Dell PowerStore

Configuración de NFS

4.3

AVISO: Este contenido se tradujo utilizando inteligencia artificial (IA). Puede contener errores y se proporciona "tal cual" sin ninguna garantía de ningún tipo. Para ver el contenido original (sin traducir), consulte la versión en inglés. Si tiene preguntas o dudas sobre este contenido, comuníquese con Dell en Dell.Translation.Feedback@dell.com.

Diciembre de 2025
Rev. A08

DELL Technologies

Notas, avisos y advertencias

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

PRECAUCIÓN: CAUTION indica la posibilidad de daños en el hardware o la pérdida de datos y le informa cómo evitar el problema.

AVISO: WARNING indica la posibilidad de daños en la propiedad, lesiones 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. Póngase en contacto con el proveedor de servicio si un producto no funciona correctamente o como se describe en este documento.

NOTA: Clientes de Modelo PowerStore X: Para acceder a las guías y los manuales técnicos con los tutoriales más recientes de su modelo, descargue el *Conjunto de documentación de PowerStore 3.2.x* desde la página Documentación PowerStore en dell.com/powerstoredocs.

Dónde obtener ayuda

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

- **Información del producto**: Para acceder a la documentación o las notas de la versión de productos y características, vaya a la página Documentación PowerStore en dell.com/powerstoredocs.
- **Solución de problemas**: para obtener información sobre productos, actualizaciones de software, licenciamiento y servicio, vaya al soporte de Dell y busque la página de soporte del producto correspondiente.
- **Soporte técnico**: Para realizar solicitudes de servicio y de soporte técnico, vaya al Soporte de Dell y busque la página **Solicitudes de servicio**. 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

Descripción general

Este capítulo incluye la siguiente información:

Temas:

Soporte de NFS

Modelo PowerStore T y Modelo PowerStore Q soportan NFSv3 y NFSv4. Estos modelos también soportan un NFS seguro con Kerberos para una autenticación sólida. Aunque Modelo PowerStore T y Modelo PowerStore Q soportan la mayoría de las funcionalidades de NFSv4 y v4.1 descritas en las RFC pertinentes, las delegaciones de directorio y pNFS no son soportadas. En PowerStore 3.0 y versiones posteriores, también está disponible el soporte básico para NFSv4.2 en modo de compatibilidad. A partir de PowerStore la versión 4.3, la compatibilidad con NFSv4.2 se mejoró con funciones adicionales, que incluyen las siguientes:

- Copia dentro del servidor: esta función permite a los clientes solicitar operaciones de copia interna, lo que reduce el tráfico de red innecesario.
- Compatibilidad con archivos dispersos -
  - La operación READ_PLUS puede identificar agujeros (regiones llenas de ceros) en archivos dispersos, lo que elimina la necesidad de transferir datos cero innecesarios y mejora el rendimiento.
  - La operación SEEK permite a los clientes determinar la ubicación de los siguientes datos u orrenos en un archivo.
- NFS etiquetado: esta función permite que el servidor NFS compatible con MAC almacene etiquetas de control de acceso obligatorio (MAC) en los archivos. Luego, las etiquetas se utilizan para aplicar controles de acceso a datos.

La compatibilidad con NFS se habilita en un servidor NAS durante o después de la creación, lo que le permite crear sistemas de archivos habilitados para NFS en ese servidor NAS.

Acerca de NFS seguro

Puede configurar NFS seguro cuando crea o modifica un servidor NAS que es compatible con recursos compartidos de UNIX. NFS seguro proporciona autenticación de usuario basada en Kerberos, que puede proporcionar integridad y privacidad de datos de red.

Kerberos es un servicio de autenticación distribuido diseñado para brindar una autenticación sólida con criptografía de clave secreta. Su funcionamiento se basa en “vales” que permiten que los nodos se comuniquen a través de una red no segura para demostrar su identidad de manera segura. Cuando se configura para actuar como un servidor NFS seguro, el servidor NAS usa la infraestructura de seguridad RPCSEC_GSS y el protocolo de autenticación Kerberos para verificar los usuarios y los servicios.

Opciones de seguridad

NFS seguro es compatible con las siguientes opciones de seguridad:

- krb5: autenticación Kerberos
- krb5i: autenticación Kerberos e integridad de datos mediante la adición de una firma a cada paquete NFS que se transmite a través de la red
- krb5p: autenticación Kerberos, integridad de datos y privacidad de datos mediante el cifrado de los datos antes de su envío a través de la red

  El cifrado de datos requiere más recursos para el procesamiento del sistema y puede causar un rendimiento más lento.

En un ambiente de NFS seguro, el acceso de los usuarios a sistemas de archivos NFS se otorga en función de los nombres entidad de seguridad de Kerberos. Sin embargo, el control de acceso a recursos compartidos dentro de un sistema de archivos se basa en el UID y el GID de UNIX, o en las ACL.

NOTA: NFS seguro admite credenciales de NFS con más de 16 grupos, lo que equivale a la opción de credenciales extendidas de UNIX.

Configuración de NFS seguro

Si está implementando NFS seguro, configure lo siguiente:

- Se debe configurar al menos un servidor NTP en el dispositivo PowerStore para sincronizar la fecha y la hora. Se recomienda configurar un mínimo de dos servidores NTP por dominio para evitar un punto único de falla.
- Un servicio de directorio de UNIX (UDS)
- Uno o más servidores DNS
- Se debe agregar un dominio de AD o personalizado para la autenticación de Kerberos
- Se debe cargar un archivo keytab en el servidor NAS cuando se usa un dominio personalizado en una configuración de Kerberos

Consideraciones de planificación

Revise la siguiente información antes de configurar las exportaciones de NFS:

El soporte del almacenamiento de archivos está disponible solamente en dispositivos Modelo PowerStore T y Modelo PowerStore Q.

Redes de servidores NAS

La creación de redes VLAN y direcciones IP de red es opcional para los servidores NAS. Si piensa crear una VLAN para servidores NAS, esta no se puede compartir con la administración de Modelo PowerStore T y Modelo PowerStore Q ni con redes de almacenamiento. Además, asegúrese de trabajar con el administrador de red para reservar los recursos de red y configurar la red en el switch. Para obtener más información, consulte *Guía de redes T y Q de PowerStore para servicios de almacenamiento*.

Escalabilidad

A partir de PowerStoreOS versión 3.5 y posteriores, hay un límite compartido para los volúmenes de sistemas de archivos y los vVols. La cantidad total de objetos se determina según el límite más alto de los tres tipos de objetos.

Para ver el límite de sistemas de archivos por plataforma, consulte la *Matriz de soporte simple de Dell Technologies PowerStore* en la página Documentación de PowerStore.

Requisitos de implementación

Los servicios de NAS están disponibles solamente en dispositivos Modelo PowerStore T y Modelo PowerStore Q.

Debe haber seleccionado **Unificado** durante la configuración inicial de los dispositivos Modelo PowerStore T y Modelo PowerStore Q. Si seleccionó **Optimizado para bloques** en el Asistente de configuración inicial, los servicios de NAS no se instalaron. Para instalar los servicios de NAS, un representante del soporte técnico debe reinicializar el sistema. Reinicialización del sistema:

- Configura el dispositivo en el estado de fábrica.
- Elimina toda la configuración que se realizó en el sistema a través del **Asistente de configuración inicial**.
- Elimina la configuración que se realizó en PowerStore después de la configuración inicial.

Más consideraciones

Ambos nodos del dispositivo deben estar en funcionamiento para crear un servidor NAS. Si uno de los nodos está inactivo en el dispositivo, no será posible crear un servidor NAS.

Crear la interfaz de red para el tráfico NAS

Puede configurar una red NAS mediante vinculaciones del protocolo de control de adición de enlaces (LACP) o con la creación de una red a prueba de errores para el tráfico de NAS.

Crear vinculaciones LACP para el tráfico NAS

Si los switches están configurados con MC-LAG, puede usar la vinculación de red mediante la creación de un grupo de agregación de enlaces (LAG) para el tráfico NAS.

Cuando los switches de la parte superior del rack (ToR) están configurados con una interconexión MC-LAG, se recomienda configurar la interfaz de NAS a través de vinculaciones LACP con el uso de grupos de agregación de enlaces (LAG). La vinculación LACP es un proceso en el que se combinan dos o más interfaces de red con una sola interfaz. El uso de la vinculación LACP proporciona mejoras de rendimiento y redundancia con el aumento del ancho de banda y el rendimiento de la red. Si una de las interfaces combinadas está inactiva, las otras se usan para mantener una conexión estable.

1. Seleccione **Hardware** > **[dispositivo]** > **Puertos**.
2. En la lista de puertos, seleccione de dos a cuatro puertos de la misma velocidad en el nodo en el que desea agregarlos para la vinculación del protocolo de control de agregación de enlaces (LACP) con el fin de gestionar el tráfico NAS.

   NOTA: La configuración es simétrica en todo el nodo par.

3. Seleccione **Agregación de enlaces** > **Enlaces agregados**.
4. De manera opcional, proporcione una descripción para el vínculo.
5. Seleccione **Agregar**.
6. Desplácese por la lista de puertos y busque el nombre de enlace generado.

   NOTA: Cuando crea el servidor NAS, debe seleccionar el nombre de la vinculación.

Crear una red a prueba de errores

Se debe crear una red a prueba de errores (FSN) cuando los switches de la parte superior del rack (ToR) no se han configurado con una interconexión MC-LAG. Una FSN extiende la conmutación por error de enlaces a la red proporcionando redundancia en el nivel de switches. Una FSN se puede configurar en un puerto, una agregación de enlaces o cualquier combinación de ambos.

1. Seleccione **Hardware** > **[dispositivo]** > **Puertos**.
2. Si planea usar enlaces agregados para la FSN, cree en primer lugar los grupos de agregación de enlaces. Para obtener detalles, consulte Crear vinculaciones LACP para el tráfico NAS.
3. En la lista, seleccione dos puertos o dos agregaciones de enlaces o una combinación de un puerto y un grupo de agregación de enlaces que desee usar para la FSN en el nodo A y, a continuación, seleccione **FSN** > **Crear FSN**.
4. En el panel **Crear FSN**, seleccione los puertos o la agregación de enlaces que se usarán como la red primaria (activa).

   NOTA: El puerto primario no se puede modificar una vez que se utiliza para crear un servidor NAS.

5. De manera opcional, agregue una descripción de la red a prueba de errores.
6. Haga clic en **Crear**.

   PowerStore Manager crea automáticamente un nombre para la red a prueba de errores con el formato: “BaseEnclosure-<Node>-fsn<nextLACPbondcreated>”

   - BaseEnclosure es constante.
   - Node es el nodo que se muestra en la lista **Nodo-Módulo-Nombre**.
   - nextLACPbondcreated es un valor numérico que se determina según el orden en que se creó la vinculación en PowerStore Manager a partir de cero para la primera vinculación creada.

   La primera FSN creada en PowerStore Manager en el nodo A se denominaría BaseEnclosure-NodeA-FSN0.

   La misma FSN se configura en el nodo opuesto. Por ejemplo, si configuró la FSN en el nodo A, entonces se configuraría la misma FSN en el nodo B.

7. Cree un servidor NAS con la red a prueba de errores.

   La red a prueba de errores se aplica al servidor NAS durante la creación de este en PowerStore Manager. Consulte Crear un servidor NAS para los sistemas de archivos NFS.

