

Dell EMC PowerStore

Configuración de exportaciones de NFS

2.x

Notas, precauciones y advertencias

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

 **PRECAUCIÓN:** Una PRECAUCIÓN indica la posibilidad de daños en el hardware o la pérdida de datos, y le explica cómo evitar el problema.

 **AVISO:** Un mensaje de AVISO indica el riesgo de daños materiales, lesiones corporales o incluso la muerte.

Tabla de contenido

Recursos adicionales.....	4
Capítulo 1: Descripción general.....	5
Compatibilidad con NFS.....	5
Acerca de NFS seguro.....	5
Consideraciones de planificación.....	6
Capítulo 2: Creación de servidores NAS.....	8
Descripción general de la configuración de servidores NAS.....	8
Crear un servidor NAS para los sistemas de archivos de NFS (solamente UNIX).....	8
Configurar los servicios de asignación de nombres del servidor NAS.....	9
Configurar DNS.....	9
Configurar el servicio de directorio de UNIX de un servidor NAS mediante NIS.....	10
Configurar el servicio de directorio de UNIX de un servidor NAS mediante LDAP.....	10
Configurar el servidor NAS para utilizar archivos locales para los servicios de asignación de nombres.....	11
Configurar los protocolos de uso compartido del servidor NAS.....	12
Configurar el servidor NFS.....	12
Configurar el protocolo de uso compartido FTP o SFTP.....	12
Configurar Kerberos para la seguridad del servidor NAS.....	13
Crear un dominio personalizado para Kerberos.....	13
Configurar la seguridad de Kerberos para el servidor NAS.....	14
Capítulo 3: Configurar exportaciones de NFS.....	15
Visión general de sistemas de archivos y exportaciones de NFS.....	15
Crear un sistema de archivos para las exportaciones de NFS.....	15
Crear una exportación de NFS.....	17
Capítulo 4: Funciones adicionales del servidor NAS.....	18
Configurar el servicio de directorio de UNIX preferido.....	18
Configurar redes de servidores NAS.....	18
Configurar interfaces de archivos para un servidor NAS.....	18
Configurar rutas para la interfaz de archivos para conexiones externas.....	19
Habilitar la protección y los eventos de NDMP.....	19
Capítulo 5: Más funciones del sistema de archivos.....	20
Cuotas de sistemas de archivos.....	20
Habilitar cuotas de usuario.....	21
Agregar una cuota de usuario en un sistema de archivos.....	21
Agregar un árbol de cuotas en un sistema de archivos.....	21
Agregar una cuota de usuario en un árbol de cuotas.....	22

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.

Dónde obtener ayuda

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

- **Información de productos**

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

- **Solución de problemas**

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

- **Soporte técnico**

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

Descripción general

En este capítulo se incluye la siguiente información:

Temas:

- [Compatibilidad con NFS](#)
- [Acerca de NFS seguro](#)
- [Consideraciones de planificación](#)

Compatibilidad con NFS

Modelo PowerStore T es compatible con NFSv3 y NFSv4. También es compatible con NFS seguro con Kerberos para una autenticación sólida. Aunque Modelo PowerStore T es compatible con la mayoría de las funcionalidades de NFSv4 y v4.1 descritas en las RFC pertinentes, la delegación de directorio y pNFS no son compatibles. 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 usuarios basada en Kerberos, la cual puede proporcionar integridad y privacidad de los 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:

La compatibilidad con el almacenamiento de archivos está disponible solamente en dispositivos Modelo PowerStore T. El almacenamiento de archivos no es compatible con dispositivos Modelo PowerStore X.

Redes de servidores NAS

La creación de redes VLAN y direcciones IP de red es opcional para los servidores NAS. Si planea crear una VLAN para los servidores NAS, la VLAN no se puede compartir con la administración de Modelo PowerStore T ni con las 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 de PowerStore para modelos PowerStore T*.

Requisitos de implementación

Los servicios de NAS están disponibles solamente en dispositivos Modelo PowerStore T. Si ejecuta dispositivos Modelo PowerStore X, este servicio no está disponible.

Debe haber seleccionado **Unified** durante la configuración inicial de su dispositivo Modelo PowerStore T. Si seleccionó **Block Optimized** en el asistente de configuración inicial, los servicios de NAS no se instalaron. Para instalar los servicios de NAS, un representante de servicio al cliente 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 de **Initial Configuration Wizard**.
- 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.

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
<i>Guía de redes de PowerStore para modelos PowerStore T</i>	Proporciona información sobre la planificación y la configuración de la red.	https://www.dell.com/powerstoredocs
<i>Guía de configuración de recursos compartidos de SMB de PowerStore</i>	Proporciona información necesaria para configurar recursos compartidos de SMB con PowerStore Manager.	

