorio de UNIX (UDS) activo. Como NIS no está protegido, no se recomienda utilizarlo con el NFS seguro. Se recomienda usar Kerberos con LDAP o LDAPS.

NFS seguro se puede configurar a través de PowerStore Manager.

Relaciones con los protocolos de archivos

Con Kerberos, se necesita lo siguiente:

- DNS: debe usar el nombre de DNS en lugar de direcciones IP.
- NTP: PowerStore debe tener un servidor NTP configurado.

  NOTA: Kerberos depende de la sincronización de hora correcta entre el KDC, los servidores y el cliente en la red.
- UDS: permite crear las credenciales.
- Nombre de host: Kerberos funciona con nombres, no con direcciones IP.

NFS seguro utiliza uno o dos nombres de entidad de seguridad de servicio (SPN) en función del valor del nombre de host. Si es el nombre de host tiene el formato de nombre de dominio calificado host.dominio:

- SPN corto: **`nfs/host@REALM`**
- SPN largo: **`nfs/host.domainFQDN@REALM`**

Si el nombre de host no tiene el formato de nombre de dominio calificado, solo se usará el SPN corto.

De manera similar a lo que ocurre con SMB, si es posible unir un servidor SMB a un dominio, también lo es unir un servidor NFS a un dominio (el equivalente en Kerberos). Para hacerlo, existen dos opciones:

- Utilizar el dominio de Windows configurado, si lo hay
- Configurar por completo un dominio de Kerberos basado en el KDC de UNIX

Si el administrador decide utilizar el dominio de Windows configurado, no hay que hacer nada más. Todos los SPN que utiliza el servicio de NFS se agregan al KDC o se quitan de él de forma automática al unir o desvincular el servidor de SMB. Tenga en cuenta que el servidor de SMB no puede destruirse si el NFS seguro está configurado para usar la configuración de SMB.

Si el administrador decide utilizar un dominio de Kerberos basado en UNIX, se requiere más configuración:

- Nombre del dominio: el nombre del dominio de Kerberos, cuyas letras están, por lo general, en mayúscula.
- Configure por completo un dominio de Kerberos basado en el KDC de UNIX.

Para asegurarse de que el cliente monta la exportación de NFS con una seguridad concreta, se proporciona el parámetro de seguridad sec, el cual indica la seguridad mínima permitida. Hay cuatro clases de seguridad:

- `AUTH_SYS`: seguridad heredada estándar que no utiliza Kerberos. el servidor confía en la credencial proporcionada por el cliente
- `KRB5`: autenticación mediante Kerberos versión 5
- `KRB5i`: autenticación Kerberos con integridad (firma)
- `KRB5p`: autenticación Kerberos con integridad y privacidad (cifrado)

Si el cliente de NFS intenta montar la exportación con una seguridad inferior a la seguridad mínima configurada, se denegará el acceso. Por ejemplo, si el acceso mínimo es `KRB5i`, se rechazará cualquier montaje con `AUTH_SYS` o `KRB5`.

Creación de credenciales

Cuando un usuario se conecta al sistema, presenta solamente su entidad de seguridad, **`user@REALM`**, la que se extrae del vale de Kerberos. A diferencia de la seguridad `AUTH_SYS`, la credencial no se incluye en la solicitud de NFS. La parte del usuario (antes del símbolo @) se extrae del principal y se utiliza para consultar el UID correspondiente en el UDS. A partir de ese UID, el sistema crea la credencial usando el UDS activo, de modo similar a cuando está habilitada la credencial extendida de NFS (con la excepción de que, sin Kerberos, la solicitud proporciona directamente el UID).

Si el principal no está mapeado en el UDS, se utiliza en su lugar la información de identificación de UNIX predeterminada configurada. Si no está configurado el usuario de UNIX predeterminado, se utilizará la credencial nobody.

Seguridad en los objetos de los sistemas de archivos

En un ambiente multiprotocolo, la política de seguridad se configura en el nivel del sistema de archivos y es independiente para cada sistema de archivos. Cada sistema de archivos usa su política de acceso para determinar cómo conciliar las diferencias entre las semánticas de control de acceso de NFS y SMB. La selección de una política de acceso determina el mecanismo que se utiliza para aplicar la seguridad de archivos en el sistema de archivos específico.

NOTA: Si es necesario admitir el protocolo SMB1 más antiguo en el entorno, se puede habilitar mediante el comando de servicio `svc_nas_cifssupport`. Para obtener más información sobre este comando de servicio, consulte *PowerStore Service Scripts Guide*.

Modelo de seguridad de UNIX

Cuando se selecciona la política de UNIX, no se hace caso de los intentos de modificación de la seguridad en el nivel de archivos desde el protocolo SMB, como la modificación de las listas de control de acceso (ACL). A los derechos de acceso de UNIX se les denomina los bits de modo o la ACL de NFSv4 de un objeto del sistema de archivos. Los bits de modo se representan mediante una cadena de bits. Cada bit equivale a un modo o derecho de acceso otorgado al usuario que posee el archivo, al grupo asociado con el objeto del sistema de archivos y a todos los demás usuarios. Los bits de modo de UNIX se representan como tres conjuntos de triadas rwx (lectura, escritura y ejecución) concatenadas para cada categoría de usuarios (usuario, grupo u otro). Una ACL es una lista de usuarios y grupos de usuarios mediante la cual se controla el acceso a servicios y la negación de estos.

Modelo de seguridad de Windows

El modelo de seguridad de Windows se basa principalmente en derechos de objetos, lo cual implica el uso de un descriptor de seguridad (SD) y de su ACL. Cuando se selecciona la política de SMB, no se hace caso de las modificaciones en los bits de modo desde el protocolo NFS.

El acceso a un objeto del sistema de archivos se basa en si los permisos se configuraron en Permitir o Rechazar mediante el uso de un descriptor de seguridad. El SD describe el propietario del objeto y los SID de grupo para el objeto, junto con sus ACL. Una ACL es parte del

descriptor de seguridad de cada objeto. Cada ACL contiene entradas de control de acceso (ACE). A su vez, cada ACE contiene un único SID que identifica a un usuario, un grupo o una computadora, y una lista de derechos que se rechazan o se permiten para ese SID.

Acceso a sistemas de archivos en un ambiente multiprotocolo

El acceso a archivos se proporciona a través de servidores NAS. Un servidor NAS contiene un conjunto de sistemas de archivos donde están almacenados los datos. El servidor NAS proporciona acceso a estos datos para los protocolos de archivos NFS y SMB mediante el uso compartido de los sistemas de archivos a través de recursos compartidos SMB y NFS. El modo del servidor NAS para el uso compartido multiprotocolo permite el uso compartido de los mismos datos entre SMB y NFS. Dado que el modo de uso compartido multiprotocolo ofrece acceso simultáneo de SMB y NFS a un sistema de archivos, el mapeo de usuarios de Windows a usuarios de UNIX y la definición de las reglas de seguridad que se deben utilizar (bits de modo, ACL e información del usuario) se deben tener en cuenta y configurar correctamente para el uso compartido multiprotocolo.

NOTA: Para obtener información sobre la configuración y la administración de servidores NAS con respecto al uso compartido multiprotocolo, el mapeo de usuarios, las políticas de acceso y la información de identificación, consulte la ayuda en línea de PowerStore Manager.

Mapeo de usuarios

En un contexto multiprotocolo, un usuario de Windows se debe asociar a un usuario de UNIX. Sin embargo, un usuario de UNIX se debe mapear a un usuario de Windows solamente cuando la política de acceso es Windows. Esta coincidencia es necesaria para que se pueda aplicar la seguridad del sistema de archivos, incluso si no es nativa para el protocolo. Los siguientes componentes son parte del mapeo de usuarios:

- Servicios de directorio de UNIX, archivos locales o ambos
- Solucionadores de Windows
- Mapeo seguro (secmap): Una caché que contiene todos los mapeos entre SID y UID o GID que usa un servidor NAS.
- ntxmap

NOTA: El mapeo de usuarios no afecta a los usuarios o los grupos que son locales en el servidor SMB.

Servicios de directorio de UNIX y archivos locales

Los servicios de directorio de UNIX (UDS) y los archivos locales se usan para realizar lo siguiente:

- Devuelven el nombre de cuenta de UNIX correspondiente para un identificador de usuario (UID) específico.
- Devuelven el UID y el ID de grupo (GID) primario correspondientes para un nombre de cuenta de UNIX específico.

Los servicios compatibles son:

- LDAP
- NIS
- Archivos locales
- Ninguno (el único mapeo posible es a través del usuario predeterminado)

Cuando está activado el uso compartido multiprotocolo, debe estar activado un UDS, los archivos locales o ambos para el servidor NAS. La propiedad del servicio de directorio de UNIX del servidor NAS determina lo que se utiliza para el mapeo de usuarios.

Solucionadores de Windows

Los solucionadores de Windows se usan para realizar lo siguiente para el mapeo de usuarios:

- Devuelven el nombre de cuenta de Windows correspondiente para un identificador de seguridad (SID) específico
- Devuelven el SID correspondiente para un nombre de cuenta de Windows específico

Los solucionadores de Windows son:

- La controladora de dominio (DC) del dominio
- Base de datos del grupo local (LGDB) del servidor SMB

secmap

La función de secmap es almacenar todos los mapeos de SID a UID y GID primario y de UID a SID con el fin de garantizar la coherencia en todos los sistemas de archivos del servidor NAS.

ntxmap

ntxmap se usa para asociar una cuenta de Windows a una cuenta de UNIX cuando el nombre es diferente. Por ejemplo, si hay un usuario con una cuenta denominada Gerald en Windows, pero la cuenta en UNIX se llama Gerry, se usa ntxmap para establecer la correlación entre ambas cuentas.