Creación de exportaciones de NFS

Realice lo siguiente antes de poder crear exportaciones de NFS en PowerStore:

1. Crear servidores NAS con el protocolo NFS

2. Crear un sistema de archivos para las exportaciones de NFS

Recursos de documentación

Consulte lo siguiente para obtener información adicional:

Tabla 1. Recursos de documentación

Documento	Descripción	Ubicación
Guía de redes T y Q de PowerStore para servicios de almacenamiento	En el documento, se proporciona información sobre la planificación y la configuración de la red.	dell.com/powerstoredocs
Guía de configuración de SMB de PowerStore	En el documento, se proporciona información necesaria para configurar recursos compartidos de SMB con PowerStore Manager.	
Documentación técnica Funcionalidades de archivos de PowerStore	En el documento, se analizan las características, la funcionalidad y los protocolos compatibles con la arquitectura de archivos de Dell PowerStore.	
Ayuda en línea de PowerStore	En la ayuda en línea, se proporciona información contextual para la página que se abre en PowerStore Manager.	Integrada en PowerStore Manager

2

Creación de servidores NAS

Este capítulo incluye la siguiente información:

Temas:

Descripción general de la configuración de servidores NAS

Antes de que pueda aprovisionar el almacenamiento de archivos en el sistema de almacenamiento, debe haber un servidor NAS en ejecución en el sistema. Un servidor NAS es un servidor de archivos que utiliza el protocolo SMB, el protocolo NFS o ambos para compartir datos con los hosts de la red. También cataloga, organiza y optimiza las operaciones de lectura y escritura en los sistemas de archivos asociados.

En este documento se describe cómo configurar un servidor NAS con el protocolo NFS, en el cual se pueden crear sistemas de archivos con exportaciones de NFS.

Crear un servidor NAS para los sistemas de archivos NFS

Los servidores NAS se crean antes de crear sistemas de archivos.

Asegúrese de que la información de la red NAS esté disponible.

1. Seleccione **Almacenamiento** > **Servidores NAS**.
2. Seleccione **Crear**.
3. Continúe avanzando en el asistente **Create NAS Server**.

Pantalla del asistente	Descripción
Detalles	• Nombre del servidor NAS • Descripción del servidor NAS • Interfaz de red: seleccione un grupo de agregación de enlaces o una red a prueba de errores (consulte Crear la interfaz de red para el tráfico NAS). **NOTA:** Si selecciona una red a prueba de errores (FSN), la red primaria no se puede modificar una vez que se configura un servidor NAS con el uso de la FSN. • Información de red: dirección IP, máscara de subred, gateway e ID de VLAN **NOTA:** No puede reutilizar las VLAN que se utilizan para las redes de administración y almacenamiento. • Habilitar reflejo de paquetes: las respuestas del servidor se envían de vuelta al host o enrutador de origen, independientemente de la dirección IP de destino, lo que evita las búsquedas de enrutamiento.

Pantalla del asistente	Descripción
	NOTA: Esta opción no se aplica para la comunicación iniciada por el servidor NAS.
Protocolo de uso compartido	**Select Sharing Protocol** Seleccione NFSv3, NFSv4 o ambos. **NOTA:** Si selecciona SMB y un protocolo NFS, habilitará automáticamente el servidor NAS para que soporte el multiprotocolo. Para obtener detalles sobre el uso compartido de archivos multiprotocolo, consulte *la Guía de configuración del uso compartido de archivos multiprotocolo de Dell PowerStore* en la PowerStore página Documentación. **Servicios de directorio de Unix** (servicios de asignación de nombres) Puede configurar los servicios de asignación de nombres con una combinación de archivos locales y NIS o LDAP. Consulte la configuración en las siguientes secciones: ● Uso de archivos locales ● Con NIS ● Con LDAP Puede optar por habilitar un NFS seguro aquí. Un NFS seguro requiere lo siguiente: ● Se debe configurar al menos un servidor NTP en el dispositivo PowerStore para sincronizar la fecha y la hora. Se recomienda configurar un mínimo de dos servidores NTP por dominio para evitar un punto único de falla. ● Un servicio de directorio de UNIX (UDS) ● Uno o más servidores DNS ● Se debe agregar un dominio de AD o personalizado para la autenticación de Kerberos ● Se debe cargar un archivo keytab en el servidor NAS cuando se usa un dominio personalizado en una configuración de Kerberos **DNS** La información del servidor DNS es obligatoria cuando se realiza lo siguiente: ● Unión a un dominio de AD, pero opcional para un servidor NAS independiente. ● Configuración de NFS seguro. El DNS también se puede utilizar para resolver los hosts definidos en las listas de acceso de exportación de NFS.
Política de protección	De manera opcional, seleccione una política de protección en la lista.
Política de QoS de archivos	De manera opcional, seleccione una política QoS de archivos en la lista.
Resumen	Revise el contenido y seleccione **Previous** para regresar y realizar las correcciones que sean necesarias.

4. Seleccione **Create NAS Server** para crear el servidor NAS.
   Se abre la ventana **Status** y se redirige a la página **NAS Servers** una vez que el servidor aparece en la página.

Una vez que haya creado el servidor NAS para NFS, puede continuar con la configuración del servidor.

Si habilitó NFS seguro, debe continuar con la configuración de Kerberos.

Seleccione el servidor NAS para continuar con la configuración o editar los ajustes del servidor NAS.

NOTA: Cuando hay una conexión a un sistema remoto, los cambios en la configuración del servidor NAS pueden tardar hasta 15 minutos en reflejarse en el servidor NAS remoto.

Configurar los servicios de asignación de nombres del servidor NAS

Puede configurar o modificar los servicios de asignación de nombres para un servidor NAS.

Los servicios de asignación de nombres incluyen la configuración de una o más de las siguientes opciones:

- DNS
- NIS para los servicios de directorio de Unix (UDS)
- LDAP para UDS
- Archivos locales

Configurar DNS

Puede deshabilitar DNS o habilitar y configurar un servidor NAS para utilizar DNS.

DNS también se puede utilizar para resolver los hosts definidos en las listas de acceso a exportaciones de NFS.

DNS se requiere para lo siguiente:

- NFS seguro
- Unirse a un dominio de AD.

No puede deshabilitar DNS para los servidores NAS configurados con lo siguiente:

- Uso compartido de archivos multiprotocolo
- Uso compartido de archivos de SMB unido a Active Directory (AD)
- NFS seguro

1. Seleccione **Storage** > **NAS Servers** > **[nas server]** > **DNS**.
2. Habilite o deshabilite DNS. Si habilitó DNS, ingrese la información del servidor DNS.

Configurar el servicio de directorio de UNIX de un servidor NAS mediante NIS

Puede configurar el servicio de directorio de UNIX (UDS) de un servidor NAS mediante NIS.

1. Seleccione la tarjeta **Storage** > **NAS Servers** > **[nas server]** > **Naming Services** > **UDS**.
2. Si **Disabled** está activo, deslice el botón para seleccionar **Enabled**.
3. En el menú desplegable **Unix Directory Service**, seleccione **NIS**.
4. Ingrese un valor de **Domain** de NIS y los valores de **IP Addresses** para los servidores NIS.
5. Seleccione **Aplicar**.

Para solucionar problemas con la configuración de un UDS mediante NIS, asegúrese de que las direcciones IP del servidor y del dominio del servidor NIS ingresadas estén correctas.

Configurar el servicio de directorio de UNIX de un servidor NAS mediante LDAP

Puede configurar el servicio de directorio de UNIX (UDS) de un servidor NAS mediante LDAP.

LDAP debe cumplir los esquemas IDMU, RFC2307 o RFC2307bis. Entre algunos ejemplos se incluyen LDAP de AD con IDMU, iPlanet y OpenLDAP. El servidor LDAP debe estar configurado correctamente para proporcionar UID a cada usuario. Por ejemplo, en IDMU, el administrador debe acceder a las propiedades de cada usuario y agregar un UID a la pestaña Attributes de UNIX.

Puede configurar LDAP para que use autenticación anónima, simple y con Kerberos. Si utiliza autenticación Kerberos, debe configurar lo siguiente antes de continuar configurando LDAP con Kerberos:

1. Desde la tarjeta **Naming Services**, configure el servidor DNS que se utiliza para unir un servidor de Kerberos a un dominio y desunirlo de este.
2. En la tarjeta **Security**, agregue el dominio de Kerberos.

1. Seleccione la tarjeta **Storage** > **NAS Servers** > **[nas server]** > **Naming Services** > **UDS**.
2. Si **Disabled** está activo, deslice el botón para seleccionar **Enabled**.
3. En el menú desplegable **Unix Directory Service** , seleccione **LDAP**.
4. Deje el valor predeterminado o ingrese un valor de **Port Number** diferente.

   NOTA: De forma predeterminada, LDAP utiliza el puerto 389 y LDAP mediante SSL (LDAPS), el puerto 636.

5. Agregue las direcciones IP/FQDN para los servidores LDAP.

   El servidor NAS se puede configurar para usar el descubrimiento de servicios de DNS con el fin de obtener automáticamente las direcciones IP del servidor LDAP.

   NOTA: Para que este proceso de descubrimiento funcione, el servidor DNS debe contener punteros a los servidores LDAP, y los servidores LDAP deben compartir la misma configuración de autenticación.

6. Configure la autenticación de LDAP como se describe en la siguiente tabla:

Opción	Descripción
Anónimo	Especifique el DN base y el DN de perfil del servidor de iPlanet/OpenLDAP.
Simple	Especifique los siguientes elementos: ● Si utiliza AD, LDAP/IDMU: ○ DN de enlace en formato de notación de LDAP; por ejemplo, **cn=administrator,cn=users,dc=svt,dc=lab,dc=com**. ○ DN base, en el formato X.509 (por ejemplo, **dc=svt,dc=lab,dc=com**). ○ DN de perfil. ● Si utiliza el servidor de iPlanet/OpenLDAP: ○ DN de enlace en formato de notación de LDAP; por ejemplo, **cn=administrator,cn=users,dc=svt,dc=lab,dc=com**. ○ Contraseña ○ DN base. Por ejemplo, si usa **svt.lab.com**, el DN base sería **DC=svt,DC=lab,DC=com**. ○ DN de perfil (opcional): para el servidor de iPlanet/OpenLDAP.
Kerberos	Configure un dominio personalizado de modo que se mantenga suspendido sobre cualquier tipo de dominio de Kerberos (Windows, MIT o Heimdal). Con esta opción, el servidor NAS usa el dominio personalizado de Kerberos definido en la subsección Kerberos de la pestaña **Security** del servidor NAS. **NOTA:** Si utiliza un NFS seguro con un dominio personalizado, debe cargar un archivo de pestaña de claves.

7. Haga clic en **Retrieve Current Schema** para descargar el archivo ldap.conf.
8. Edite y guarde el `ldap.conf` archivo.
9. Seleccione **Cargar nuevo esquema** para cargar el archivo actualizado `ldap.conf` .
10. De manera opcional, habilite LDAP seguro (usar SSL) y cargue el certificado de CA.

Para solucionar problemas con la configuración de un UDS mediante LDAP, asegúrese de lo siguiente:

- La configuración de LDAP se adhiere a uno de los esquemas compatibles, como se describió anteriormente.
- Los contenedores que se especifican en el archivo `ldap.conf` se mantienen suspendidos sobre contenedores que son válidos y existen.
- Cada usuario LDAP está configurado con un UID único.