Tabla 1. Recursos de documentación (continuación)

Documento	Descripción	Ubicación
<i>Documentación técnica sobre las funcionalidades de archivos de PowerStore de Dell EMC</i>	Analiza las funciones, la funcionalidad y los protocolos compatibles con la arquitectura de archivos de PowerStore de Dell EMC.	
<i>Ayuda en línea de PowerStore</i>	Proporciona información confidencial contextual para la página que se abre en PowerStore Manager.	Integrada en PowerStore Manager

Creación de servidores NAS

En este capítulo se incluye la siguiente información:

Temas:

- Descripción general de la configuración de servidores NAS
- Crear un servidor NAS para los sistemas de archivos de NFS (solamente UNIX)
- Configurar los servicios de asignación de nombres del servidor NAS
- Configurar los protocolos de uso compartido del servidor NAS
- Configurar Kerberos para la seguridad del servidor NAS

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 de NFS (solamente UNIX)

Debe crear servidores NAS antes de crear sistemas de archivos.

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

1. Seleccione **Storage > NAS Servers**.
2. Seleccione **Create**.
3. Continúe avanzando en el asistente **Create NAS Server**.

Pantalla del asistente	Descripción
Detalles	Ingrese el nombre, la descripción y la información de la red del servidor NAS.  NOTA: No puede reutilizar las VLAN que se utilizan para las redes de administración y almacenamiento.
Sharing Protocol	Seleccione Sharing Protocol Seleccione NFSv3, NFSv4 o ambos.  NOTA: Si selecciona SMB y un protocolo NFS, habilita automáticamente el servidor NAS para ofrecer compatibilidad con multiprotocolo. 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 las siguientes secciones para configurar lo siguiente: • Uso de archivos locales

Pantalla del asistente	Descripción
	• Con NIS • Con LDAP Aquí puede optar por habilitar NFS seguro. 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 es opcional para un servidor NAS independiente). • Configuración de NFS seguro. DNS también se puede utilizar para resolver los hosts definidos en las listas de acceso a exportaciones de NFS.
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 lo redirige a la página **NAS Servers** cuando el servidor aparece en la página.

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

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

Haga clic en el servidor NAS para continuar con la configuración o editar sus ajustes.

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 **Apply**.

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 con los esquemas IDMU, RFC2307 o RFC2307bis. Algunos ejemplos incluyen LDAP de AD con IDMU, iPlanet y OpenLDAP. El servidor LDAP debe configurarse correctamente a fin de proporcionar el UID para cada usuario. Por ejemplo, en IDMU, el administrador debe ir a las propiedades de cada usuario y agregar un UID a la pestaña "Atributos de UNIX".

Puede configurar LDAP de modo que use autenticación anónima, simple y 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 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 para el servidor de iPlanet/OpenLDAP.
Simple	Especifique lo siguiente: • Si usa AD, LDAP/IDMU: ○ DN de enlace en formato de notación de LDAP; por ejemplo, cn=admin, cn=users, dc=svt, dc=lab, dc=com. ○ DN base, que es lo mismo que el nombre de dominio calificado (por ejemplo, svt.lab.com). ○ DN de perfil. • Si usa el servidor de iPlanet/OpenLDAP:

Opción	Descripción
	○ DN de enlace en formato de notación de LDAP; por ejemplo, cn=administrator,cn=users,dc=svt,dc=lab,dc=com. ○ Password ○ DN base. Por ejemplo, si usa svt.lab.com, el DN base sería DC=svt,DC=lab,DC=com. ○ DN de perfil 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 usa NFS seguro con un dominio personalizado, debe cargar un archivo keytab.

7. Haga clic en **Retrieve Current Schema** para descargar el archivo `ldap.conf`.
8. Edite y guarde el archivo `ldap.conf`.
9. Seleccione **Upload New Schema** para cargar el archivo `ldap.conf` actualizado.
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 describe anteriormente en este tema.
- 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.

Configurar los 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 **Linux/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 usa el ID de usuario (UID) para obtener el ID de grupo (GID) primario y todos los GID de grupo a los cuales pertenece. El servidor NAS obtiene los GID desde el archivo de contraseña local o el UDS.
 - Si se deselecciona este campo, la credencial de UNIX de la solicitud de NFS se descomprime directamente de la información de red que se incluye en la trama. Este método tiene un mejor rendimiento, pero solo se pueden incluir 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.

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**.

- De manera opcional, seleccione **Show Access Control List** para proporcionar acceso o denegar el acceso a **Filtered Users, Filtered Groups** y **Filtered hosts**.
- Haga clic en **Apply**.

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 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.

- Ejecute la herramienta `kadmin.local`.
- 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.DELLEMCOM -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.