Mapeo de SID a UID, GID primario

La siguiente secuencia es el proceso que se usa para resolver un mapeo de SID a UID, GID primario:

1. El SID se busca en secmap. Si el SID se encuentra, el mapeo del UID y el GID se resuelve.
2. Si el SID no se encuentra en secmap, se debe buscar el nombre de Windows relacionado con el SID.
    a. El SID se busca en las bases de datos del grupo local de los servidores SMB de NAS. Si el SID se encuentra, el nombre de Windows relacionado es el nombre de usuario local junto con el nombre del servidor SMB.
    b. Si el SID no se encuentra en la base de datos del grupo local, se busca en la DC del dominio. Si el SID se encuentra, el nombre de Windows relacionado es el nombre de usuario. Si el SID no se puede resolver, se niega el acceso.
3. El nombre de Windows se traduce a un nombre de UNIX. Para esto se utiliza ntxmap.
    a. Si el nombre de Windows se encuentra en ntxmap, la entrada se utiliza como el nombre de UNIX.
    b. Si el nombre de Windows no se encuentra en ntxmap, el nombre de Windows se utiliza como el nombre de UNIX.
4. Se busca en el UDS (servidor NIS, servidor LDAP o archivos locales) mediante el nombre de UNIX.
    a. Si el nombre de usuario de UNIX se encuentra en el UDS, el mapeo de UID y GID se resuelve.
    b. Si el nombre de UNIX no se encuentra, pero la función de mapeo automático de las cuentas de Windows sin mapear está activada, el UID se asigna automáticamente.
    c. Si el nombre de usuario de UNIX no se encuentra en el UDS, pero hay una cuenta predeterminada de UNIX, el mapeo de UID y GID se resuelve en el de la cuenta predeterminada de UNIX.
    d. Si el SID no se puede resolver, se niega el acceso.

Si el mapeo se encuentra, se agrega en la base de datos persistente de secmap. Si no se encuentra, el mapeo fallido se agrega en la base de datos persistente de secmap.

En el siguiente diagrama se ilustra el proceso que se utiliza para resolver un mapeo de SID a un UID, GID primario:

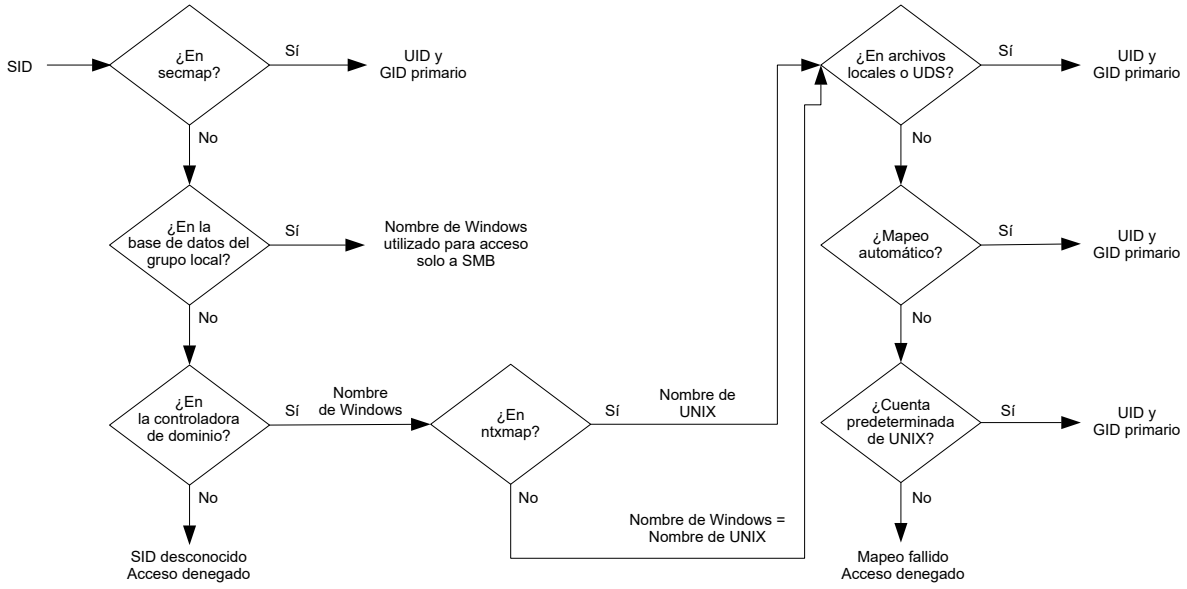

Ilustración 1. Proceso para resolver un mapeo de un SID a un UID, GID primario

Mapeo de UID a SID

La siguiente secuencia es el proceso que se usa para resolver un mapeo de UID a un SID:

1. El UID se busca en secmap. Si el UID se encuentra, el mapeo de SID se resuelve.
2. Si el UID no se encuentra en secmap, se debe buscar el nombre de UNIX relacionado con el UID.
    a. Se busca en el UDS (servidor NIS, servidor LDAP o archivos locales) mediante el UID. Si el UID se encuentra, el nombre de UNIX relacionado es el nombre de usuario.
    b. Si el UID no se encuentra en el UDS, pero hay una cuenta predeterminada de Windows, el UID se mapea al SID de la cuenta predeterminada de Windows.
3. Si la información de la cuenta predeterminada de Windows no se utiliza, el nombre de UNIX se traduce a un nombre de Windows. Para esto se utiliza ntxmap.
    a. Si el nombre de UNIX se encuentra en ntxmap, la entrada se utiliza como el nombre de Windows.
    b. Si el nombre de UNIX no se encuentra en ntxmap, el nombre de UNIX se utiliza como el nombre de Windows.
4. Se busca en la controladora de dominio de Windows o en la base de datos del grupo local mediante el nombre de Windows.
    a. Si el nombre de Windows se encuentra, el mapeo de SID se resuelve.
    b. Si el nombre de Windows contiene un punto y la parte del nombre tras el último punto (.) coincide con un nombre de servidor SMB, se busca en la base de datos del grupo local de ese servidor SMB para resolver el mapeo de SID.
    c. Si el nombre de Windows no se encuentra, pero hay una cuenta predeterminada de Windows, el SID se mapea al de esa cuenta predeterminada de Windows.
    d. Si el SID no se puede resolver, se niega el acceso.

Si el mapeo se encuentra, se agrega en la base de datos persistente de secmap. Si no se encuentra, el mapeo fallido se agrega en la base de datos persistente de secmap.

En el siguiente diagrama se ilustra el proceso que se utiliza para resolver un mapeo de UID a un SID:

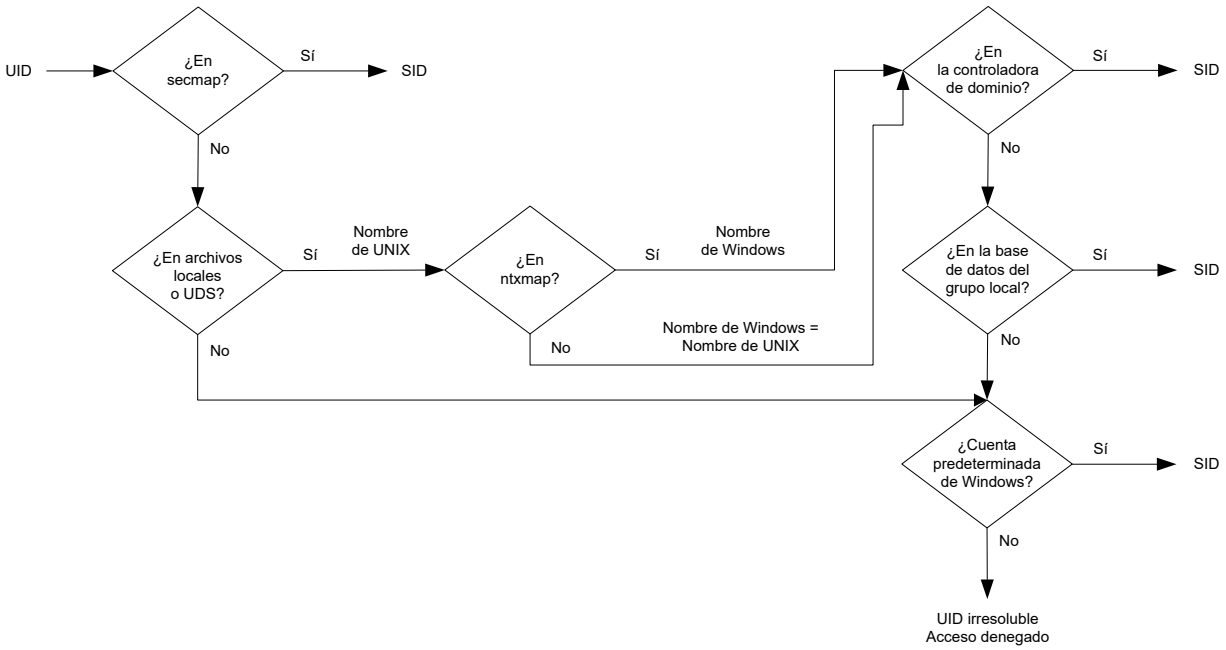

Ilustración 2. Proceso que se utiliza para resolver un mapeo de un UID a un SID

Políticas de acceso para NFS, SMB y FTP

En un ambiente multiprotocolo, el sistema de almacenamiento usa políticas de acceso del sistema de archivos para administrar el control de acceso de los usuarios a sus sistemas de archivos. Existen dos tipos de seguridad, UNIX y Windows.

Para la autenticación de seguridad de UNIX, la credencial se crea a partir de los servicios de directorio de UNIX (UDS), excepto para el acceso NFS no seguro, en el cual el cliente de host la proporciona. Los derechos de usuario se determinan a partir de los bits de modo y la ACL de NFSv4. Los identificadores de usuario y de grupo (UID y GID, respectivamente) se usan para la identificación. No hay privilegios asociados con la seguridad de UNIX.

En el caso de la autenticación de seguridad de Windows, la credencial se crea a partir de la controladora de dominio de Windows y la base de datos del grupo local (LGDB) del servidor de SMB. Los derechos de usuario se determinan según las ACL de SMB. El identificador de seguridad (SID) se usa para la identificación. La LGDB o el objeto de política de grupo (GPO) del servidor SMB otorgan los privilegios asociados a la seguridad de Windows, como Tomar posesión, Respaldar y Restaurar.