Configurar el servidor NAS para utilizar archivos locales para los servicios de asignación de nombres

Puede configurar los servicios de asignación de nombres para utilizar archivos locales.

- Los archivos locales se pueden utilizar en lugar de los servicios de directorio DNS, LDAP y NIS o también con estos.
- Si configura los archivos locales con un servicio de directorio de UNIX (UDS), el sistema de almacenamiento consulta primero los archivos locales.
- Cuando haya terminado de crear el servidor NFS, puede volver y cargar más archivos locales.
- Una vez que se haya creado el servidor NAS, habilite los archivos locales como se describe en los siguientes pasos:

1. Seleccione **Storage** > **NAS Servers** > **[nas server]** > **Naming Services** > **Local Files**.
2. Para cada tipo de archivo local, seleccione la flecha hacia abajo para descargar el archivo actual. Si no existe ningún archivo en el sistema de almacenamiento, el sistema descarga una plantilla de archivo.
3. Actualice el archivo con la información del sistema.

   Para usar archivos locales para el acceso a FTP, el archivo `passwd` debe incluir una contraseña cifrada para los usuarios. Esta contraseña se utiliza solamente para el acceso a FTP. El archivo `passwd` usa el mismo formato y la misma sintaxis que un sistema UNIX estándar, por lo que puede aplicar la contraseña para generar el archivo `passwd` local. En un sistema UNIX, use `useradd` para agregar un usuario y `passwd` para configurar la contraseña para ese usuario. A continuación, copie la contraseña con hash desde el archivo `/etc/shadow`, agréguela en el segundo campo del archivo `/etc/passwd` y cargue el archivo `/etc/passwd` en el servidor NAS.
4. Guarde el archivo actualizado en su máquina local.
5. Seleccione **Upload Local Files** y busque la ubicación del archivo que editó y seleccione el archivo que desea cargar.
6. Repita este paso para cada tipo de archivo.

Para solucionar problemas con la configuración de los archivos locales, asegúrese de lo siguiente:

- El archivo se crea con la sintaxis correcta. (Se requieren seis dos puntos para cada línea). Haga referencia a la plantilla para obtener información más detallada sobre la sintaxis y ejemplos.
- Cada usuario tiene un nombre y UID únicos.

Configuración de protocolos de uso compartido del servidor NAS

Puede configurar o modificar los protocolos de uso compartido que están configurados para un servidor NAS.

La configuración de protocolos de uso compartido para NFS incluye la configuración de una o más de las siguientes opciones:

- Servidor NFS
- FTP

Configurar el servidor NFS

Configure el servidor NAS para sistemas solamente UNIX o modifique los ajustes del servidor NFS.

Es necesario configurar DNS y NTP antes de configurar un servidor NFS seguro.

1. Seleccione la pestaña **Storage** > **NAS Servers** > **[nas server]** > **Sharing Protocols** > **NFS Server**.
2. Habilite la opción **Linix/UNIX shares** para definir el servidor NAS con fines de compatibilidad con UNIX.
3. Habilite **NFSv3**, **NFSv4** o ambas opciones.
4. De manera opcional, deshabilite o habilite NFS seguro.
   Las credenciales extendidas de UNIX también se habilitan.
5. Seleccione o deseleccione la opción **Enable extended Unix credentials**.

   NOTA: NFS seguro admite credenciales de NFS con más de 16 grupos, lo que equivale a la opción de credenciales extendidas de UNIX.

   - Si se selecciona este campo, el servidor NAS utiliza el ID de usuario (UID) para obtener el ID de grupo (GID) principal y todos los GID de grupo a los que pertenece. El servidor NAS obtiene los GID del archivo de contraseña local o UDS.
   - Si se borra este campo, la credencial de UNIX de la solicitud de NFS se extrae directamente de la información de red que se encuentra en la trama. Este método tiene un mejor rendimiento, pero se limita a incluir solo 16 GID de grupo.
6. En el campo **Credential Cache Retention**, ingrese un período (en minutos) durante el cual las credenciales de acceso se conservan en la caché.
7. Haga clic en **Apply** para aplicar los cambios.

Configurar el protocolo de uso compartido FTP o SFTP

Puede configurar los ajustes de FTP o FTP sobre SSH (SFTP) únicamente para un servidor NAS existente.

FTP en modo pasivo no es compatible.

El acceso a FTP se puede autenticar con los mismos métodos que NFS. Una vez que se completa la autenticación, el acceso es igual que el de NFS con fines de seguridad y permisos. Si el formato es cualquier otro distinto de `user@domain` o `domain\user`, se utiliza la autenticación NFS. La autenticación de NFS utiliza archivos locales, LDAP, NIS o archivos locales con LDAP o NIS.

Para usar archivos locales para NFS y el acceso a FTP, el archivo `passwd` debe incluir una contraseña cifrada para los usuarios. Esta contraseña se utiliza solamente para el acceso a FTP. El archivo `passwd` usa el mismo formato y la misma sintaxis que un sistema Unix estándar, por lo que puede aprovechar esto para generar el archivo `passwd` local. En un sistema Unix, use `useradd` para agregar un nuevo usuario y `passwd` para configurar la contraseña de ese usuario. A continuación, copie la contraseña con hash desde el archivo `/etc/shadow`, agréguela en el segundo campo del archivo `/etc/passwd` y cargue el archivo `/etc/passwd` en el servidor NAS. Consulte Configurar un servidor NAS para usar archivos locales para los servicios de asignación de nombres con el fin de obtener detalles sobre la carga del archivo `/etc/passwd`.

1. Seleccione la pestaña **Storage** > **NAS Servers** > **[nas server]** > **Sharing Protocols** > **FTP**.
2. En **FTP**, si Disabled está activo, deslice el botón para seleccionar **Enable**.
3. De manera opcional, puede habilitar SSH FTP. En **SFTP**, si Disabled está activo, deslice el botón para seleccionar **Enable**.
4. En **FTP/SFTP Server Access**, seleccione el tipo de usuarios autenticados que tienen acceso a los archivos.
5. De manera opcional, muestre las opciones de **Home Directory and Audit**.
   - Seleccione o deseleccione **Home directory restrictions**. Si está desactivado, ingrese el valor de **Default home directory**.
   - Seleccione o deseleccione **Enable FTP/SFTP Auditing**. Si selecciona esta opción, ingrese la ubicación del directorio donde desea guardar los archivos de auditoría y el tamaño máximo permitido para el archivo de auditoría.
6. De manera opcional, seleccione **Show Messages**, e ingrese un valor predeterminado de **Welcome message** y **Message of the day**.
7. De manera opcional, seleccione **Show Access Control List** para proporcionar acceso o denegar el acceso a **Filtered Users**, **Filtered Groups** y **Filtered hosts**.
8. Haga clic en **Aplicar**.

Configurar Kerberos para la seguridad del servidor NAS

Puede configurar el servidor NAS con Kerberos.

Kerberos es un servicio de autenticación distribuido diseñado para brindar una autenticación sólida con criptografía de clave secreta. Su funcionamiento se basa en “vales” que permiten que los nodos se comuniquen a través de una red no segura para demostrar su identidad de manera segura. Cuando se configura para actuar como un servidor NFS seguro, el servidor NAS usa la infraestructura de seguridad RPCSEC_GSS y el protocolo de autenticación Kerberos para verificar los usuarios y los servicios.

Si el servidor NAS se configuró solamente con NFS y está configurando NFS seguro o LDAP con Kerberos, debe configurar Kerberos con un dominio personalizado antes de configurar la seguridad en PowerStore.

Si el servidor NAS se configuró con los protocolos NFS y SMB, tiene la opción de usar el servicio Kerberos heredado con AD, ya que el servidor SMB unido al dominio existe en el servidor NAS.

El sistema de almacenamiento debe estar configurado con un servidor NTP. Kerberos depende de la sincronización de hora correcta entre el KDC, los servidores y el cliente en la red.

Configuración de Kerberos para NFS seguro

Si está configurando Kerberos para NFS seguro, tenga en cuenta lo siguiente:

- Si configura el servidor NAS solamente para NFS, debe hacerlo con un dominio personalizado. Si configuró el servidor NAS con NFS y SMB, puede usar el dominio de AD o personalizado.
- Para un mayor nivel de seguridad, se recomienda usar LDAPS o LDAP con Kerberos.
- Debe haber un servidor DNS configurado en el nivel del servidor NAS. Todos los miembros del dominio Kerberos, incluido el KDC, el servidor NFS y los clientes NFS, deben estar registrados en el servidor DNS.
- El nombre de dominio calificado del nombre de host del cliente NFS y el nombre de dominio calificado del servidor NAS deben estar registrados en el servidor DNS. Los clientes y los servidores deben poder resolver cualquier miembro de los nombres de dominio calificados del dominio Kerberos como una dirección IP.
- La parte del nombre de dominio calificado del SPN del cliente NFS debe estar registrada en el servidor DNS.
- Se debe cargar un archivo keytab en el servidor NAS cuando se configura NFS seguro.

Crear un dominio personalizado para Kerberos

Puede configurar un dominio personalizado para usar con Kerberos.

Un dominio personalizado de Kerberos le permite configurar cualquier tipo de KDC (MIT/Heimdal o AD). Use este método cuando no haya un dominio de servidor SMB configurado en el servidor NAS o si desea usar un dominio de Kerberos distinto del dominio configurado para el servidor SMB.

Crear un dominio personalizado para el servidor NFS puro

Para usar un KDC basado en UNIX, siga estos pasos antes de configurar Kerberos en PowerStore. Los pasos suponen que desea usar myrealm en el dominio de Kerberos linux.dellemc.com como el nombre de host del servidor NFS.

1. Ejecute la herramienta `kadmin.local`.
2. Cree las entidades de seguridad y sus claves:

   ```
   kadmin.local: addprinc -randkey nfs/myrealm.linux.dellemc.com
   ```

   y/o

   ```
   kadmin.local: addprinc -randkey nfs/myrealm
   ```

3. Coloque la clave de la entidad de seguridad en el archivo keytab myrealm.linux.dellemc.fr:

   ```
   kadmin.local: ktadd -k myrealm.linux.dellemc.com.keytab nfs/myrealm.linux.dellemc.fr
   ```

Crear un dominio personalizado para el servidor NAS multiprotocolo (NFS y SMB)

Para usar un KDC basado en Windows sin utilizar la cuenta del servidor SMB en el servidor NAS, siga estos pasos antes de configurar Kerberos en PowerStore. Los pasos suponen que desea usar myrealm.windows.dellemc.com como el nombre de dominio calificado para el servidor NFS.

1. Cree la cuenta myrealm para el servidor NAS en Active Directory (AD) del dominio de Windows windows.dellemc.com.
2. Registre el SPN del servicio en la cuenta de la computadora que creó:

   ```
   C:\setspn -S nfs/myrealm.windows.dellemc.com myrealm
   ```

3. Verifique que el SPN se haya creado.

   ```
   C:\setspn myrealm
   ```

4. Genere un archivo keytab para el SPN:

   ```
   C:\ktpass -princ nfs/myrealm.windows.dellemc.com@WINDOWS.DELLEMC.COM -mapuser
   WINDOWS\myrealm
    -crypto ALL +rndpass -ptype KRB5_NT_PRINCIPAL -out myrealm.windows.dellemc.com.keytab
   ```

Configurar la seguridad de Kerberos para el servidor NAS

Puede configurar el servidor NAS con seguridad de Kerberos.