Configurar exportaciones de NFS

En este capítulo se incluye la siguiente información:

Temas:

- [Visión general de sistemas de archivos y exportaciones de NFS](#)
- [Crear un sistema de archivos para las exportaciones de NFS](#)
- [Crear una exportación de NFS](#)

Visión general de sistemas de archivos y exportaciones de NFS

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

- Antes de crear un sistema de archivos, se debe configurar un servidor NAS que admita el protocolo NFS.
- Puede optar por agregar exportaciones de NFS la primera vez que crea el sistema de archivos, o puede agregarlas a un sistema de archivos después de su creación.

Crear un sistema de archivos para las exportaciones de NFS

Puede crear un sistema de archivos para las exportaciones de NFS.

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

1. Seleccione **Storage > File Systems**.
2. Haga clic en **Add**.
Se inicia el asistente **Add File System**.
3. Seleccione un servidor NAS habilitado para NFS para el sistema de archivos.
4. Especifique los detalles del sistema de archivos, incluidos su nombre y tamaño; el tamaño mínimo es 3 GB y el máximo, 256 TB.

i **NOTA:** Todos los sistemas de archivos delgados, independientemente del tamaño, tienen 1,5 GB reservados para metadatos después de la creación. Por ejemplo, después de crear un sistema de archivos delgado de 100 GB, Modelo PowerStore T muestra inmediatamente 1,5 GB en uso. Cuando el sistema de archivos se monta en un host, muestra 98,5 GB de capacidad útil.

Esto se debe a que se reserva el espacio de metadatos en la capacidad útil del sistema de archivos.

5. Configure la exportación inicial para el sistema de archivos.

i **NOTA:** Puede agregar exportaciones de NFS al sistema de archivos en un momento posterior.

6. Configure el acceso de host.

Opción	Descripción
Minimum Security	Seleccione Sys 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 with Integrity a fin de permitir ambas opciones de seguridad Kerberos with integrity y Kerberos with encryption para la autenticación de usuarios (krb5i/krb5p).

Opción	Descripción
	● Kerberos with Encryption a fin de permitir solo la opción de seguridad Kerberos with encryption 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: ● No Access: Sin acceso al recurso de almacenamiento ni al recurso compartido. ● Read/Write: Los hosts tienen permiso para ver el contenido del recurso de almacenamiento o del recurso compartido, pero no para escribir en ellos. ● Read-Only: Los hosts tienen permiso para leer y escribir en el almacén de datos NFS o en el recurso compartido. ❗ NOTA: Los hosts ESXi deben tener acceso Read//Write para montar un almacén de datos NFS mediante NFSv4 con autenticación de Kerberos NFS owner. ● Read/Write, allow Root: Los hosts tienen permiso para leer y escribir en el recurso de almacenamiento o en el recurso compartido, y para otorgar y revocar permisos de acceso (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, evite otorgar acceso de lectura/escritura a más de un host. ❗ NOTA: Los hosts ESXi deben tener acceso de Read/Write, allow Root para montar un almacén de datos NFS mediante NFSv4 con autenticación NFS Owner:root. ● Read-Only, allow Root: 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 los hosts individualmente o puede agregarlos mediante la carga de un archivo .CSV con el formato correcto. Puede descargar el archivo CSV en primer lugar para obtener una plantilla. Para descargar, editar y usar una plantilla de archivo CSV: - Haga clic en el icono Export Hosts. - Actualice el archivo CSV con los hosts y los tipos de acceso que desea importar. - Guarde el archivo CSV en su máquina local. - Haga clic en Import CSV file. - 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.

Opción	Descripción
Ruta local	La ruta al recurso de almacenamiento de sistemas de archivos en el sistema de almacenamiento. Esta ruta especifica la ubicación única del recurso compartido en el sistema de almacenamiento. ● Cada recurso compartido de NFS debe tener una ruta local única. PowerStore asigna automáticamente esta ruta a la exportación inicial creada dentro de un nuevo sistema de archivos. El nombre de ruta local se basa en el nombre del sistema de archivos. ● Antes de que pueda crear más exportaciones dentro de un sistema de archivos NFS, cree un directorio para compartir desde un host Linux/UNIX que esté conectado al sistema de archivos. A continuación, puede crear una exportación desde PowerStore y configurar permisos de acceso según corresponda.
Ruta de exportación	La ruta que utiliza el host para conectarse a la exportación. PowerStore crea la ruta de exportación que se basa en la dirección IP del host y el nombre de la exportación. Los hosts utilizan el nombre de archivo o la ruta de exportación para el montaje de la exportación o el mapeo a esta desde un host de red.

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

Si agrega una política de protección al sistema de archivos, esta se debe haber creado antes de la creación del sistema de archivos. Para la protección de los sistemas de archivos solamente se admiten las instantáneas. La replicación no es compatible con el sistema de archivos.

8. 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 **NFS export**.