La tabla siguiente describe las políticas de acceso que definen la seguridad que usan los distintos protocolos:

Política de acceso	Descripción
Nativa (valor predeterminado)	• Cada protocolo administra el acceso con su seguridad nativa. • La seguridad de los recursos compartidos NFS usa la credencial de UNIX asociada con la solicitud para comprobar los bits de modo de UNIX de NFSv3 o la ACL de NFSv4. El acceso se concede o se rechaza. • La seguridad de los recursos compartidos SMB usa la credencial de Windows asociada con la solicitud para comprobar la ACL de SMB. El acceso se concede o se rechaza. • Los bits de modo de UNIX de NFSv3 y los cambios de permisos de la ACL de NFSv4 se sincronizan entre sí. • No hay ninguna sincronización entre los permisos de Unix y Windows.
Windows	• Protege el acceso en el nivel de archivo para Windows y UNIX mediante la seguridad de Windows. • Usa una credencial de Windows para comprobar la ACL de SMB. • Los permisos para archivos creados recientemente se determinan mediante una conversión de la ACL de SMB. Los cambios de permisos de la ACL de SMB se sincronizan con los bits de modo de UNIX de NFSv3 o la ACL de NFSv4. • Se deniegan los cambios de permisos en los bits de modo de NFSv3 y la ACL de NFSv4.
UNIX	• Protege el acceso en el nivel de archivo para Windows y UNIX mediante la seguridad de UNIX. • Tras la solicitud de acceso de SMB, la credencial de UNIX creada desde los archivos locales o el UDS se usa para comprobar los bits de modo de NFSv3 o la ACL de NFSv4 en búsqueda de permisos. • Los permisos de los archivos creados recientemente se determinan mediante la UMASK. • Los cambios de permisos de los bits de modo de UNIX de NFSv3 o la ACL de NFSv4 se sincronizan con la ACL de SMB. • Se permiten los cambios de permisos en la ACL de SMB a fin de evitar la interrupción, pero estos permisos no se conservan.

En el caso de FTP, la autenticación con Windows o UNIX depende del formato del nombre de usuario que se usa cuando se realiza la autenticación en el servidor NAS. Si se usa la autenticación de Windows, el control de acceso de FTP es similar al de SMB; de lo contrario, la autenticación es similar a la de NFS. Los clientes FTP y SFTP se autentican cuando se conectan al servidor NAS. Puede ser una autenticación de SMB (cuando el formato del nombre de usuario es `domain\user` o `user@domain`) o una autenticación de UNIX (para los otros formatos de nombre de usuario único). La controladora de dominio de Windows del dominio definido en el servidor NAS garantiza la autenticación de SMB. El servidor NAS garantiza la autenticación de UNIX de acuerdo con la contraseña cifrada almacenada en un servidor LDAP remoto, un servidor NIS remoto o el archivo password local del servidor NAS.

Credenciales para la seguridad en el nivel de archivos

Para aplicar la seguridad en los archivos, el sistema de almacenamiento debe crear una credencial que se asocie a la solicitud SMB o NFS que se maneja. Hay dos tipos de credenciales, Windows y UNIX. El servidor NAS crea las credenciales de UNIX y de Windows para los siguientes casos de uso:

- Para crear una credencial de UNIX con más de 16 grupos para una solicitud de NFS. Con el fin de ofrecer esta capacidad, se debe configurar la propiedad de credencial extendida del servidor NAS.
- Para crear una credencial de UNIX para una solicitud de SMB cuando la política de acceso para el sistema de archivos es UNIX.
- Para crear una credencial de Windows para una solicitud de SMB.

- Para crear una credencial de Windows para una solicitud de NFS cuando la política de acceso para el sistema de archivos es Windows.

NOTA: Para una solicitud de NFS cuando la propiedad de credencial extendida no está configurada, se utiliza la credencial de UNIX de la solicitud de NFS. Cuando se usa la autenticación Kerberos para una solicitud de SMB, la credencial de Windows del usuario del dominio se incluye en el vale de Kerberos de la solicitud de configuración de la sesión.

Una caché de credenciales persistente se usa para lo siguiente:

- Credenciales de Windows creadas para el acceso a un sistema de archivos que tiene una política de acceso de Windows.
- Credencial de UNIX para acceso a través de NFS si está activada la opción de credencial extendida.

Hay una instancia de caché para cada servidor NAS.

Concesión de acceso a usuarios no mapeados

El ambiente multiprotocolo requiere lo siguiente:

- Un usuario de Windows debe estar mapeado a un usuario de UNIX.
- Un usuario de UNIX debe estar mapeado a un usuario de Windows de modo que se cree la credencial de Windows cuando el usuario acceda a un sistema de archivos que tenga una política de acceso de Windows.

Hay dos propiedades asociadas al servidor NAS con respecto a los usuarios no mapeados:

- El usuario de UNIX predeterminado.
- El usuario de Windows predeterminado.

Cuando un usuario no mapeado de Windows intenta conectarse a un sistema de archivos multiprotocolo y está configurada la cuenta de usuario predeterminada de UNIX para el servidor NAS, se usan el identificador de usuario (UID) y el ID de grupo (GID) primario del usuario predeterminado de UNIX en la credencial de Windows. De manera similar, cuando un usuario no mapeado de UNIX intenta conectarse a un sistema de archivos multiprotocolo y está configurada la cuenta de usuario predeterminada de Windows para el servidor NAS, se usa la credencial de Windows del usuario predeterminado de Windows.

NOTA: Si el usuario predeterminado de UNIX no está configurado en los servicios de directorio de UNIX (UDS), se niega el acceso de SMB para los usuarios no mapeados. Si el usuario predeterminado de Windows no se encuentra en la controladora de dominio de Windows ni en la LGDB, se niega el acceso de NFS para los usuarios no mapeados en un sistema de archivos que tiene una política de acceso de Windows.

NOTA: El usuario predeterminado de UNIX puede ser un nombre de cuenta de UNIX existente y válido o seguir el formato nuevo `@uid=`*`xxxx`*`,gid=`*`yyyy`*`@`, donde *xxxx* e *yyyy* son los valores numéricos decimales del UID y del GID primario, respectivamente, los cuales se pueden configurar en el sistema mediante PowerStore Manager.

Credencial de UNIX para solicitudes NFS

Para manejar las solicitudes de NFS para un sistema de archivos solo NFS o multiprotocolo con una política de acceso de UNIX o nativa, se debe utilizar una credencial de UNIX. La credencial de UNIX está siempre incorporada en cada solicitud; sin embargo, está limitada a 16 grupos adicionales. La propiedad `extendedUnixCredEnabled` del servidor NFS ofrece la capacidad de crear una credencial con más de 16 grupos. Si se configura esta propiedad, se consulta al UDS activo con el UID para obtener el GID primario y todos los GID de grupo a los cuales pertenece. Si el UID no se encuentra en el UDS, se usa la credencial de UNIX incorporada en la solicitud.

NOTA: Para el acceso seguro de NFS, la credencial se crea siempre mediante UDS.

Credencial de UNIX para solicitudes SMB

Para manejar las solicitudes de SMB para un sistema de archivos multiprotocolo con una política de acceso de UNIX, primero se debe crear una credencial de Windows para el usuario de SMB en el momento de la configuración de la sesión. El SID del usuario de Windows se utiliza para buscar el nombre en AD. A continuación, ese nombre se utiliza (opcionalmente a través de ntxmap) para buscar un UID y un GID de Unix desde el UDS o el archivo local (archivo passwd). El UID del propietario del usuario se incluye en la credencial de Windows. Cuando se accede a un sistema de archivos con una política de acceso de UNIX, el UID del usuario se utiliza para consultar los UDS de modo que se cree la credencial de UNIX, lo que se asemeja a la creación de una credencial extendida para NFS. El UID se requiere para la administración de cuotas.

Credencial de Windows para solicitudes SMB

Para manejar las solicitudes de SMB para un sistema de archivos solo SMB o multiprotocolo con una política de acceso de Windows o nativa, se debe utilizar una credencial de Windows. La credencial de Windows para SMB solo tiene que crearse una vez en el momento en que se solicita la configuración de la sesión cuando se conecta el usuario.

Cuando se usa la autenticación Kerberos, la credencial del usuario se incluye en el vale de Kerberos de la solicitud de configuración de la sesión, a diferencia de cuando se usa NT LAN Manager (NTLM). Otra información se consulta al DC de Windows o a la LGDB. Para Kerberos, la lista de SID de grupos adicionales se obtiene del vale de Kerberos y la lista de SID de grupos locales adicionales. La lista de privilegios se obtiene de la LGDB. Para NTLM, la lista de SID de grupos adicionales se obtiene de la DC de Windows y la lista de SID de grupos locales adicionales. La lista de privilegios se obtiene de la LGDB.

Además, el UID y el GID primario correspondientes también se recuperan del componente de mapeo de usuarios. Dado que el SID del grupo primario no se usa para comprobar el acceso, en su lugar se usa el GID primario de UNIX.

NOTA: NTLM es un conjunto más antiguo de protocolos de seguridad de propiedad que proporciona autenticación, integridad y confidencialidad a los usuarios. Kerberos es un protocolo estándar abierto que ofrece una autenticación más rápida mediante un sistema de vales. Kerberos brinda mayor seguridad que NTLM para los sistemas que están en una red.

Credencial de Windows para solicitudes NFS

La credencial de Windows solo se crea o se recupera cuando un usuario intenta, a través de una solicitud de NFS, acceder a un sistema de archivos que tiene una política de acceso de Windows. El UID se obtiene de la solicitud NFS. Hay una caché global de credenciales de Windows que ayuda a evitar la creación de la credencial en cada solicitud NFS con un tiempo de retención asociado. Si la credencial de Windows se encuentra en esta caché, no se requiere ninguna otra acción. Si la credencial de Windows no se encuentra, se consultan los UDS o el archivo local para buscar el nombre correspondiente al UID. A continuación, el nombre se utiliza (opcionalmente a través de ntxmap) para buscar un usuario de Windows y la credencial se recupera desde la DC de Windows o la LGDB. Si el mapeo no se encuentra, se usa en su lugar la credencial de Windows del usuario de Windows predeterminado o se niega el acceso.

Comprensión de Common AntiVirus Agent (CAVA)

Common AntiVirus Agent (CAVA) ofrece una solución antivirus para los clientes que utilizan un servidor NAS. Utiliza un protocolo SMB estándar del sector en un ambiente de Microsoft Windows Server. CAVA utiliza software antivirus de otros fabricantes para identificar y eliminar virus conocidos antes de que infecten los archivos del sistema de almacenamiento.