Si está configurando NFS, DNS y UDS deben estar configurados para el servidor NAS y todos los miembros del dominio de Kerberos deben estar registrados en el servidor DNS.

Si utiliza un servidor NAS configurado para SMB y NFS, asegúrese de agregar el servidor SMB al dominio de AD.

1. Seleccione **Storage** > **NAS Servers** > **[nas server]** > **Security** > **Kerberos**.
2. Si Disabled está activo, deslice el botón para seleccionar **Enabled**.
3. Ingrese un nombre en **Realm**.
4. Ingrese **Kerberos IP Address** y haga clic en **Add**.
5. Ingrese el puerto TCP que utilizará Kerberos. 88 es el puerto predeterminado.
6. Haga clic en **Apply**.

Si decide cambiar de un dominio de AD a un dominio personalizado después de la creación correcta del servidor NAS con NFS seguro, no puede montar ninguna exportación de NFS hasta que realice las siguientes operaciones:

1. Cree un archivo keytab.
2. Elimine el dominio de AD del servidor NAS.
3. Ingrese el nombre de usuario y la contraseña para el servidor de AD.
4. Ingrese el dominio personalizado.
5. Cargue el archivo keytab.

Eliminar un servidor NAS

Para eliminar un servidor NAS, selecciónelo y confirme la eliminación, asegurándose de que no haya sistemas de archivos ni políticas de protección asociados con este.

- Asegúrese de que no haya sistemas de archivos en el servidor.
- Asegúrese de que no haya políticas de protección asociadas con el servidor.

1. Seleccione **Storage** > **NAS Servers** para abrir la lista NAS Servers.
2. En la lista, seleccione la casilla de verificación junto al servidor que desea eliminar.
3. Seleccione **More Actions** > **Delete**.

   NOTA: Si el servidor NAS seleccionado contiene sistemas de archivos o está asociado con una política de protección, la opción Eliminar no está disponible. Si pasa el cursor sobre la opción Eliminar, se muestra el motivo de su desactivación.

4. Seleccione **Eliminar** para confirmar la selección.

Se elimina el servidor NAS seleccionado.

3

Configurar exportaciones de NFS

Este capítulo incluye la siguiente información:

Temas:

Descripción general de los sistemas de archivos y las exportaciones de NFS

Al crear sistemas de archivos y exportaciones de NFS, es útil tener en cuenta lo siguiente:

- Se debe configurar un servidor NAS para soportar el protocolo NFS antes de crear un sistema de archivos.
- Puede optar por agregar exportaciones de NFS la primera vez que crea el sistema de archivos, o puede agregar exportaciones de NFS a un sistema de archivos después de su creación.

Creación de un sistema de archivos para exportaciones de NFS

Puede crear un sistema de archivos para exportaciones de NFS.

Asegúrese de que haya un servidor NAS configurado para soportar el protocolo NFS.

1. Seleccione **Almacenamiento** > **Sistemas de archivos**.
2. Haga clic en **Create**.
   Se inicia el asistente **Create File System**.
3. Seleccione **General** o **Sistema de archivos de VMware** como el tipo de sistema de archivos.

   NOTA: El sistema de archivos de VMware es un sistema de archivos PowerStore optimizado para VMware y utilizado para cargas de trabajo de VMware. Esta opción se debe seleccionar solo para almacenes de datos VMware NFS. Para todos los demás sistemas de archivos, seleccione **General**.

4. Seleccione un servidor NAS habilitado para NFS correspondiente al sistema de archivos.
5. Especifique los detalles del sistema de archivos, incluido el nombre y el tamaño del sistema de archivos, el tamaño mínimo es de 3 GB y el tamaño máximo es de 256 TB.

   NOTA: Todos los sistemas de archivos delgados, independientemente del tamaño, tienen 1,5 GB reservados para metadatos en el momento de la creación. Por ejemplo, después de crear un sistema de archivos delgado de 100 GB, los modelos Modelo PowerStore T y PowerStore Q muestran 1,5 GB utilizados. Cuando el sistema de archivos se monta en un host, muestra 98,5 GB de capacidad útil. Esto se debe a que el espacio de metadatos se reserva de la capacidad útil del sistema de archivos.

6. De manera opcional, seleccione el tipo de retención de archivos (disponible solo para sistemas de archivos generales):
   - Enterprise (FLR-E): protege el contenido de cambios realizados por los usuarios a través de NFS y FTP. Un administrador puede eliminar un sistema de archivos FLR-E que contiene archivos protegidos.
   - Compliance (FLR-C): protege el contenido de cambios realizados por los usuarios y los administradores y cumple con los requisitos de la norma 17a-4(f) de SEC. El sistema de archivos FLR-C se puede eliminar solo cuando no contiene ningún archivo protegido.

   NOTA: El estado de FLR y el tipo de retención de archivos se configuran en la creación del sistema de archivos y no se pueden modificar.

Configure los períodos de retención:

- Mínimo: especifica el período más corto durante el cual se pueden bloquear los archivos (el valor predeterminado es 1 día).
- Predeterminado: se utiliza cuando un archivo se bloquea y no se especifica ningún período de retención.
- Máximo: especifica el período más largo durante el cual se pueden bloquear los archivos.

7. Opcionalmente, configure la exportación inicial para el sistema de archivos.

   NOTA: Puede agregar exportaciones de NFS al sistema de archivos más adelante.

8. Si configuró la exportación inicial, configure el acceso de host.

Opción	Descripción
Minimum Security	Seleccione **Sist.** para permitir que los usuarios con NFS no seguro o seguro realicen montaje y exportación de NFS en el sistema de archivos. Si no planea configurar NFS seguro, debe seleccionar esta opción. Si planea crear un sistema de archivos con NFS seguro, puede elegir entre las siguientes opciones: • **Kerberos** a fin de permitir cualquier tipo de seguridad de Kerberos para la autenticación (krb5/krb5i/krb5p). • **Kerberos con integridad** a fin de permitir ambas opciones de seguridad Kerberos con integridad y Kerberos con cifrado para la autenticación de usuarios (krb5i/krb5p). • **Kerberos con cifrado** a fin de permitir solo la opción de seguridad Kerberos con cifrado para la autenticación de usuarios (krb5p).
Default Access	El tipo de acceso que se aplica a los hosts de manera predeterminada. De manera opcional, puede elegir un tipo diferente de acceso al host cuando agrega hosts individuales. Entre las opciones, se incluyen las siguientes: • **Sin acceso**: no se permite el acceso al recurso de almacenamiento ni al recurso compartido. • **Lectura/escritura**: los hosts tienen permiso para leer y escribir en el recurso compartido o en el almacén de datos de NFS. • **De solo lectura**: los hosts tienen permiso para ver el contenido del recurso de almacenamiento o del recurso compartido, pero no para escribir en ellos. **NOTA:** Los hosts ESXI deben tener acceso de **lectura/escritura** para montar un almacén de datos NFS mediante NFSv4 con autenticación de **propietario de Kerberos NFS**. • **Lectura/escritura, permitir raíz**: los hosts tienen permiso para leer y escribir en el recurso de almacenamiento o en el recurso compartido, así como para otorgar permisos de acceso revocados (por ejemplo, permiso para leer, modificar y ejecutar archivos y directorios específicos) para otras cuentas de inicio de sesión que acceden al almacenamiento. La raíz del cliente NFS tiene acceso raíz al recurso compartido. **NOTA:** A menos que los hosts formen parte de una configuración de clúster compatible, se anula la concesión del acceso de lectura/escritura a más de un host. **NOTA:** Los hosts ESXi deben tener acceso de **Lectura/escritura, permitir raíz** para montar un almacén de datos NFS mediante NFSv4 con autenticación Propietario de NFS: raíz. • **De solo lectura, permitir raíz**: los hosts tienen permiso para ver el contenido del recurso compartido, pero no para escribir en él. La raíz del cliente NFS tiene acceso raíz al recurso compartido.
Agregar host	Ingrese hosts individualmente o puede agregar hosts cargando un archivo CSV con el formato correcto. Puede descargar el archivo CSV primero para obtener una plantilla. Para descargar, editar y usar una plantilla de archivo CSV: a. Haga clic en el icono **Export Hosts**. b. Actualice el archivo CSV con los hosts y los tipos de acceso que desea importar. c. Guarde el archivo CSV en su máquina local. d. Haga clic en **Import CSV file**. e. Busque el archivo CSV y haga clic en **Open** en la ventana del explorador de archivos de Microsoft. Los hosts del archivo CSV aparecen en **Import Host List** con el valor de **Access Type** que definió en el archivo CVS.

9. De manera opcional, agregue una política de protección al sistema de archivos.

   Si va a agregar una política de protección al sistema de archivos, la política debe haberse creado antes de crear el sistema de archivos. La política de protección seleccionada puede incluir reglas de instantáneas y de replicación.

10. De manera opcional, agregue una política de QoS al sistema de archivos.

NOTA: Si la política seleccionada establece un ancho de banda que supera el ancho de banda máximo establecido para el servidor NAS, entonces el ancho de banda efectivo es el ancho de banda máximo del servidor.

11. Revise el resumen y haga clic en **Create File System**.
El sistema de archivos se agrega a la pestaña **File System**. Si creó una exportación simultáneamente, esta se muestra en la pestaña **Exportación NFS**.

Crear una exportación de NFS

Puede crear una exportación de NFS en un sistema de archivos.

1. Seleccione la pestaña **Storage** > **File Systems** > **NFS Export**.
2. Haga clic en **Crear**.
Se inicia el asistente **Create NFS Export**.
3. Ingrese la información solicitada, pero considere lo siguiente:
   - Si desea crear una exportación basada en una instantánea, se deben crear las instantáneas antes de crear la exportación de NFS.
   - El valor de **Local Path** debe corresponder a un nombre de carpeta existente dentro del sistema de archivos que se creó desde el host.
   - Los valores especificados en los campos **Detalles de la exportación de NFS** y **Nombre** junto con la dirección IP del servidor NAS corresponden a la ruta de exportación.

     NOTA: También puede montar la exportación mediante la dirección IP del servidor NAS y la ruta local.

   - Por protocolo, los nombres de exportaciones de NFS deben ser únicos en el nivel del servidor NAS. Sin embargo, puede especificar el mismo nombre para un recurso compartido de SMB y para exportaciones de NFS.
4. Una vez que apruebe los ajustes, haga clic en **Create NFS Export**.
La exportación de NFS se muestra en la página **NFS Export**.

Retención de archivos

La retención en el nivel de archivos (FLR) le permite evitar modificaciones o eliminación de archivos durante un período de retención especificado. La protección de un sistema de archivos mediante FLR permite crear un conjunto de archivos y directorios permanente e inalterable. La FLR garantiza la integridad y la accesibilidad de los datos, simplifica los procedimientos de archivado para los administradores y mejora la flexibilidad de la administración del almacenamiento.