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 **Create**.
Se inicia el asistente **Create NFS Export**.
3. Ingrese la información solicitada, pero considere lo siguiente:
 - Antes de crear la exportación de NFS, se deben crear instantáneas.
 - El valor de **Local Path** debe corresponder a un nombre de carpeta existente dentro del sistema de archivos que se creó desde el host.
 - El valor que se especifica en **NFS Export Details**, campo **Name**, junto con el nombre del servidor NAS, corresponde al nombre a través del cual los hosts acceden a la exportación.
 - 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**.

Funciones adicionales del servidor NAS

En este capítulo se incluye lo siguiente.

Temas:

- [Configurar el servicio de directorio de UNIX preferido](#)
- [Configurar redes de servidores NAS](#)
- [Habilitar la protección y los eventos de NDMP](#)

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. Haga clic en **Add** para agregar otra interfaz de archivos al servidor NAS.
3. Ingrese las propiedades de la interfaz de archivos.

 **NOTA:** No puede reutilizar 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. Haga clic en:

Opción	Descripción
Modificar	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 recomendada	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 necesita configurar rutas más granulares a 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 **Storage > NAS Servers > [nas server] > Networks > Routes to External Services**.
 2. Haga clic en **Add** para ingresar la información de la ruta en el asistente **Add Route**.

Habilitar la protección y los eventos de 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. Una vez que NDMP está habilitado, una aplicación de administración de datos (DMA) de otros fabricantes, como Dell EMC 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 a través de la DMA a través de una red de área local (LAN) o una red de área extendida (WAN).
 - Respaldos completos e incrementales.
1. Seleccione **Storage > NAS Servers > [nas server] > Protection and Events**.
 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 **Verify Password**.
 5. Haga clic en **Apply**.

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

Más funciones del sistema de archivos

En este capítulo se incluye la siguiente información:

Temas:

- [Cuotas de sistemas de archivos](#)

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.

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 que almacena datos en el sistema de archivos.
Cuota de árbol	La cuota de árbol limita la cantidad total de almacenamiento que se consume en un árbol específico del directorio. Puede usar cuotas de árboles para: • Establecer límites de almacenamiento en función del proyecto. Por ejemplo, puede establecer cuotas de árboles para el directorio de un proyecto con varios usuarios que comparten y crean archivos en él. • Rastrear el uso de los directorios mediante la configuración en 0 (cero) de los límites máximo y de advertencia de la cuota de árbol.  NOTA: Si cambia los límites de una cuota de árbol, los cambios se aplican de inmediato 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 que almacena datos en el árbol de cuotas.

Límites de cuotas

Tabla 3. Límites máximo y de advertencia

Tipo	Descripciones
Rígido	Un límite máximo es un límite absoluto en el uso del almacenamiento. Si se alcanza un límite máximo para una cuota de usuario en un sistema de archivos o árbol de cuotas, el usuario no puede escribir datos en el sistema de archivos ni en el árbol hasta que está disponible más espacio. Si se alcanza un límite máximo para un árbol de cuotas, ningún usuario puede escribir datos en el árbol hasta que está disponible más espacio.
Límite de advertencia	Un límite de advertencia es un límite recomendado en el uso del almacenamiento. El usuario puede utilizar espacio hasta que se alcance un período de gracia.

Tabla 3. Límites máximo y de advertencia (continuación)

Tipo	Descripciones
	El usuario recibe una alerta cuando se alcanza el límite de advertencia hasta que finaliza el período de gracia. Después de eso, se alcanza una condición de falta de espacio hasta que el usuario vuelve a estar bajo el límite de advertencia.

Período de gracia de cuotas

El período de gracia de cuotas proporciona la capacidad de establecer un período de gracia específico para cada cuota de árbol en un sistema de archivos. El período de gracia cuenta el tiempo entre el límite máximo y mínimo, y alerta al usuario sobre el tiempo restante antes de que se alcance el límite máximo. Si el período de gracia vence, no puede escribir en el sistema de archivos hasta que no se agregue más espacio, incluso si no se alcanzó el límite máximo.

Puede establecer una fecha de vencimiento para el período de gracia. El valor predeterminado es de 7 días. De manera alternativa, puede configurar la fecha de vencimiento del período de gracia en una cantidad infinita de tiempo y el período de gracia nunca vencerá, o en una cantidad determinada de días, horas o minutos. Cuando 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 sobre las funcionalidades de archivos de PowerStore de Dell EMC*.

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 en un sistema de archivos.

1. Seleccione **Storage > File Systems > [file system] > Cuotas**.
2. Seleccione **Storage > File Systems > [file system] > Cuotas > Properties**.
3. Deslice el botón **Disabled** hacia la derecha hasta que se seleccione **Enabled**.
4. Ingrese el valor predeterminado de **Grace Period** para la cuota de usuario en el sistema de archivos, el cual contará el tiempo de inactividad después de que se cumpla el límite mínimo 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] > Cuotas > 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.