¿Por qué el antivirus es importante?

Gracias a su arquitectura, el sistema de almacenamiento es resistente a la invasión de virus. El servidor NAS ejecuta Data Access in Real Time mediante un sistema operativo integrado. Otros fabricantes no pueden ejecutar programas que contienen virus en este sistema operativo. Si bien el software del sistema operativo es resistente a los virus, los clientes de Windows que acceden al sistema de almacenamiento requieren protección contra virus. La protección contra virus en los clientes reduce la posibilidad de que se almacene un archivo infectado en el servidor y protege a los clientes en caso de que se abra uno de estos archivos. La solución antivirus consta de una combinación del software del sistema operativo, el agente CAVA y un motor antivirus de otros fabricantes. El software CAVA y el motor antivirus de otros fabricantes deben instalarse en un servidor de Windows en el dominio.

Para obtener información adicional acerca de CAVA, que forma parte de Common Event Enabler (CEE), consulte *Using the Common Event Enabler on Windows Platforms* en www.dell.com/powerstoredocs.

Firma de código

PowerStore está diseñado para aceptar actualizaciones de software tanto para versiones nuevas como para versiones de parche. Una clave maestra de GNU Privacy Guard (GPG) firma todos los paquetes de software de PowerStore y Dell EMC la controla. El proceso de actualización de software de PowerStore verifica la firma del paquete de software y rechaza firmas no válidas que puedan indicar una posible manipulación o daño. El paso de verificación está incorporado en el proceso de actualización y la firma del paquete de software se verifica automáticamente durante la fase previa a la instalación.

2

Ajustes de seguridad para la comunicación

Esta sección contiene los siguientes temas:

Temas:

Uso de puertos

En las siguientes secciones se describe el conjunto de puertos de red y los servicios correspondientes que se pueden encontrar en el dispositivo. El dispositivo funciona como un cliente de red en diversas circunstancias, por ejemplo, en la comunicación con una instancia de vCenter Server. En estos casos, el dispositivo inicia la comunicación y la infraestructura de red deberá admitir estas conexiones.

NOTA: Para obtener información adicional acerca de los puertos, consulte el artículo 542240 de la base de conocimientos, *PowerStore: reglas de firewall de la red del cliente: puertos TCP/UDP* [en inglés]. Vaya a https://www.dell.com/support/kbdoc/en-us/542240. La herramienta Reglas de firewall de la red del cliente permite filtrar y revisar la lista de reglas y puertos de firewall que son pertinentes a la implementación de PowerStore.

Puertos de red del dispositivo

En la siguiente tabla se describe el conjunto de puertos de red y los servicios correspondientes que se pueden encontrar en el dispositivo.

Tabla 2. Puertos de red del dispositivo

Puerto	Servicio	Protocolo	Dirección de acceso	Descripción
22	Cliente SSH, SupportAssist Connect Home	TCP	Bidireccional	• Permite el acceso mediante el protocolo SSH (si está habilitado). • Se requiere para SupportAssist Connect Home. Si está cerrado, las conexiones de administración por medio de SSH no estarán disponibles.
25	SMTP	TCP	Saliente	Permite que el dispositivo envíe un correo electrónico. Si está cerrado, las notificaciones por correo electrónico no estarán disponibles.
26	Cliente SSH	TCP	Bidireccional	El acceso mediante SSH al puerto 22 se redirige a este puerto. Si está cerrado, las conexiones de administración por medio de SSH no estarán disponibles.
53	DNS	TCP/UDP	Saliente	Se utiliza para transmitir consultas de DNS al servidor DNS. Si está cerrado, la resolución de nombres de DNS no funcionará.
80, 8080 y 8128	SupportAssist	TCP	Saliente	Se utiliza para la conexión del proxy de SupportAssist.
123	NTP	TCP/UDP	Saliente	Sincronización horaria de NTP. Si está cerrado, la hora no se sincronizará entre los dispositivos.

Tabla 2. Puertos de red del dispositivo (continuación)

Puerto	Servicio	Protocolo	Dirección de acceso	Descripción
443	HTTPS	TCP	Bidireccional	Tráfico HTTP seguro a PowerStore Manager. Si está cerrado, la comunicación con el dispositivo no estará disponible.
500	IPsec (IKEv2)	UDP	Bidireccional	Para hacer que IPsec funcione a través de los firewalls, abra el puerto UDP 500 y permita los números de protocolo IP 50 y 51 en los filtros de firewall entrantes y salientes. El puerto UDP 500 se debe abrir para permitir que el tráfico de Internet Security Association and Key Management Protocol (ISAKMP) se reenvíe a través de los firewalls. El ID de protocolo IP 50 se debe configurar para permitir el reenvío del tráfico de IPsec Encapsulating Security Protocol (ESP). El ID de protocolo IP 51 se debe configurar para permitir el reenvío del tráfico del encabezado de autenticación (AH). Si está cerrado, la conexión IPsec entre los dispositivos PowerStore no estará disponible.
587	SMTP	TCP	Saliente	Permite que el dispositivo envíe un correo electrónico. Si está cerrado, las notificaciones por correo electrónico no estarán disponibles.
3033	Importar	TCP/UDP	Saliente	Se requiere para la importación del almacenamiento desde los sistemas EqualLogic Peer Storage y Compellent Storage Center heredados.
3260	iSCSI	TCP	• Entrante para acceso de host y host ESXi • Bidireccional para replicación • Saliente para la importación del almacenamiento	Se requiere para proporcionar el siguiente acceso a servicios de iSCSI: • Acceso iSCSI a host externo • Acceso iSCSI a host ESXi externo o integrado en PowerStore • Acceso entre clústeres para replicación • Acceso a la importación del almacenamiento desde los sistemas EqualLogic Peer Storage, Compellent Storage Center, Unity y VNX2 heredados Si está cerrado, los servicios iSCSI no estarán disponibles. Lo utiliza la movilidad de datos para admitir un rendimiento de replicación razonable en una conexión de baja latencia.
3261	Movilidad de datos	TCP	Bidireccional	Lo utiliza la movilidad de datos para admitir un rendimiento de replicación razonable en una conexión de alta latencia.
5353	DNS de multidifusión (mDNS)	UDP	Bidireccional	Consulta DNS de multidifusión. Si está cerrado, la resolución de nombres de mDNS no funcionará.
8443	VASA, SupportAssist	TCP	• Entrante para VASA • Saliente para SupportAssist	• Se requiere para el proveedor de VASA para VASA 3.0. • Se requiere para las funciones de SupportAssist Connect Home relacionadas.
8443, 50443, 55443 o 60443	Agente de host de importación de	TCP	Saliente	Uno de estos puertos debe estar abierto cuando se importa almacenamiento de datos

Tabla 2. Puertos de red del dispositivo (continuación)

Puerto	Servicio	Protocolo	Dirección de acceso	Descripción
	Windows, agente de host de importación de Linux o agente de host de importación de VMware			desde sistemas de almacenamiento heredado.
9443	SupportAssist	TCP	Saliente	Se requiere para la API REST de SupportAssist relacionada con Connect Home.

Puertos de red del dispositivo relacionados con archivos

En la siguiente tabla se describe el conjunto de puertos de red y los servicios correspondientes que se pueden encontrar en el dispositivo en relación con archivos.

NOTA: Los puertos salientes son efímeros.

Tabla 3. Puertos de red del dispositivo relacionados con archivos

Puerto	Servicio	Protocolo	Dirección de acceso	Descripción
20	FTP	TCP	Saliente	Es el puerto utilizado para las transferencias de datos por FTP. Este puerto se puede abrir mediante la habilitación de FTP. La autenticación se ejecuta en el puerto 21 y está definida por el protocolo FTP.
21	FTP	TCP	Entrante	El puerto 21 es el puerto de control en el que el servicio FTP escucha para las solicitudes entrantes de FTP.
22	SFTP	TCP	Entrante	Permite notificaciones de alerta mediante SFTP (FTP por medio de SSH). SFTP es un protocolo de cliente/servidor. Los usuarios pueden usar SFTP para realizar transferencias de archivos en un dispositivo en la subred local. También proporciona control de la conexión del FTP saliente. Si está cerrado, el FTP no estará disponible.
53	DNS	TCP/UDP	Saliente	Se utiliza para transmitir consultas de DNS al servidor DNS. Si está cerrado, la resolución de nombres de DNS no funcionará. Se requiere para SMB v1.
88	Kerberos	TCP/UDP	Saliente	Se requiere para los servicios de autenticación de Kerberos.
111	Enlace RPC (para espacios de nombres de SDNAS; de lo contrario, servicio de host)	TCP/UDP	Bidireccional	Lo abre el servicio portmapper o rpcbind estándar, y es un servicio de red auxiliar del dispositivo. No puede detenerse. Por definición, si un sistema cliente cuenta con conectividad de red al puerto, puede consultarlo. No se realiza ninguna acción de autenticación.
123	NTP	UDP	Saliente	Sincronización horaria de NTP. Si está cerrado, la hora no se sincronizará entre los dispositivos.