Hay dos tipos de retención en el nivel de archivos:

- Enterprise (FLR-E): protege los datos de cambios realizados por los usuarios y los administradores de almacenamiento mediante SMB, NFS y FTP. Un administrador puede eliminar un sistema de archivos FLR-E que incluye archivos bloqueados.
- Compliance (FLR-C): protege los datos de cambios realizados por los usuarios y los administradores de almacenamiento mediante SMB, NFS y FTP. Un administrador no puede eliminar un sistema de archivos FLR-C que incluye archivos bloqueados. FLR-C cumple con la norma 17a-4(f) de SEC.

Se aplican las siguientes restricciones:

- FLR está disponible en el sistema unificado PowerStore 3.0 o posterior.
- La FLR no se admite en sistemas de archivos VMware.
- La habilitación de FLR para un sistema de archivos y el tipo de FLR se configuran en el momento de la creación del sistema de archivos y no se pueden modificar.
- FLR-C no es compatible con la restauración desde una instantánea.
- Cuando se actualiza mediante una instantánea, ambos sistemas de archivos deben ser del mismo tipo de FLR.
- Cuando se replica un sistema de archivos, los sistemas de archivos de origen y destino deben ser del mismo tipo de FLR.
- Un sistema de archivos clonado tiene el mismo tipo de FLR que el origen (no se puede modificar).

El modo FLR se muestra en la columna **FLR Mode** de la tabla **File Systems** .

Configurar el servidor DHSM

La retención en el nivel de archivos requiere credenciales del servidor DHSM.

El servidor DHSM también es necesario para los hosts de Windows que desean usar FLR y que se requieren para instalar el kit de herramientas de FLR que permite la administración de sistemas de archivos habilitados para FLR.

1. Seleccione **Almacenamiento** > **Servidores NAS** > **[NAS server]** > **Protección** > **DHSM**.
2. Si está deshabilitado, deslice el botón a **Habilitado**.
3. Ingrese el nombre de usuario y la contraseña del servidor DHSM y verifique la contraseña.
4. Seleccione **Aplicar**.

Configurar la retención en el nivel de archivos

La retención en el nivel de archivos se configura en la creación del sistema de archivos. Para obtener más información, consulte Crear sistema de archivos.

NOTA: La retención en el nivel de archivos y su nivel se determinan en la creación del sistema de archivos y no se pueden modificar, pero los parámetros del período de retención sí se pueden modificar.

Modificar retención en el nivel de archivos

Los parámetros del período de retención se pueden configurar en la creación del sistema de archivos o después de esta y se pueden modificar.

NOTA: La modificación de los parámetros del período de retención no afecta a los archivos que ya están bloqueados.

1. Seleccione **Almacenamiento** > **Sistemas de archivos** > **[file system]** > **Seguridad y eventos** > **Retención en el nivel de archivos**.
2. Configure los parámetros del período de retención:
   - Período de retención mínimo: especifica el período más corto durante el cual se puede proteger un sistema de archivos con FLR habilitada (el valor predeterminado es un día).
   - Período de retención predeterminado: se utiliza cuando un archivo está bloqueado y no se especifica un período de retención (el valor predeterminado es un año).
   - Período de retención máximo: especifica el período más largo durante el cual se puede proteger un sistema de archivos con FLR habilitada (el valor predeterminado es infinito).
3. Opcionalmente, configure los ajustes avanzados:
   - Bloqueo automático de archivos: puede especificar si desea bloquear automáticamente los archivos en un sistema de archivos con FLR habilitada y establecer un intervalo de políticas que determine el período entre la modificación de archivos y el bloqueo automático (el valor predeterminado del intervalo de políticas es una hora).
   - Eliminación automática de archivos: puede especificar si desea eliminar automáticamente los archivos bloqueados tras el vencimiento de su período de retención. El primer análisis para localizar archivos a fin de eliminarlos es siete días después de la habilitación de la característica.
4. Seleccione **Apply**.

4

Características adicionales del servidor NAS

Este capítulo incluye la siguiente información:

Temas:

Configurar el servicio de directorio de UNIX preferido

Después de crear un servidor NAS, puede establecer el orden de búsqueda preferido de los servicios de directorio de UNIX (UDS) para el acceso de los usuarios.

1. Seleccione **Storage** > **NAS Servers**.
2. Seleccione la casilla de verificación en la columna **Name** a la izquierda del servidor NAS.
3. Haga clic en **Modify**.
4. Seleccione el orden de búsqueda de UDS recomendado en la lista del menú desplegable **Unix Directory Service Search Order**.
5. Haga clic en **Apply**.

Configurar redes de servidores NAS

Puede modificar o configurar redes de servidores NAS.

Configure lo siguiente para las redes de servidores NAS:

- Las interfaces de archivos
- Rutas a servicios externos, como hosts.

Configurar interfaces de archivos para un servidor NAS

Puede configurar las interfaces de archivos para un servidor NAS después de que el servidor se ha agregado a PowerStore.

Puede agregar más interfaces de archivos y definir cuál es la interfaz preferida que se usará. Además, puede definir la interfaz que se usará para producción y respaldo, o para IPv4 o IPv6.

1. Seleccione **Storage** > **NAS Servers** > **[nas server]**.
2. En la página **Red**, haga clic en **Agregar** para agregar otra interfaz de archivos al servidor NAS.
3. Ingrese las propiedades de la interfaz de archivos.

   NOTA: No reutilice las VLAN que se utilizan para las redes de administración y almacenamiento.

4. Puede realizar lo siguiente en una interfaz de archivos seleccionando una interfaz de archivo en la lista. Seleccione:

Opción	Descripción
Modificación	Para cambiar las propiedades de la interfaz de archivos.
Eliminar	Para eliminar la interfaz de archivos del servidor NAS.
Ping	Para probar la conectividad del servidor NAS a una dirección IP externa.
Interfaz preferida	Para definir la interfaz que PowerStore debe usar de manera predeterminada cuando se han definido varias interfaces de producción y respaldo.

Configurar rutas para la interfaz de archivos para conexiones externas

Puede configurar las rutas que utiliza el sistema de archivos para las conexiones externas.

Puede utilizar la opción **Ping** de la tarjeta **File Interface** para determinar si la interfaz de archivos tiene acceso al recurso externo.

Generalmente, las interfaces del servidor NAS se configuran con un gateway predeterminado, el cual se usa para enrutar solicitudes desde la interfaz del servidor NAS a los servicios externos.

Siga los pasos a continuación:

- Si requiere configurar rutas más granulares hacia los servicios externos.
- Para agregar una ruta con el fin de acceder a un servidor desde una interfaz específica a través de un gateway específico.

1. Seleccione **Almacenamiento** > **Servidores NAS** > **[nas server]** > **Red** > **Rutas a los servicios externos**.
2. Haga clic en **Add** para ingresar la información de la ruta en el asistente **Add Route**.

Habilitar el respaldo NDMP

Puede configurar el respaldo estándar para los servidores NAS con NDMP. Network Data Management Protocol (NDMP) proporciona un estándar para realizar el respaldo de servidores de archivos en una red. Cuando NDMP está habilitado, una aplicación de administración de datos (DMA) de terceros, , como Dell NetWorker, puede detectar el NDMP de PowerStore mediante la dirección IP del servidor NAS.

La habilitación de NDMP se realiza después de la creación del servidor NAS.

PowerStore admite:

- NDMP de tres vías: los datos se transfieren mediante la DMA a través de una red de área local (LAN) o una red de área extendida (WAN).
- Respaldos completos e incrementales

1. Seleccione **Almacenamiento** > **Servidores NAS** > **[nas server]** > **Protección**.
2. En **NDMP Backup**, si **Disabled** está activo, deslice el botón para seleccionar **Enabled**.
3. Ingrese una contraseña en **New Password**.
   El nombre de usuario siempre es `ndmp`.
4. Vuelva a ingresar la misma contraseña nueva en **Verificar contraseña**.
5. Haga clic en **Aplicar**.

Salga de la página de NDMP y regrese a ella para validar que NDMP esté habilitado.

5

Más funciones del sistema de archivos

Este capítulo incluye la siguiente información:

Temas:

Cuotas de sistemas de archivos

Puede rastrear y limitar el consumo de espacio de las unidades mediante la configuración de cuotas para sistemas de archivos en el nivel de directorio o de sistema de archivos. Puede habilitar o inhabilitar cuotas en cualquier momento, pero se recomienda que lo haga durante horas de menor producción para evitar consecuencias en las operaciones del sistema de archivos.

NOTA: No puede habilitar cuotas para sistemas de archivos de solo lectura.

NOTA: Las cuotas no se admiten en sistemas de archivos de VMware.

NOTA: Cuando se crea una sesión de replicación, las cuotas no son visibles en el sistema de destino, incluso si están habilitadas en el sistema de origen.

Tipos de cuotas

Hay tres tipos de cuotas que puede colocar en un sistema de archivos.

Tabla 2. Tipos de cuota

Tipo	Descripción
Cuotas de usuario	Limita la cantidad de almacenamiento que consume un usuario individual mediante el almacenamiento de datos en el sistema de archivos.
Cuota de árbol	Las cuotas de árbol limitan la cantidad total de almacenamiento que se consume en un árbol de directorios específico. Puede usar cuotas de árbol para: • Establecer límites de almacenamiento según el proyecto. Por ejemplo, puede establecer cuotas de árbol para un directorio de proyecto que tenga varios usuarios que compartan y creen archivos en este. • Rastree el uso del directorio mediante la configuración de los límites máximo y de advertencia de la cuota de árbol en 0 (cero). **NOTA:** Si cambia los límites de una cuota de árbol, los cambios se aplican inmediatamente sin interrumpir las operaciones del sistema de archivos.
Cuota de usuario en un árbol de cuotas	Limita la cantidad de almacenamiento que consume un usuario individual mediante el almacenamiento de datos en el árbol de cuotas.

Límites de cuota

Tabla 3. Límites máximo y de advertencia

Tipo	Descripciones
Hard	Un límite máximo es un límite absoluto en cuanto al uso del almacenamiento.

Tabla 3. Límites máximo y de advertencia (continuación)

Tipo	Descripciones
	Si se alcanza un límite máximo para una cuota de usuario en un sistema de archivos o un árbol de cuotas, el usuario no puede escribir datos en el sistema de archivos ni en el árbol hasta que haya más espacio disponible. Si se alcanza el límite máximo de un árbol de cuotas, ningún usuario puede escribir datos en el árbol hasta que haya más espacio disponible.
Límite de advertencia	Un límite de advertencia es un límite recomendado del uso del almacenamiento. El usuario puede utilizar espacio hasta que se alcanza un período de gracia. Se alerta al usuario cuando se alcanza el límite de advertencia hasta que finaliza el período de gracia. Después de eso, se alcanza una condición de espacio insuficiente hasta que el usuario vuelve a estar bajo el límite de advertencia.

Período de gracia de cuota

El período de gracia de cuotas le permite establecer un período de gracia específico para cada cuota de árbol en un sistema de archivos. El período de gracia cuenta el tiempo transcurrido entre el límite de advertencia y el máximo, y avisa al usuario del tiempo que falta para que se alcance el límite máximo. Si vence el período de gracia, no podrá escribir en el sistema de archivos hasta que se haya agregado más espacio, incluso si no se ha alcanzado el límite máximo.

Puede establecer una fecha de vencimiento para el período de gracia. El valor predeterminado es de 7 días. Como alternativa, puede configurar la fecha de vencimiento del período de gracia en una cantidad infinita de tiempo (el período de gracia nunca vence) o en una cantidad determinada de días, horas o minutos. Una vez que se alcanza la fecha de vencimiento del período de gracia, el período de gracia ya no se aplica al directorio del sistema de archivos.