Tabla 3. Puertos de red del dispositivo relacionados con archivos (continuación)

Puerto	Servicio	Protocolo	Dirección de acceso	Descripción
135	RPC de Microsoft	TCP	Entrante	Múltiples usos para cliente de Microsoft. También se utiliza para NDMP.
137	WINS para NetBIOS de Microsoft	UDP; TCP/UDP	Entrante; saliente	El servicio de nombres de NetBIOS está asociado a los servicios de uso compartido de archivos SMB del dispositivo y es un componente principal de esa función (Wins). Si está deshabilitado, este puerto deshabilita todos los servicios relacionados con SMB.
138	BROWSE de Microsoft para NetBIOS	UDP	Saliente	El servicio de datagramas de NetBIOS está asociado a los servicios de uso compartido de archivos SMB del dispositivo y es un componente principal de esa función. Solo se usa el servicio de navegación. Si está deshabilitado, el puerto deshabilita la funcionalidad de navegación.
139	CIFS de Microsoft	TCP	Bidireccional	El servicio de sesiones de NetBIOS está asociado a los servicios de uso compartido de archivos SMB del dispositivo y es un componente principal de esa funcionalidad. Si están habilitados los servicios de SMB, este puerto está abierto. Se requiere específicamente para SMB v1.
389	LDAP	TCP/UDP	Saliente	Consultas de LDAP no seguras. Si está cerrado, no estarán disponibles las consultas de autenticación LDAP no seguras. El protocolo LDAP seguro es configurable como alternativa.
445	SMB de Microsoft	TCP	Entrante	Se ofrece SMB (en controladoras de dominio) y puerto de conectividad SMB para clientes con Windows 2000 o posteriores. Los clientes con acceso legítimo a los servicios de SMB del dispositivo deben contar con conectividad de red al puerto para su funcionamiento continuo. La deshabilitación de este puerto deshabilita todos los servicios relacionados con SMB. Si el puerto 139 también está deshabilitado, se deshabilita el uso compartido de archivos SMB.
464	Kerberos	TCP/UDP	Saliente	Se requiere para los servicios de autenticación de Kerberos y SMB.
500	IPsec (IKEv2)	UDP	Bidireccional	Para hacer que IPsec funcione a través de los firewalls, abra el puerto UDP 500 y permita los números de protocolo IP 50 y 51 en los filtros de firewall entrantes y salientes. El puerto UDP 500 se debe abrir para permitir que el tráfico de Internet Security Association and Key Management Protocol (ISAKMP) se reenvíe a través de los firewalls. El ID de protocolo IP 50 se debe configurar para permitir el reenvío del tráfico de IPsec Encapsulating Security Protocol (ESP). El ID de protocolo IP 51 se debe configurar para permitir el reenvío del tráfico del encabezado de autenticación (AH). Si está cerrado, la

Tabla 3. Puertos de red del dispositivo relacionados con archivos (continuación)

Puerto	Servicio	Protocolo	Dirección de acceso	Descripción
				conexión IPsec entre los dispositivos PowerStore no estará disponible.
636	LDAPS	TCP/UDP	Saliente	Consultas de LDAP seguras. Si está cerrado, no estarán disponibles las consultas de autenticación LDAP seguras.
1234	mountd de NFS	TCP/UDP	Bidireccional	Se utiliza para el servicio de montaje, que es un componente principal del servicio de NFS (versiones 2, 3 y 4).
2000	SSHD	TCP	Entrante	SSHD para facilidad de reparación (opcional)
2049	I/O de NFS	TCP/UDP	Bidireccional	Se utiliza para proporcionar servicios NFS.
3268	LDAP	UDP	Saliente	Consultas de LDAP no seguras. Si está cerrado, no estarán disponibles las consultas de autenticación LDAP no seguras.
4000	STATD para NFSv3	TCP/UDP	Bidireccional	Se utiliza para proporcionar servicios statd de NFS. statd es el monitor de estado de bloqueo de archivos NFS y funciona junto con lockd para proporcionar funciones de falla y recuperación para NFS. Si está cerrado, no están disponibles los servicios statd de NAS.
4001	NLMD para NFSv3	TCP/UDP	Bidireccional	Se utiliza para proporcionar servicios lockd de NFS. lockd es el demonio de bloqueo de archivos NFS. Procesa solicitudes de bloqueo de clientes de NFS y funciona junto con el demonio statd. Si está cerrado, no están disponibles los servicios lockd de NAS.
4002	RQUOTAD para NFSv3	TCP/UDP; UDP	Entrante; saliente	Se utiliza para proporcionar servicios rquotad de NFS. El demonio rquotad proporciona información de cuotas a los clientes de NFS que han montado un sistema de archivos. Si está cerrado, no están disponibles los servicios rquotad de NAS.
4003	XATTRPD (atributo de archivo extendido)	TCP/UDP	Entrante	Se requiere para la administración de atributos de archivos en un entorno multiprotocolo.
4658	PAX (archivo del servidor NAS)	TCP	Entrante	PAX es un protocolo de archivos de dispositivo que funciona con formatos de cinta UNIX estándares.
8888	RCPD (ruta de datos de replicación)	TCP	Entrante	Lo utiliza el replicador (en el lado secundario). El replicador lo mantiene abierto tan pronto como advierte la existencia de datos que deben replicarse. Una vez que se inicia, no hay manera de detener el servicio.
10000	NDMP	TCP	Entrante	• Permite controlar el respaldo y la recuperación de un servidor del protocolo de administración de datos de red (NDMP) por medio de una aplicación de respaldo en red, sin instalar software de otros fabricantes en el servidor. En un dispositivo, el servidor NAS funciona como servidor NDMP.

Tabla 3. Puertos de red del dispositivo relacionados con archivos (continuación)

Puerto	Servicio	Protocolo	Dirección de acceso	Descripción
				• El servicio NDMP puede deshabilitarse si no se utiliza el respaldo en cinta de NDMP. • El servicio NDMP se autentica con un nombre de usuario y una contraseña. El nombre de usuario puede configurarse. La documentación de NDMP describe cómo configurar la contraseña para distintos ambientes.
[10500,10531]	Rango reservado de NDMP para puertos dinámicos de NDMP	TCP	Entrante	En las sesiones de respaldo o restauración de tres vías, los servidores NAS utilizan del puerto 10500 al puerto 10531.
12228	Servicio del programa antivirus	TCP	Saliente	Se requiere para el servicio del programa antivirus.

Puertos de red relacionados con los dispositivos modelo X de PowerStore

En la siguiente tabla se describe el conjunto de puertos de red y los servicios correspondientes que se pueden encontrar en dispositivos PowerStore X model.

Tabla 4. Puertos de red relacionados con los dispositivos PowerStore X model

Puerto	Servicio	Protocolo	Dirección de acceso	Descripción
22	Servidor de SSH	TCP	Entrante	Permite el acceso mediante el protocolo SSH (si está habilitado). Si está cerrado, las conexiones de administración por medio de SSH no estarán disponibles.
80 y 9000	vSphere Web Access	TCP	Entrante	Acceso para el plug-in de vSphere Update Manager Web Client para vSphere Web Client.
427	Protocolo de ubicación de servicios (SLP) de CIM	TCP/UDP	Bidireccional	El cliente de CIM utiliza el protocolo de ubicación de servicios versión 2 (SLPv2) para buscar servidores de CIM.
443	vSphere Web Client	TCP	Entrante	Se utiliza para las conexiones de clientes.
902	Copia de archivos de red (NFC), VMware vCenter y vSphere Web Client	TCP	• Bidireccional para NFC • Saliente para VMware vCenter • Entrante para vSphere Web Client	• NFC proporciona un servicio FTP con reconocimiento del tipo de archivo para componentes de vSphere. De manera predeterminada, ESXi utiliza NFC para operaciones como copia y transferencia de datos entre almacenes de datos. • Agente de VMware vCenter • Para vSphere Web Client, se utiliza para las conexiones de clientes.
5900, 5901, 5902, 5903 y 5904	Protocolo RFB	TCP	Entrante	Acceso remoto a interfaces gráficas de usuario, como VNC.
5988	Servidor de Common Information Model (CIM)	TCP	Entrante	Servidor para CIM.

Tabla 4. Puertos de red relacionados con los dispositivos PowerStore X model (continuación)

Puerto	Servicio	Protocolo	Dirección de acceso	Descripción
5989	Servidor de CIM seguro	TCP	Entrante	Servidor para CIM.
6999	Enrutador lógico distribuido virtual de NSX, rabbitmqproxy	UDP	• Bidireccional para el servicio de enrutador distribuido virtual de NSX • Saliente para rabbitmqproxy	• Para el servicio de enrutador distribuido virtual de NSX, el puerto del firewall asociado a este servicio se abre cuando se instalan VIB de NSX y se crea el módulo VDR. Si no hay ninguna instancia de VDR asociada al host, no es necesario que el puerto esté abierto. • Para rabbitmqproxy, un proxy que se ejecuta en el host ESXi. Este proxy permite que las aplicaciones que se ejecutan dentro de máquinas virtuales se comuniquen con los intermediadores de AMQP que se ejecutan en el dominio de red de vCenter. No es necesario que la máquina virtual esté en la red, es decir, no se requiere ninguna NIC. Asegúrese de que las direcciones IP de la conexión saliente incluyan al menos los intermediadores en uso o futuros. Puede agregar intermediadores más adelante para realizar un escalamiento vertical.
8000	vMotion	TCP	Bidireccional	Se requiere para la migración de máquinas virtuales con vMotion. Los hosts ESXi escuchan en el puerto 8000 las conexiones TCP desde hosts ESXi remotos para el tráfico de vMotion.
8100, 8200 y 8300	Tolerancia a fallas	TCP/UDP	Bidireccional	Se utiliza para el tráfico entre hosts para vSphere Fault Tolerance (FT).
8301 y 8302	DVSSync	UDP	Bidireccional	Los puertos DVSSync se utilizan para sincronizar los estados de los puertos virtuales distribuidos entre los hosts que tienen habilitada la grabación/reproducción de VMware FT. Solamente los hosts en los que se ejecutan máquinas virtuales principales o de respaldo deben tener estos puertos abiertos. En los hosts que no usan VMware FT, no es necesario que estos puertos estén abiertos.
9080	Filtro de I/O	TCP	Saliente	Lo utiliza la función de almacenamiento de filtros de I/O.
31031	vSphere Replication y VMware Site Recovery Manager	TCP	Saliente	vSphere Replication y VMware Site Recovery Manager lo utilizan para el tráfico de replicación continuo.
44046	vSphere Replication y VMware Site Recovery Manager	TCP	Saliente	vSphere Replication y VMware Site Recovery Manager lo utilizan para el tráfico de replicación continuo.

3

Auditoría

Este capítulo contiene la siguiente información:

Temas:

Auditoría

La auditoría proporciona una vista histórica de la actividad de los usuarios en el sistema. Un usuario con la función de administrador, administrador de seguridad o administrador de almacenamiento puede usar la API REST para buscar y ver eventos de cambio en la configuración en el sistema. Estos eventos que se auditan no se relacionan únicamente con la seguridad; todas las operaciones de configuración (es decir, POST/PATCH/DELETE) se registran en la auditoría.

Se pueden utilizar otras interfaces, como la interfaz de usuario y la CLI de PowerStore Manager, para buscar y ver eventos de auditoría.

4

Configuración de la seguridad de datos

Esta sección contiene los siguientes temas:

Temas:

Cifrado de datos en reposo

El cifrado de datos en reposo (D@RE) en PowerStore utiliza unidades de autocifrado (SED) con validación de FIPS 140-2 para el almacenamiento primario (SSD NVMe, SCM NVMe y SSD SAS). El dispositivo de almacenamiento en caché NVRAM está cifrado, pero no tiene validación de FIPS 140-2 en este momento.

El cifrado se realiza dentro de cada unidad antes de que los datos se escriban en los medios. Esto protege los datos de la unidad contra robo o pérdida e intentos por leer la unidad directamente mediante su desmontaje físico. El cifrado también proporciona un medio para borrar de manera rápida y segura la información de una unidad con el fin de asegurarse de que no se pueda recuperar. Además de brindar protección contra amenazas relacionadas con la extracción física de los medios, puede replanificarlos fácilmente destruyendo la clave de cifrado utilizada para proteger los datos almacenados anteriormente en ellos.

La lectura de datos cifrados requiere la clave de autenticación para la SED a fin de desbloquear la unidad. Solamente las SED autenticadas se desbloquearán y estarán accesibles. Una vez que se desbloquea la unidad, la SED descifra los datos cifrados y estos vuelven a su forma original.

El dispositivo PowerStore debe contener todas las SED. Si intenta agregar una unidad que no es de autocifrado a un dispositivo, este genera un error. Además, no se admite el uso de dispositivos sin cifrar en un clúster cifrado.

Activación del cifrado

La función de cifrado de datos en reposo en los dispositivos PowerStore se configura en la fábrica. En todos los países que permiten la importación de un dispositivo compatible con el cifrado, el cifrado está habilitado de manera predeterminada. Una vez habilitado, el cifrado no se puede deshabilitar. En todos los países que no permiten la importación de un dispositivo compatible con el cifrado, la función de cifrado de datos en reposo está deshabilitada.

NOTA: Los dispositivos que no admiten el cifrado de datos en reposo no se pueden agrupar en clústeres con dispositivos cifrados.

Estado de cifrado

El estado de cifrado de un dispositivo se informa en los siguientes niveles:

- Nivel del clúster
- Nivel del dispositivo
- Nivel de las unidades

El estado de cifrado en el nivel del clúster refleja simplemente si un dispositivo está habilitado para el cifrado. No está relacionado con el estado de las unidades.

El estado de cifrado de un dispositivo aparece como uno de los siguientes:

- Encrypted: la funcionalidad de cifrado está habilitada en el dispositivo.
- Unencrypted: la funcionalidad de cifrado no es compatible con el dispositivo.
- Encrypting: aparece durante el proceso de activación del cifrado. Cuando el proceso de cifrado se completa correctamente, el estado de cifrado en el nivel del clúster aparece como cifrado.

El estado de cifrado en el nivel de las unidades se proporciona para cada unidad de un dispositivo y aparece como uno de los siguientes:

- Encrypted: la unidad está cifrada. Este es el estado típico de una unidad en un dispositivo que admite el cifrado.
- Encrypting: el dispositivo está habilitando el cifrado en la unidad. Este estado se puede ver durante la activación inicial del cifrado en un dispositivo o durante la adición de unidades nuevas a un dispositivo configurado.
- Disabled: el cifrado no se puede habilitar en la unidad debido a restricciones de importación específicas del país. Si alguna unidad informa este estado, todas las unidades del clúster también lo informarán.
- Unknown: el dispositivo aún no intenta habilitar el cifrado en la unidad. Este estado se puede ver durante la activación inicial del cifrado en un dispositivo o durante la adición de unidades nuevas a un dispositivo configurado.
- Unsupported: la unidad no es compatible con el cifrado.
- Foreign: la unidad es compatible, pero otro dispositivo la bloqueó. Se debe retirar del servicio antes de que se pueda usar.

Administración de claves

En el nodo activo de cada dispositivo PowerStore se ejecuta un servicio de administrador de claves (KMS) integrado. Este servicio administra el almacenamiento de la caja de seguridad de los archivos del almacenamiento de claves local para admitir el respaldo automático de claves de cifrado en unidades del sistema y de arranque. También controla el proceso de bloqueo y desbloqueo de las unidades de autocifrado (SED) en el dispositivo y es responsable de administrar el contenido del almacenamiento de claves local para el dispositivo. El archivo del almacenamiento de claves local está cifrado con una clave AES de 256 bits y el almacenamiento de la caja de seguridad de los archivos del almacenamiento de claves aprovecha la tecnología BSAFE de RSA.

El KMS genera automáticamente una clave de autenticación aleatoria para las SED durante la inicialización del dispositivo. Cada unidad tiene una clave de autenticación única, incluidas las que se agregan al dispositivo más adelante, que se utiliza en los procesos de bloqueo y desbloqueo de SED. Una clave de cifrado de claves cifra las claves de autenticación y cifrado en el almacenamiento de archivos del almacenamiento de claves y en transferencia dentro del dispositivo. Las claves de cifrado de medios se almacenan en el hardware dedicado de las SED y no se puede acceder a ellas. Cuando el cifrado está habilitado, todas las claves de autenticación se almacenan en el dispositivo.

Archivo de respaldo del almacenamiento de claves

El KMS admite la creación y la descarga de un respaldo fuera del dispositivo del archivo del almacenamiento de claves. El respaldo fuera del dispositivo reduce la posibilidad de una pérdida de claves catastrófica, la que dejaría inutilizables a un dispositivo o a un clúster. Si un dispositivo específico no está disponible cuando se inicia el respaldo del almacenamiento de claves de un clúster, la operación general se realizará correctamente, pero se emitirá una advertencia que indica que el respaldo no contiene los archivos del almacenamiento de claves para todos los dispositivos del clúster y que la operación se debe reintentar cuando el dispositivo offline esté disponible.

NOTA: El dispositivo primario en un clúster contiene un archivo del almacenamiento de claves del clúster que incluye una copia de los respaldos del almacenamiento de claves de cada dispositivo que se descubre en el clúster, entre ellos el dispositivo primario.

Cuando se producen cambios en la configuración de un sistema dentro del clúster que dan lugar a cambios en el almacenamiento de claves, se recomienda generar un nuevo archivo de almacenamiento de claves para descarga. Solamente se puede ejecutar una operación de descarga de respaldo del archivo del almacenamiento de claves a la vez.

NOTA: Se recomienda descargar el archivo del almacenamiento de claves generado a una ubicación externa segura. Si los archivos del almacenamiento de claves de un sistema se dañan y quedan inaccesibles, el sistema ingresará al modo de servicio. Para solucionar esto, se requieren el archivo del almacenamiento de claves y la contratación de un servicio.

Para respaldar el archivo del almacenamiento de claves se requiere la función de usuario administrador o administrador de almacenamiento. Para respaldar el archivo del almacenamiento de claves, haga clic en **Settings** y, bajo **Security**, seleccione **Encryption**. En la página **Encryption**, bajo **Lockbox backup**, haga clic en **Download Keystore Backup**.

NOTA: Para restaurar el respaldo del almacenamiento de claves en caso de que se produzca una falla, póngase en contacto con el proveedor de servicio.

Replanificar una unidad en un dispositivo con el cifrado habilitado

Sobre esta tarea

Una unidad de autocifrado (SED) se bloquea cuando se inicializa un dispositivo o cuando se inserta en un dispositivo ya inicializado. La unidad no se puede utilizar en otro sistema sin que antes de desbloquee. La unidad bloqueada se vuelve inutilizable cuando se inserta en un dispositivo diferente y su estado de cifrado aparece como `Foreign` en el nuevo dispositivo. La unidad se puede replanificar para el nuevo dispositivo; sin embargo, se perderán todos los datos existentes en ella.

Para replanificar una unidad que tenga un estado de cifrado de `Foreign` en un dispositivo, realice lo siguiente:

Pasos

1. Registre el PSID (ID de seguridad física) que se encuentra en la etiqueta de la parte posterior de la unidad. El PSID se debe proporcionar como parte del proceso de replanificación.
2. En PowerStore Manager, haga clic en **Hardware**, seleccione el dispositivo y seleccione la tarjeta **Hardware**.
3. Seleccione la unidad que desea replanificar.
   El valor de **Encryption Status** para la unidad debe aparecer como `Foreign`.
4. Haga clic en **Repurpose Drive**.
   Aparece el menú deslizante **Repurpose Drive**.
5. Escriba el PSID de la unidad y haga clic en **Apply**.

Resultados

La unidad se replanifica en el dispositivo como una nueva unidad y su estado de cifrado cambia a `Encrypted` al finalizar el proceso de replanificación.

Reemplazo de un gabinete base y nodos en un sistema en el que está habilitado el cifrado

Se requiere una contratación de servicio para reemplazar un base enclosure y nodes en un dispositivo en el que está habilitado el cifrado.

Restablecimiento de un dispositivo a los ajustes de fábrica

Un script de servicio, `svc_factory_reset`, devuelve un único clúster de dispositivos al estado como se entregó de fábrica, con lo cual se eliminan todos los datos de usuario y las configuraciones persistentes.

Para los clústeres de múltiples dispositivos, `svc_factory_reset` no se puede ejecutar en los dispositivos secundarios. En su lugar, se debe ejecutar el script de servicio `svc_remove_appliance`. Este script hace que el dispositivo secundario vuelva al estado como se entregó de fábrica, con lo cual se eliminan todos los datos de usuario y las configuraciones persistentes. Cuando solamente el dispositivo primario permanece en el clúster, puede ejecutar `svc_factory_reset` para restablecer ese dispositivo.

NOTA: Se recomienda que solamente un proveedor de servicios calificado ejecute estos scripts.

Para obtener más información sobre estos scripts, consulte *PowerStore Service Scripts Guide*.