Información adicional

Para obtener más información sobre las cuotas, consulte la *documentación técnica Funcionalidades de archivos de Dell PowerStore*.

Habilitar cuotas de usuario

Debe habilitar las cuotas y establecer los valores predeterminados de la cuota de usuario antes de agregar una cuota de usuario a un sistema de archivos.

1. Seleccione **Storage** > **File Systems** > **[file system]** > **Quotas**.
2. Seleccione **Storage** > **File Systems** > **[file system]** > **Quotas** > **Properties**.
3. Deslice el botón **Deshabilitado** hasta **Habilitado**.
4. Ingrese el valor predeterminado de **Período de gracia** correspondiente a la cuota del usuario en el sistema de archivos, el cual hará una cuenta regresiva después de que se cumpla el límite mínimo y hasta que se alcance el límite máximo.
5. Ingrese un valor predeterminado de **Soft Limit** y **Hard Limit**, y haga clic en **Update**.

Agregar una cuota de usuario en un sistema de archivos

Cree una cuota de usuario en un sistema de archivos para limitar o rastrear la cantidad de espacio de almacenamiento que cada usuario consume en ese sistema de archivos. Cuando crea o modifica cuotas de usuario, puede usar límites máximo y de advertencia predeterminados que se configuran en el nivel del sistema de archivos.

Debe habilitar las cuotas y establecer los valores predeterminados de la cuota de usuario antes de agregar una cuota de usuario en un sistema de archivos. Consulte Habilitar cuotas de usuario.

NOTA: No puede crear cuotas para sistemas de archivos de solo lectura.

1. Seleccione **Storage** > **File Systems** > **[file system]** > **Quotas** > **User**.
2. Seleccione **Add** en la página **User Quota**.
3. En el asistente **Add User Quota**, proporcione la información solicitada. Para rastrear el consumo de espacio sin establecer límites, configure **Soft Limit** y **Hard Limit** en 0, lo cual indica que no hay límites.

4. Seleccione **Add**.

Agregar un árbol de cuotas en un sistema de archivos

Cree un árbol de cuotas en el nivel de directorio de un sistema de archivos para limitar o rastrear el espacio total de almacenamiento que se consume de ese directorio.

1. Seleccione **Storage** > **File Systems** > **[file system]** > **Quotas** > **Tree Quotas**.
2. Seleccione **Add**.
3. Deslice la opción **Enforce User Quota** a la derecha para activar los valores predeterminados de cuota de usuario en la cuota de árbol.
4. Proporcione la información solicitada.
   - Ingrese un valor de **Grace Period** para contar el tiempo entre el límite mínimo y máximo. Comenzará a recibir alertas una vez que se alcance el periodo de gracia.
   - Para rastrear el consumo de espacio sin establecer límites, configure los campos **Soft Limit** y **Hard Limit** en 0, lo cual indica que no hay límites.
5. Seleccione **Add**.

Agregar una cuota de usuario en un árbol de cuotas

Cree una cuota de usuario en un árbol de cuotas para limitar o rastrear la cantidad de espacio de almacenamiento que cada usuario consume en ese árbol. Cuando crea cuotas de usuario en un árbol, puede usar el período de gracia y los límites máximo y mínimo predeterminados configurados en el nivel de cuota de árbol.

1. Seleccione **Storage** > **File Systems** > **[file system]** > **Quotas** > **Tree Quotas**.
2. Seleccione una ruta y haga clic en **Add User Quota**.
3. En la pantalla **Add User Quota**, proporcione la información solicitada. Para rastrear el consumo de espacio sin establecer límites, configure los campos **Soft Limit** y **Hard Limit** en 0, lo cual indica que no hay límites.

Calidad de servicio (QoS) de archivos

En un sistema que ejecuta cargas de trabajo variables con demandas impredecibles, la calidad de servicio garantiza que las aplicaciones críticas puedan obtener prioridad y proporciona un rendimiento predecible para cada aplicación.

Puede aplicar políticas de calidad de servicio (QoS) para establecer el ancho de banda máximo para los servidores NAS y los sistemas de archivos.

Cuando asigna una política de QoS a un servidor NAS o sistema de archivos, SDNAS aplica la política en los servicios NFS/SMB.

Los límites de ancho de banda se aplican en función de los protocolos NFS/SMB y SFTP/FTP.

Si el ancho de banda establecido supera el ancho de banda máximo establecido para el servidor NAS, entonces el ancho de banda efectivo es el ancho de banda máximo del servidor.

NOTA: Es posible que la política de QoS tarde un tiempo en surtir efecto.

NOTA: La QoS no es compatible con los clones del servidor NAS, los clones del sistema de archivos, las instantáneas, los clones de instantáneas y la actualización de instantáneas.

NOTA: El ancho de banda aplicado a los servidores NAS y los sistemas de archivos como parte de una política de QoS puede experimentar una desviación dentro de un margen del 10 %.

Límites de QoS de archivos:

- Una política de QoS puede incluir una regla de límite de I/O.
- Se pueden definir hasta 100 políticas de QoS de archivos.
- Se pueden definir hasta 100 reglas de QoS de archivos.
- Solo se puede aplicar una política de QoS a un servidor NAS o sistema de archivos.
- Se puede asignar la misma política de QoS a varios servidores NAS y sistemas de archivos.

QoS y replicación de archivos:

- Cuando el servidor NAS tiene una regla de replicación, la política de QoS asignada se replica en el servidor de destino.
- Cuando modifica las políticas de QoS asignadas al servidor NAS, los cambios se replican en el servidor de destino.

- No es posible modificar la configuración de la política de QoS replicada en el servidor de destino.
- No es posible asignar una política de QoS a un servidor NAS o sistema de archivos en el servidor de destino.
- Después de asignar una política de QoS a un servidor NAS o un sistema de archivos en el servidor de origen, no es posible cancelar la asignación de la política del servidor de destino.
- Después de cancelar la asignación de una política de QoS desde un servidor NAS, la política también se debe cancelar en el destino.
- Después de la conmutación por error, puede asignar, cancelar la asignación y modificar las políticas de QoS replicadas.

Límites de QoS de archivos

Puede crear reglas de límite de I/O para servidores NAS y sistemas de archivos. Una regla de límite de I/O define el ancho de banda máximo permitido.

- Cada servidor NAS o sistema de archivos se puede asociar con una sola regla de límite.
- Cada política puede incluir solo una regla.
- Puede definir hasta 100 reglas.

NOTA: El ancho de banda observado puede superar el valor establecido, especialmente en los límites establecidos más bajos.

Las reglas de límite de I/O se aplican solo a las operaciones de I/O de hosts externos y no a las operaciones de replicación interna, ya sean asíncronas o síncronas, ni a las operaciones de migración de I/O.

Las reglas de límite de I/O no se aplican a los objetos que se crean internamente, como los respaldos de NDMP servidos por un servidor NDMP en SDNAS.

No se admiten alertas específicas para los límites de QoS de archivos. Para saber si los límites establecidos requieren un ajuste, puede monitorear los gráficos de latencia, IOPS y ancho de banda para cada servidor NAS y sistema de archivos.

Creación de una regla y una política de límite de ancho de banda de calidad de servicio (QoS)

Puede crear una regla de límite de ancho de banda y agregarla a una política de QoS.

1. Seleccione **Almacenamiento** > **Calidad de servicio (QoS)** > **Reglas de límites de I/O de archivos**.
2. Seleccione **Crear**.
3. En el panel deslizable **Crear regla de límite de I/O de archivos**, configure el nombre de la regla y el ancho de banda máximo (MB/s).
4. Seleccione **Crear**.
   La regla se agrega a la tabla Reglas de límite de I/O de archivos.
5. Seleccione **Políticas de QoS de archivos**.
6. Seleccione **Crear**.
7. En el menú desplegable **Crear política de QoS de archivos**, configure el nombre de la política. También puede agregar una descripción.
8. En la lista de reglas, seleccione la regla que desea agregar a la política.
9. Seleccione **Crear**.
   La política se agrega a la tabla Políticas de QoS de archivos.

Asignación de una política de QoS de archivos

Después de definir una regla de límite de I/O como parte de una política de QoS de archivos, puede asignarla a un servidor NAS o a un sistema de archivos. También puede modificar la política de QoS asignada.

NOTA: También es posible asignar una política de QoS como parte del procedimiento para crear un servidor NAS o un sistema de archivos.

1. Seleccione **Almacenamiento** > **Servidores NAS** o **Almacenamiento** > **Sistemas de archivos**.
2. Seleccione la casilla de verificación junto al servidor NAS o sistema de archivos correspondiente.
3. Seleccione **Más acciones** > **Cambiar política de QoS**.
4. En el menú desplegable **Cambiar política de QoS**, seleccione una política de QoS de archivos y, a continuación, seleccione **Aplicar**.
   La política se ha asignado. Puede ver el nombre de la política asignada en la columna **Política de QoS** en las tablas Servidor NAS y Sistemas de archivos. Puede ver el impacto de la política asignada en el rendimiento seleccionando **Almacenamiento** > **Servidores NAS** > **[servidor NAS]** > **Rendimiento** o **Almacenamiento** > **Sistemas de archivos** > **[sistema de archivos]** > **Rendimiento**.

NOTA: También puede configurar la política de QoS seleccionando el servidor NAS o el sistema de archivos pertinentes y, a continuación, seleccionando **Modificar**.

Modificación de una política de QoS de archivos

Puede modificar una política de QoS seleccionando una regla de límite de I/O diferente.

No puede modificar una política asignada a un servidor NAS o sistema de archivos.

1. Seleccione **Almacenamiento** > **Calidad de servicio (QoS)**.
2. En la tabla **Políticas de QoS de archivos**, seleccione la casilla de verificación junto a la política de QoS que desee modificar.
3. Seleccione **Modify**.
4. En la ventana **Modificar política de QoS**, puede modificar el nombre y la descripción de la política y seleccionar una regla de límite de I/O diferente.
5. Seleccione **Aplicar**.

NOTA: También puede modificar una política de QoS desde la pantalla **Propiedades** del recurso de almacenamiento.

Eliminación de una política de QoS de archivos

Asegúrese de que la política de QoS que desea eliminar no esté asignada a un servidor NAS o sistema de archivos.

1. Seleccione **Almacenamiento** > **Calidad de servicio (QoS)**.
2. En la tabla **Políticas de QoS de archivos**, seleccione la política de QoS que desee eliminar.
3. Seleccione **More Actions** > **Delete**.
4. Seleccione **Eliminar** para confirmar la selección.

6

Replicación del servidor NAS

Este capítulo incluye la siguiente información:

Temas:

Descripción general

Para habilitar la redundancia y la recuperación mejoradas si se produce una pérdida de datos, PowerStore permite replicar servidores NAS de un sistema local en un sistema remoto.

De manera predeterminada, la replicación se produce en el nivel del servidor NAS: todos los sistemas de archivos dentro del servidor NAS replicado se replican en el sistema remoto. Puede optar por agregar sistemas de archivos o eliminarlos del servidor NAS, incluso cuando forme parte de una sesión de replicación.