5

Configuración de facilidad de reparación segura

Este capítulo contiene la siguiente información:

Temas:

Descripción operacional de SupportAssist™

La función SupportAssist proporciona una conexión basada en IP que permite al soporte de Dell EMC recibir archivos de error y alertas desde el dispositivo, además de realizar tareas remotas de solución de problemas en un tiempo de resolución rápido y eficiente.

NOTA: Se recomienda enfáticamente habilitar la función SupportAssist para agilizar el diagnóstico de problemas, realizar tareas de solución de problemas y acelerar el tiempo de resolución. Si no habilita la función SupportAssist, es posible que deba recolectar manualmente información del dispositivo para apoyar al soporte de Dell EMC en la solución de problemas de este. Además, la función SupportAssist se debe habilitar en el dispositivo para que se envíen datos a CloudIQ. Para obtener información sobre CloudIQ, visite www.dell.com/support. Después de iniciar sesión, busque la página **Product Support** de CloudIQ.

SupportAssist y seguridad

La función SupportAssist emplea varias capas de seguridad en cada paso del proceso de conectividad remota para asegurarse de que usted y Dell EMC puedan usar la solución con confianza:

- Todas las notificaciones a Dell EMC se originan desde su sitio, nunca desde un origen externo, y se mantienen seguras gracias al uso del cifrado de estándar de cifrado avanzado (AES) de 256 bits.
- La arquitectura basada en IP se integra a la infraestructura existente y mantiene la seguridad de su ambiente.
- Las comunicaciones entre su sitio y Dell EMC se autentican de manera bilateral mediante certificados digitales de RSA®.
- Solamente los profesionales de servicio al cliente de Dell EMC autorizados y verificados mediante una autenticación de doble factor pueden descargar los certificados digitales necesarios para ver una notificación desde su sitio.
- La aplicación opcional de administrador de políticas de SupportAssist v3 permite otorgar o restringir el acceso del soporte de Dell EMC en función de sus propios requisitos y reglas únicos, e incluye un registro de auditoría detallado.

Administración de SupportAssist

Puede administrar la función SupportAssist mediante PowerStore Manager o la API REST. Puede habilitar o deshabilitar el servicio y proporcionar la información pertinente necesaria para la opción de SupportAssist que seleccione.

NOTA: Las opciones **Gateway Connect with remote assist** y **Gateway Connect without remote assist** para SupportAssist centralizado no admiten la alta disponibilidad (HA). Estas opciones no proporcionan una funcionalidad de conmutación por error a un clúster de SupportAssist de HA activo. Cuando un dispositivo PowerStore se implementa en un único servidor de clúster de gateway de HA, que es la única opción de configuración, no hay ninguna funcionalidad de conmutación por error al servidor de gateway

sobreviviente en el clúster. Si el servidor de gateway de HA al cual está conectado el dispositivo queda inactivo, el dispositivo dejará de transferir archivos salientes, como archivos de CloudIQ y Call Home, al soporte de Dell EMC. La conectividad entrante de SupportAssist para el acceso remoto al dispositivo continuará funcionando mediante el servidor de gateway de HA sobreviviente del clúster. Además, las opciones **Gateway Connect with remote assist** y **Gateway Connect without remote assist** de SupportAssist se deben configurar solamente en el dispositivo primario designado del sistema.

El propio dispositivo no implementa ninguna política. Si necesita un mayor control sobre el acceso remoto al dispositivo, puede usar un administrador de políticas para configurar permisos de autorización. El componente de software de administrador de políticas se puede instalar en un servidor suministrado por el cliente. Controla el acceso remoto a sus dispositivos, mantiene un registro de auditoría de las conexiones remotas y es compatible con operaciones de transferencia de archivos. Puede controlar quién accede al dispositivo, qué clase de acceso es y cuándo se produce. Para obtener más información sobre el administrador de políticas, visite www.dell.com/support. Después de iniciar sesión, busque la página **Support by Product** correspondiente y el enlace a la documentación técnica específica del producto SupportAssist.

Comunicación de SupportAssist

NOTA: SupportAssist no se puede habilitar en los modelos de PowerStore configurados con IPv6 para la red de administración. SupportAssist no es compatible a través de IPv6. Además, no se permite la reconfiguración de la red de administración IPv4 a IPv6 cuando SupportAssist está configurado en un clúster.

Para que la función SupportAssist funcione, se requiere acceso a un servidor DNS.

En **Connection Status** de SupportAssist se indica tanto el estado de la conexión entre PowerStore y los servicios de soporte de back-end de Dell EMC como la calidad de servicio de la conexión. El estado de la conexión se determina en períodos de cinco minutos y la calidad de servicio de la conexión, en períodos de 24 horas. La información de **Connection Status** para la conexión puede corresponder a uno de los siguientes valores en función de cualquiera de los dispositivos del clúster:

- `Unavailable` : los datos de conectividad no están disponibles. Es posible que haya perdido contacto con un dispositivo o que SupportAssist se haya habilitado y que no haya datos suficientes para determinar el estado.
- `Disabled` : SupportAssist no se ha habilitado.
- `Not connected` : la conectividad se perdió. Se detectaron cinco fallas consecutivas de Keepalive.
- `Reconnecting` : PowerStore está intentando volver a conectarse después de la pérdida de conectividad. Se necesitan cinco solicitudes correctas consecutivas de Keepalive para realizar la transición nuevamente a un estado conectado.

La información de **Connection Status** de la conexión puede aparecer como uno de los siguientes valores en función del promedio de todos los dispositivos del clúster cuando PowerStore está conectado a los servicios de soporte de back-end de Dell EMC:

- `Evaluating` : la calidad de servicio de la conexión será indeterminada durante las primeras 24 horas después de la primera inicialización de SupportAssist.
- `Good` : el 80 % o más de las solicitudes Keepalive consecutivas se realizó correctamente.
- `Fair` : entre el 50 % y el 80 % de las solicitudes Keepalive consecutivas se realizó correctamente.
- `Poor` : menos del 50 % de las solicitudes Keepalive consecutivas se realizó correctamente.

Opciones de SupportAssist

La función SupportAssist proporciona una conexión basada en IP que permite al soporte de Dell EMC recibir archivos de error y alertas desde el sistema, además de realizar tareas remotas de solución de problemas en un tiempo de resolución rápido y eficiente.

Las opciones de SupportAssist que están disponibles, mediante las cuales se envía información del dispositivo al soporte de Dell EMC para la solución de problemas remota, son las siguientes:

- Gateway Connect without remote access: para SupportAssist centralizado; se ejecuta en un servidor de gateway suministrado por el cliente con transferencia de archivos bidireccional que incluye lo siguiente:
  - Call Home
  - Compatibilidad con CloudIQ
  - Notificaciones de software
  - Descarga del entorno operativo/firmware desde el soporte de Dell EMC al clúster

  El servidor de gateway de SupportAssist es el punto único de entrada y salida de todas las actividades de SupportAssist basadas en IP para los dispositivos asociados con el gateway.

- Gateway Connect with remote access: para SupportAssist centralizado; se ejecuta en un servidor de gateway suministrado por el cliente con la misma transferencia de archivos bidireccional que Gateway Connect without remote access, y con acceso remoto para el personal de soporte de Dell EMC.
- Direct Connect without remote access: para SupportAssist distribuido que se ejecuta en dispositivos individuales con la misma transferencia de archivos bidireccional que Gateway Connect without remote access.
- Direct Connect with remote access: para SupportAssist distribuido que se ejecuta en dispositivos individuales con la misma transferencia de archivos bidireccional que Gateway Connect without remote access, y con acceso remoto para el personal de soporte de Dell EMC.

Está disponible otra opción, Disabled, pero no se recomienda. Si selecciona esta opción, el soporte de Dell EMC no recibirá notificaciones sobre los problemas del dispositivo. Es posible que deba recolectar manualmente información del dispositivo para apoyar a los representantes de soporte en la solución de problemas.

Opciones de SupportAssist Gateway Connect

SupportAssist Gateway Connect se ejecuta en un servidor de gateway. Cuando selecciona la opción **Gateway Connect without remote access** o la opción **Gateway Connect with remote access**, el dispositivo se agrega a otros dispositivos en un clúster de SupportAssist. El clúster reside detrás de una única conexión segura común (centralizada) entre los servidores de soporte de Dell EMC y el servidor de gateway fuera del arreglo. El servidor de gateway es el punto único de entrada y salida de todas las actividades de Dell EMC SupportAssist basadas en IP para los dispositivos asociados con el gateway.

El servidor de gateway es una aplicación de solución de soporte remoto que se instala en uno o más servidores dedicados que proporciona el cliente. Funciona como un intermediador de comunicación entre los dispositivos asociados y la empresa Dell EMC.

Para obtener más información sobre el gateway de SupportAssist, acceda a la página del producto SupportAssist en el sitio web de soporte de Dell (www.dell.com/support).

Para configurar el dispositivo de modo que utilice la opción **Gateway Connect without remote access** o la opción **Gateway Connect with remote access** para SupportAssist, debe proporcionar la dirección IP y el número de puerto (9443 es el valor predeterminado) del servidor de gateway. Además, asegúrese de que el puerto esté abierto entre el servidor de gateway y el dispositivo.

NOTA: Para usarlo, el servidor de gateway debe estar en funcionamiento antes de que se configure el dispositivo. Los dispositivos se pueden agregar al gateway solamente desde PowerStore Manager. Si el dispositivo se agrega desde el servidor de gateway, aparecerá conectado, pero no enviará correctamente la información del sistema.

Opciones de SupportAssist Direct Connect

SupportAssist Direct Connect se ejecuta directamente en el nodo primario de cada dispositivo. En un clúster, cada dispositivo establecerá su propia conexión al soporte de Dell EMC. El tráfico no se enruta a través del dispositivo primario en un clúster. Sin embargo, SupportAssist se puede administrar solamente en el nivel del clúster, es decir, todos los cambios se aplican a todos los dispositivos del clúster.