Puede seleccionar la replicación asíncrona, en la cual los sistemas se sincronizan en función de un RPO definido, o la replicación síncrona, en la que los cambios se replican desde el sistema de origen hacia el sistema de destino inmediatamente cuando se producen.

Los siguientes requisitos son necesarios para habilitar la replicación de archivos:

- Un sistema remoto de archivos
- Debe haber configurada y asignada una red de movilidad de archivos (consulte *Guía de redes T y Q de PowerStore para servicios de almacenamiento* en la página Documentación de PowerStore).
- Una política de protección que incluya una regla de replicación.

Considere lo siguiente en cuanto a la replicación de servidores NAS:

- No es necesario definir políticas de protección por separado para los servidores NAS. Las mismas políticas de protección se pueden aplicar a la replicación de bloques y archivos.
- Puede eliminar sistemas de archivos del sistema de origen de una sesión de replicación. Después de la eliminación, solo los sistemas de archivos restantes se replican en el destino. El estado del sistema de destino no se ve afectado después de la eliminación del sistema de archivos. Si elimina sistemas de archivos de un servidor NAS de origen en proceso de replicación y, a continuación, realiza una conmutación por error al sistema de destino, los sistemas de archivos que se eliminaron de la fuente anterior no serán replicados por la nueva fuente. Si desea replicar estos sistemas de archivos, genere clones que se puedan replicar y elimine los sistemas de archivos.
- Puede conmutar por error una sesión de replicación al sistema remoto. La conmutación por error se produce para todos los sistemas de archivos dentro del servidor NAS conmutado por error.
- Cuando se crea una sesión de replicación, las cuotas no son visibles en el sistema de destino, incluso si están habilitadas en el sistema de origen.
- En el caso de la replicación asíncrona, el RPO se configura en el nivel del servidor NAS y es idéntico en todos los sistemas de archivos asociados.
- Para la replicación síncrona, el aumento del tamaño de un sistema de archivos que se está replicando requiere que, en primer lugar, la sesión de replicación se ponga en pausa. La reducción del tamaño de un sistema de archivos no requiere que la sesión de replicación se ponga en pausa.
- Para la replicación síncrona, no es posible cambiar la latencia de red del par de sistemas de replicación a un valor superior a cinco milisegundos cuando se definen sesiones de replicación síncrona.
- El cambio entre la replicación síncrona y asíncrona no se admite para la replicación de archivos.

Para obtener información detallada sobre los procedimientos de replicación del servidor NAS, consulte *la Guía de protección de datos* en la PowerStore página Documentación.

Prueba de recuperación ante desastres para servidores NAS en replicación

Una prueba de recuperación ante desastres ejecuta un plan de recuperación ante desastres que le permite comprobar que el sistema pueda recuperarse y restaurar datos y operaciones en caso de producirse un desastre.

En PowerStore, se proporcionan varias opciones para probar la capacidad del sistema de recuperarse de un desastre y recobrar la funcionalidad:

- Clonar un servidor NAS para pruebas de recuperación ante desastres mediante direcciones IP únicas.
- Clonar un servidor NAS para pruebas de recuperación ante desastres mediante una red aislada con direcciones IP duplicadas.
- Realizar una conmutación por error planificada.

Clonar un servidor NAS para pruebas de recuperación ante desastres mediante direcciones IP únicas

La clonación de un servidor NAS es la opción recomendada para probar la DR. Puede clonar el servidor NAS mediante PowerStore Manager y probarlo sin afectar la producción. Para habilitar el acceso al servidor NAS recientemente clonado, es necesario configurar una nueva interfaz de red única. La dirección IP configurada no puede estar en uso en los servidores NAS de origen o destino. También se requieren ajustes únicos para unir el servidor a un dominio de AD.

Los cambios que se hacen en los sistemas de archivos clonados no afectan a los que se hacen en los sistemas de archivos de producción y viceversa. Cuando se completa la prueba de DR, el servidor clonado se puede eliminar.

Puede elegir cualquiera de las siguientes opciones:

- Clonar el servidor NAS en el sistema de origen, replicarlo en el destino y realizar una conmutación por error planificada al sistema de destino.
- Clonar el servidor NAS en el sistema de destino y acceder a los datos (la conmutación por error no es necesaria porque los recursos clonados ya están accesibles en el sistema de destino).

1. En PowerStore Manager, seleccione **Almacenamiento** > **Servidores NAS**.
2. Seleccione el servidor NAS que desea clonar y, a continuación, elija **Replanificar** > **Clonar servidor NAS**.
3. En la ventana **Crear clon**, proporcione un nombre para el clon y seleccione los sistemas de archivos que desea clonar.
4. Seleccione **Crear**.
   El servidor NAS clonado se agrega a la lista de servidores.
5. Seleccione el nombre del servidor NAS clonado para abrir la ventana de detalles del servidor.
6. Para agregar una interfaz de archivos:
   a. Seleccione la pestaña **Red**.
   b. En **Interfaz de archivos**, seleccione **Agregar**.
   c. Proporcione la información de la interfaz y seleccione **Agregar**.
7. Para establecer el protocolo de uso compartido:
   a. Seleccione la pestaña **Protocolos de uso compartido**.
   b. Seleccione el protocolo pertinente (SMB, NFS o FTP).
   c. Configure la información necesaria y seleccione **Aplicar**.
8. Si clonó el servidor NAS de origen:
   a. Replique el servidor NAS en el sistema de destino. Para obtener detalles, consulte Replicación del servidor NAS.
   b. Realice una conmutación por error planificada al destino. Para obtener detalles, consulte Conmutación por error planificada.
   c. Compruebe si el host puede acceder a los datos.
9. Si clonó el servidor de producción replicado en el sistema de destino, no se requiere la conmutación por error. Verifique el acceso de host.

Clonar un servidor NAS para pruebas de recuperación ante desastres mediante una red aislada con direcciones IP duplicadas

Es posible probar la recuperación ante desastres usando la misma configuración que la producción. El uso de ajustes idénticos puede reducir el riesgo y aumentar la reproducibilidad en un escenario de falla. Sin embargo, el uso de direcciones IP duplicadas crea conflictos. La ejecución de la prueba de DR en un entorno aislado del entorno de producción le permite evitar estos conflictos.

En PowerStoreOS 3.6 y versiones posteriores, puede crear un entorno de pruebas de recuperación ante desastres (DRT) aislado como ayuda para estar preparado ante un desastre.

La creación de un entorno aislado le permite usar la misma dirección IP y el mismo nombre de host que el sistema de producción y realizar una DRT para un servidor NAS en replicación sin ningún impacto en la producción.

Para crear un entorno de DRT, debe configurar una red aislada con un enrutador de DRT independiente y crear agregaciones de enlaces con los puertos de I/O de red.

Mediante la PSTCLI o la API REST, cree un entorno de red dedicado en el servidor de destino clonando el servidor NAS en replicación al sistema PowerStore de destino. El clon es una copia completa del entorno de producción y un entorno de pruebas dedicado, que está aislado de la producción. Puede crear un entorno de red aislado y configurar el entorno de pruebas con la misma dirección IP y el mismo nombre de host que el sistema de producción. El servidor NAS de DRT no tiene ningún impacto en el entorno de producción y se puede ejecutar sin conflictos de dirección IP cuando se produce una conmutación por error y una conmutación por recuperación en el servidor NAS de replicación.

Para probar la DR con el uso de un entorno de pruebas aislado:

1. Cree el clon del servidor NAS en el destino. Utilice la marca `is_dr_test`.
2. Cree una interfaz de vinculación de usuario para NAS con la misma dirección IP que el servidor NAS de origen.
3. Una el clon a AD (si es necesario).
4. Verifique que los hosts puedan acceder a los datos.

NOTA: También puede usar la DRT en servidores NAS independientes.

Requisitos y limitaciones

Para crear un entorno de DRT, asegúrese de que se cumplan los siguientes requisitos:

- Adquiera la información de la red privada:
  - Gateway
  - Máscara de red
  - ID de VLAN (opcional)
- Identifique los puertos de red de la red aislada y los de la red de producción.

Tenga en cuenta las siguientes limitaciones al crear un entorno de DRT:

- La interfaz de vinculación dedicada a DRT no se puede utilizar para crear ningún otro servidor NAS de producción.
- Un servidor NAS configurado como producción no se puede reconfigurar como parte de la DRT.
- Un servidor NAS configurado como parte de la DRT no se puede reconfigurar como producción.
- Un servidor NAS que ya no forma parte de una DRT no se puede reconfigurar y se debe eliminar.
- Después de que un servidor NAS está activo y configurado con información de red, la configuración adicional (como DNS, CAVA y Kerberos) se debe realizar manualmente.
- El servidor NAS habilitado para DRT no se puede replicar.
- La modificación y la eliminación del servidor NAS se pueden realizar mediante PowerStore Manager.

Configurar el entorno de pruebas de recuperación ante desastres mediante PSTCLI

1. Adquiera el nombre del servidor NAS en el sitio de destino (que se clonará):

```
[SVC:service@9CB0BD3-B user]$ pstcli -d <PowerStore_IP> nas_server show
# | id | name | operational_status |  current_node_id  | file_interfaces.ip_addre~
--+--------------+--------+--------------------+-------------------
```

```
1 |647f545a-4b11-5cdd-4d4c-eeeba81eb143 | File80| Started | R2C4-appliance-1-node~|
127.1.1.1
```

2. Clone el servidor NAS proporcionando un nuevo nombre para el clon y utilizando el switch `-is_dr_test true`:

```
[SVC:service@9CB0BD3-B user]$ pstcli -d <PowerStore_IP> nas_server -name File80
clone -name File80_c -is_dr_test true
Success
```

3. Busque el ID del puerto IP para la vinculación de archivos NAS que está conectada a la red aislada:

NOTA: Si la vinculación de archivos NAS no se creó, puede crearla mediante PSTCLI o PowerStore Manager.

```
[SVC:service@9CB0BD3-B user]$ pstcli -d <PowerStore_IP> ip_port_show -output nvp
8:  id =IP_PORT23
    current_usages =
    ip_pool_addresses =
    bond:
    name=BaseEnclosure-NodeA-bond1
```

4. Cree la interfaz de archivos para el servidor NAS clonado:

```
[SVC:service@9CB0BD3-B user]$ pstcli -d <PowerStore_IP> file_interface create
-nas_server_name File80_c -ip_address "10.10.10.10" -prefix_length 24 -gateway
"10.10.10.1" -vlan_id 5
-ip_port_id IP_PORT23
Created
# |     id
--+------------------------------------
1 |64830ae5-2760-59ce-4c90-82772509648e
```

5. Vea la interfaz de archivos:

```
[SVC:service@9CB0BD3-B user]$ pstcli -d <PowerStore_IP> file_interface_show
# |id | nas_server_id | ip_address | prefix_length | gateway | is_disabled
--+------------+--------+-------------------+-------------------
  1 |647f5509-11f4-a52d-ee1f-82772509648e | 647f545a-4b11-5cdd-4d4c-eeeba81eb143 |
10.10.10.10 |24 | 10.10.10.1 | no
  2 |64830ae5-2760-59ce-4c90-82772509648e | 6483092f-3e71-8a92-0a0b-82772509648e |
10.10.10.10 |24 | 10.10.10.1 | no
```

Configurar un servidor NAS en un entorno de DRT mediante la API REST

NOTA: Si no utiliza la API REST, omita esta sección.