Habilite y configure SupportAssist Direct Connect desde la página de **SupportAssist**, a la que se puede acceder a través de **Settings** y que se encuentra bajo **Support** en PowerStore Manager. Estas acciones configuran el dispositivo para usar una conexión segura entre este y el soporte de Dell EMC. Puede seleccionar una de las siguientes opciones de conectividad al servicio remoto para SupportAssist Direct Connect:

- **Direct Connect without remote access**
- **Direct Connect with remote access**

Cuando selecciona la opción **Direct Connect without remote access** y acepta el acuerdo de licencia de usuario final (EULA), se configura una conexión segura entre el dispositivo y el soporte de Dell EMC. Esta opción habilita la funcionalidad de conectividad de transferencia de archivos bidireccional hacia y desde el soporte de Dell EMC. Si corresponde, puede configurar la conexión desde el dispositivo a un servidor proxy asociado (opcional). Si es necesario, puede realizar más adelante una actualización a Direct Connect con el establecimiento de la configuración de acceso remoto.

Cuando selecciona la opción **Direct Connect with Remote Access** y acepta el acuerdo de licencia de usuario final (EULA), se configura una conexión segura entre el dispositivo y el soporte de Dell EMC. Esta opción habilita la funcionalidad de conectividad del servicio de acceso remoto con el dispositivo hacia y desde el soporte de Dell EMC, junto con la transferencia de archivos bidireccional. Si corresponde, puede configurar la conexión desde el dispositivo a un administrador de políticas (opcional) y a cualquier servidor proxy asociado (opcional) a través de PowerStore Manager.

Cuando se agrega un nuevo dispositivo a un clúster existente, el dispositivo detectará los ajustes de SupportAssist del clúster y establecerá automáticamente la configuración según corresponda. Si SupportAssist Direct Connect está habilitado, se habilitará

automáticamente en el nuevo dispositivo. No es necesario realizar acciones adicionales. Si SupportAssist Direct Connect no se puede habilitar, esto no impedirá que el proceso de adición del dispositivo se realice.

Requisitos para SupportAssist Gateway Connect

Los siguientes requisitos se aplican a las implementaciones **Gateway Connect without remote access** y **Gateway Connect with remote access** de SupportAssist:

- El tráfico de red (HTTPS) se debe permitir en el puerto 9443 (o en el puerto que especifica el cliente, si es diferente) entre el dispositivo y el servidor de gateway de SupportAssist.
- La versión de SupportAssist debe ser 4.0.5 o 3.38.

NOTA: Nunca agregue ni quite manualmente un dispositivo desde el servidor de gateway. Agregue o quite un dispositivo de un servidor de gateway únicamente con el asistente de configuración de PowerStore Manager SupportAssist.

Requisitos para SupportAssist Direct Connect

El siguiente requisito se aplica a las implementaciones **Direct Connect without remote access** y **Direct Connect with remote access** de SupportAssist:

- El tráfico de red (HTTPS) se debe permitir en los puertos 443 y 8443 (salientes) hacia el soporte de Dell EMC. Cuando no se puede abrir el puerto 8443, hay un impacto considerable en el rendimiento (entre un 30 y un 45 %). Si no se abren ambos puertos, puede haber una demora en la resolución de problemas relativos al dispositivo final.

El siguiente requisito se aplica solamente a la implementación **Direct Connect with Remote Access** de SupportAssist:

- Si la implementación incluirá un administrador de políticas que brinde un mayor control del acceso remoto al dispositivo, debe indicar esto al configurar la función SupportAssist.

Configuración de SupportAssist

Configure SupportAssist para un dispositivo utilizando cualquiera de los siguientes medios:

- Initial Configuration Wizard: interfaz de usuario que lo guía a través de la configuración inicial de PowerStore Manager y que prepara el sistema para su uso.
- **SupportAssist**: página de ajustes a la que puede acceder desde PowerStore Manager (haga clic en **Settings** y, bajo **Support**, seleccione **SupportAssist**).
- Servidor de API REST: interfaz de aplicaciones que puede recibir solicitudes de la API REST para configurar los ajustes de SupportAssist. Para obtener más información sobre la API REST, consulte PowerStore REST API Reference Guide.

Para determinar el estado de la función SupportAssist, haga clic en **Settings** y, bajo **Support**, seleccione **SupportAssist** en PowerStore Manager.

Configurar SupportAssist

Sobre esta tarea

Para configurar SupportAssist mediante PowerStore Manager, realice lo siguiente:

NOTA: El cambio de la opción **Direct Connect with remote access** a las opciones **Direct Connect without remote access** o **Gateway Connect** requiere la ayuda del personal de soporte de Dell EMC.

Pasos

1. Haga clic en **Settings** y, bajo **Support**, seleccione **SupportAssist**.
2. Si el estado de SupportAssist se muestra como deshabilitado, haga clic en el icono de control de **SupportAssist** para habilitar SupportAssist.

   Aunque la función SupportAssist se puede deshabilitar, esto no se recomienda.

El botón debe desplazarse hacia la derecha y su indicación debe cambiar a `Enabled`. Sin embargo, **Connection Status** no cambiará hasta que se ingrese la información de configuración necesaria y se haga clic en **Apply**.

3. En **SupportAssist**, la casilla de verificación **Connect to CloudIQ** está seleccionada de manera predeterminada. Si no desea enviar archivos a CloudIQ, deseleccione la casilla de verificación. De lo contrario, déjela seleccionada.
4. Seleccione en la lista un valor **Type** para la opción de SupportAssist que desea usar.
5. Según el tipo de opción de SupportAssist que selecciona, realice una de las siguientes acciones:
   - Para las opciones **Gateway Connect without remote access** o **Gateway Connect with remote access**:
     - Especifique la dirección IP del servidor de gateway.
       NOTA: Para usarlo, el servidor de gateway debe estar en funcionamiento antes de que se configure el dispositivo.
     - Si el puerto que se utilizará para conectarse al servidor de gateway es diferente al predeterminado (9443), utilice los controles para seleccionar el número del puerto que se utilizará en la red.
   - Para la opción **Direct Connect without remote access**:
     - Si la conexión de red utiliza un servidor proxy, especifique la dirección IP del servidor proxy.
       NOTA: Para usarlo, el servidor proxy debe estar en funcionamiento antes de que se configure el sistema.
     - Utilice los controles para seleccionar el número del puerto que se utilizará para conectarse al servidor proxy en la red.
   - Para la opción **Direct Connect with Remote Access**:
     - Si la conexión de red utiliza un servidor proxy, especifique la dirección IP del servidor proxy.
       NOTA: Para usarlo, el servidor proxy debe estar en funcionamiento antes de que se configure el dispositivo.
     - Utilice los controles para seleccionar el número del puerto que se utilizará para conectarse al servidor proxy en la red.
     - Si desea utilizar un administrador de políticas para controlar el acceso remoto al sistema, especifique su dirección IP.
       NOTA: Para usarlo, el administrador de políticas debe estar en funcionamiento antes de que se configure el dispositivo.
     - Si el puerto que se utilizará para conectarse al administrador de políticas es diferente al predeterminado (9443), escriba el número del puerto que se utilizará en la red.
6. Según el tipo de opción de SupportAssist que selecciona, realice una de las siguientes acciones:
   - Para las opciones **Direct Connect without remote access** o **Direct Connect with Remote Access**, continúe con el paso siguiente.
   - Para las opciones **Gateway Connect without remote access** o **Gateway Connect with Remote Access**, seleccione **Test Connection** para comprobar el estado de la conexión al servidor de gateway.

   NOTA: Si Connectivity Status parece no salir de `Transitioning` y no cambia después de varios minutos (el tiempo que se debe tardar en probar la conectividad), póngase en contacto con el soporte en línea.
7. Seleccione **Send Test Alert** para enviar una alerta de prueba al soporte de Dell EMC con el fin de verificar la conectividad de punto a punto.
8. Asegúrese de que la información de contacto que se muestra sea precisa. Corrija la información que parezca incorrecta u obsoleta.
   La información de contacto de SupportAssist es fundamental para responder rápidamente a los problemas de soporte y debe ser precisa y actual.
9. Seleccione **Apply** para conservar la información de configuración de SupportAssist.

A

Conjuntos de aplicaciones de cifrado TLS

En este apéndice se incluye la siguiente información:

Temas:

- Conjuntos de cifrado TLS compatibles

Conjuntos de cifrado TLS compatibles

Un conjunto de cifrado define un conjunto de tecnologías que protegen las comunicaciones por el protocolo TLS:

- Algoritmo de intercambio de claves (la manera en que se usa la clave para cifrar los datos que se transmiten del cliente al servidor). Ejemplos: clave de RSA o Diffie-Hellman (DH)
- Método de autenticación (la manera en que los hosts pueden autenticar la identidad de hosts remotos). Ejemplos: certificado de RSA, certificado de DSS o sin autenticación
- Cifrado (la manera en que se cifran los datos). Ejemplos: AES (256 o 128 bits)
- Algoritmo hash (que asegura los datos a través de un método para determinar si se han modificado). Ejemplos: SHA-2 o SHA-1

Los conjuntos de cifrado compatibles combinan todos estos elementos.

En la siguiente lista se proporcionan los nombres de OpenSSL de los conjuntos de cifrado TLS para el dispositivo y los puertos asociados.

Tabla 5. Conjuntos de cifrado TLS predeterminadas/compatibles que admite el dispositivo

Conjuntos de aplicaciones de cifrado	Protocolos	Puertos
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	TLSv1.2	443 y 8443
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	TLSv1.2	443 y 8443
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	TLSv1.2	443 y 8443
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	TLSv1.2	443 y 8443
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	TLSv1.2	443 y 8443
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	TLSv1.2	443 y 8443
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	TLSv1.2	443 y 8443
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	TLSv1.2	443 y 8443
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	TLSv1.2	443 y 8443
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	TLSv1.2	443 y 8443
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	TLSv1.2	443 y 8443
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	TLSv1.2	443 y 8443
TLS_RSA_WITH_AES_128_CBC_SHA	TLSv1.2	443 y 8443
TLS_RSA_WITH_AES_128_CBC_SHA256	TLSv1.2	443 y 8443
TLS_RSA_WITH_AES_128_GCM_SHA256	TLSv1.2	443 y 8443
TLS_RSA_WITH_AES_256_CBC_SHA	TLSv1.2	443 y 8443
TLS_RSA_WITH_AES_256_CBC_SHA256	TLSv1.2	443 y 8443
TLS_RSA_WITH_AES_256_GCM_SHA384	TLSv1.2	443 y 8443