1. Para clonar el servidor NAS en el espacio de nombres especificado, ejecute `/nas_server/{id}/clone` y especifique `is_dr_test` como true.
2. Para crear una interfaz de red, ejecute `/file_interface` y especifique los parámetros de la red privada.

NOTA: En este paso, se crea la interfaz de archivos del servidor NAS clonado con la misma dirección IP, máscara de red y gateway que el servidor NAS de producción. Utilice la interfaz de vinculación/IP_Port asociada con la red privada.

El servidor NAS está activo y se puede utilizar para la DRT en la red aislada.

Realizar una conmutación por error planificada

Puede usar la conmutación por error planificada para probar la recuperación ante desastres. Cuando realiza una conmutación por error planificada, la sesión de replicación del servidor NAS se conmuta por error manualmente desde el sistema de origen al sistema de destino. Antes de la conmutación por error, el sistema de destino se sincroniza con el sistema de origen para impedir la pérdida de datos.

NOTA: La conmutación por error del servidor NAS de producción al sistema de destino puede afectar la producción.

Antes de realizar una conmutación por error planificada, asegúrese de detener las operaciones de I/O en todas las aplicaciones y los hosts. No puede poner en pausa una sesión de replicación que está experimentando una conmutación por error planificada.

Cuando la operación se realiza de manera normal, los cambios realizados en el servidor NAS y en los sistemas de archivos durante la prueba de DR se conservan y replican en la fuente original cuando se inicia la reprotección (ya sea de forma manual o automática). Sin embargo, si no desea guardar los cambios realizados durante las pruebas de DR (de datos o configuración), puede optar por descartar los cambios mediante los comandos de la API REST o la PSTCLI:

- API REST- `POST /replication_session/{id}/reprotect discard_changes_after_failover`
- PSTCLI: `replication_session -id <value> reprotect [-discard_changes_after_failover]`

Los cambios que se descartan:

- En el caso de los servidores NAS:
  - Cambios en la configuración
- Para los sistemas de archivos:
  - Cambios en la configuración
  - Cambios en los datos del sistema de archivos
  - Recursos de instantáneas
  - Cambios en la dimensión del sistema de archivos
  - Cambios en las cuotas
- En el caso de las exportaciones y las acciones:
  - Cambios en las exportaciones de NFS
  - Cambios en los recursos compartidos de SMB

NOTA: Esta opción solo se soporta en el caso de la replicación asíncrona.

Para conocer detalles sobre el uso de la API REST y la CLI con el fin de descartar cambios después de una conmutación por error, consulte la *Guía de referencia de la API REST de Dell PowerStore* y la *Guía de referencia de la CLI de Dell PowerStore* en dell.com/powerstoredocs.

Tras la reprotección del servidor NAS, puede volver a iniciar una conmutación por error planificada para poner los recursos en línea en el sistema de origen original.

NOTA: No realice una conmutación por error no planificada con fines de recuperación ante desastres. La conmutación por error no planificada se debe utilizar solo cuando no se puede acceder al sistema de origen.

NOTA: Para habilitar el acceso no disruptivo a los datos en el entorno SMB, se recomienda configurar la disponibilidad continua para los recursos compartidos de SMB y volver a montarlos después de restablecer la conexión.

Existen dos maneras de iniciar una conmutación por error prevista:

- En **Protección** > **Replicación**, seleccione la sesión de replicación pertinente y, a continuación, seleccione **Conmutación por error planificada**.
- En la pestaña **Protección** del recurso, seleccione **Replicación** y **Conmutación por error planificada**.

Después de una conmutación por error planificada, la sesión de replicación queda inactiva. Para sincronizar el recurso de almacenamiento de destino y reanudar la sesión de replicación, utilice la acción **Volver a proteger**. También puede seleccionar la opción Volver a proteger antes de realizar la conmutación por error, lo que inicia automáticamente la sincronización en la dirección opuesta (en el siguiente RPO) después de que se completa la conmutación por error y devuelve el sistema de origen y de destino a un estado normal.

NOTA: Después de realizar la conmutación por error, las cuotas del usuario dejan de aparecer en el sistema de destino (que se convirtió en el nuevo origen). Para ver las cuotas del usuario, actualice manualmente las cuotas mediante la selección de **Almacenamiento** > **Sistemas de archivos**, marque la casilla de verificación junto al sistema de archivos pertinente y, a continuación, seleccione **Más acciones** > **Actualizar cuotas**.

Desconexión de red durante una DRT

Cuando se realiza una DRT, no se recomienda simular una falla de red entre los sistemas local y remoto y, a continuación, realizar una conmutación por error no planificada al sistema de destino para habilitar el acceso al servidor NAS de DR. Dado que no hay comunicación entre los sistemas, PowerStore no puede garantizar que ambos servidores NAS estén en un estado compatible. Una vez que se restaura la conexión, ambos servidores NAS están en modo de producción (desconexión entre sitios). Como resultado, ambos sistemas cambian al modo de destino para evitar que los datos se escriban en ambas ubicaciones.

Para resolver este estado, se requiere la intervención del soporte técnico.

Para obtener más información, consulte el artículo de la base de conocimientos 000215482 de Dell (Interrupción de la conexión de red entre sitios... [en inglés]).

7

Uso de CEPA con PowerStore

Este capítulo incluye la siguiente información:

Temas:

Publicación de eventos

CEE permite que aplicaciones de otros fabricantes reciban información de eventos del sistema de almacenamiento cuando acceden a sistemas de archivos.

Common Event Enabler (CEE) proporciona una solución de publicación de eventos para los clientes de PowerStore que permite a las aplicaciones de otros fabricantes registrarse y recibir contexto y notificación de eventos del sistema de almacenamiento cuando acceden a sistemas de archivos. La recepción de notificación de eventos permite realizar acciones impulsadas por eventos en el almacenamiento para evitar amenazas de seguridad, como ransomware o acceso no autorizado.

Common Events Publishing Agent (CEPA) de CEE consta de aplicaciones diseñadas para procesar archivos SMB y NFS y notificaciones de eventos de directorio. CEPA envía tanto la notificación de eventos como el contexto asociado a la aplicación en un mensaje. El contexto puede incluir metadatos de archivo o metadatos de directorio necesarios para las decisiones con respecto a políticas comerciales.

Para habilitar la compatibilidad con CEPA de CEE, debe habilitar CEPA de CEE y crear un pool de publicación de eventos en el servidor NAS.

Un pool de publicación de eventos define los servidores CEPA y los eventos específicos que activan notificaciones.

Una vez que configura el servidor NAS, puede habilitar la publicación de eventos en el sistema de archivos desde el cual desea recibir eventos. Cuando un host genera un evento en el sistema de archivos mediante SMB o NFS, la información se reenvía al servidor CEPA a través de una conexión HTTP. El software CEPA de CEE en el servidor recibe el evento y lo publica, lo que permite que el software de otros fabricantes lo procese.

Para utilizar Events Publishing Agent, es necesario disponer de un sistema PowerStore con al menos un servidor NAS configurado en la red.

Para obtener información adicional sobre CEPA, que forma parte de Common Event Enabler (CEE), consulte *Uso de Common Event Enabler en plataformas Windows* en el sitio de soporte de Dell Technologies.

Crear un pool de publicación

Para crear un pool de publicación de eventos, debe tener un FQDN de servidor de publicación de eventos (CEPA).

Un pool de publicación de eventos define el servidor CEPA y los eventos específicos que activan notificaciones. Defina al menos una de las siguientes opciones de eventos:

- Eventos previos: eventos que se envían al servidor CEPA para su aprobación antes del procesamiento.
- Eventos posteriores: eventos que se envían al servidor CEPA después de que se producen con fines de registro o auditoría.
- Eventos de error posteriores: eventos de error que se envían al servidor CEPA después de que se producen con fines de registro o auditoría.

1. Seleccione **Almacenamiento** > **Servidores NAS**.
2. Seleccione **Ajustes de NAS**.
3. En la ventana **Publicación de eventos**, seleccione **Pools de publicación** y, a continuación, seleccione **Crear**.
4. Ingrese un **Nombre del pool**.
5. Ingrese el FQDN del servidor CEPA.

6. En la sección Configuración de evento, haga clic en los tipos de evento y seleccione los que desea agregar al pool.
7. Haga clic en **Aplicar** para crear el pool de publicación de eventos.

Crear un publicador de eventos

Después de configurar pools de publicación, cree un publicador de eventos para configurar la respuesta a los diferentes tipos de evento.

NOTA: Los publicadores de eventos se crean en el nivel del sistema y uno de ellos se puede asociar con varios servidores NAS.

1. Seleccione **Almacenamiento** > **Servidores NAS**.
2. Seleccione **Ajustes de NAS**.
3. Seleccione **Publicadores de eventos** y, a continuación, seleccione **Crear**.
4. Continúe avanzando en el asistente **Crear publicador de eventos**.

Pantalla del asistente	Descripción
Seleccionar pools de publicación	• Ingrese un nombre. • Seleccione hasta 3 pools de publicación. Para crear un nuevo pool de publicación, haga clic en **Crear**.

Configurar publicador de eventos	• Política de falla de eventos previos: seleccione el comportamiento deseado cuando todos los servidores CEPA están offline para los eventos previos:
	  ○ Ignorar (valor predeterminado): suponer que todos los eventos se confirman.
	  ○ Denegar: denegar eventos que requieren aprobación hasta que los servidores CEPA estén en línea.
	• Política de falla de eventos posteriores: seleccione el comportamiento deseado cuando todos los servidores CEPA están offline para los eventos posteriores:
	  ○ Ignorar (valor predeterminado): continuar con la operación. Los eventos que ocurrieron mientras los servidores CEPA estaban inactivos se perderán.
	  ○ Acumular: continuar con la operación y guardar eventos en un buffer local (hasta 500 MB).
	  ○ Garantía: continuar con la operación y guardar eventos en un buffer local (hasta 500 MB). Denegar el acceso cuando el buffer está lleno.
	  ○ Denegar: denegar el acceso a los sistemas de archivos cuando los servidores CEPA estén offline.
	• HTTP/Llamada a procedimiento remoto de Microsoft
	• Puerto HTTP

5. Seleccione **Aplicar** para crear el publicador de eventos.

Habilitación de un publicador de eventos para un servidor NAS

Después de configurar el publicador de eventos, habilítelo para el servidor NAS y para todos los sistemas de archivos definidos en él.

1. Seleccione **Almacenamiento** > **Servidores NAS** > **[nas server]**.
2. En la página **Seguridad y eventos**, seleccione **Publicación de eventos**.
3. Seleccione un publicador de eventos de la lista y habilítelo.
4. Seleccione si desea habilitar el publicador de eventos para todos los sistemas de archivos definidos en el servidor NAS.

   Como alternativa, puede optar por habilitar el publicador de eventos para sistemas de archivos específicos. Para obtener más información, consulte Habilitar el publicador de eventos para un sistema de archivos.
5. Haga clic en **Aplicar**.

Habilitar el publicador de eventos para un sistema de archivos

Puede habilitar el publicador de eventos para sistemas de archivos seleccionados.

1. Seleccione **Almacenamiento** > **Sistemas de archivos** > **[file system]**.

2. En la página **Protección**, seleccione **Publicación de eventos**.
3. Habilite el publicador de eventos para el sistema de archivos y seleccione el protocolo.
4. Haga clic en **Aplicar**.