Dell PowerStore

Configuración del uso compartido de archivos multiprotocolo

4.1

Febrero de 2025
Rev. A01

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.

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.

Tabla de contenido

1

Descripción general

Este capítulo incluye la siguiente información:

Temas:

Acerca del uso compartido de archivos multiprotocolo en PowerStore

Para acceder a un archivo de datos compartido por un servidor NAS a través de la red, los clientes de host utilizan principalmente dos protocolos de archivos: SMB y NFS. Los clientes de Windows utilizan el protocolo SMB y los clientes de UNIX utilizan el protocolo NFS. Los protocolos NFS y SMB tienen muchas diferencias; algunas de ellas se describen en la siguiente tabla:

Tabla 1. Principales diferencias entre los protocolos de NFS y SMB

Funciones	NFS	SMB
Identificación de usuario	Usa un identificador de usuario (UID) y un identificador de grupo (GID).	Usa un identificador de seguridad (SID).
Política de bloqueo	Se recomienda usar bloqueos de rango de NFSv3, en cambio, los bloqueos de rango de NFSv4 son recomendados u obligatorios (opción predeterminada).	Los bloqueos de rango de SMB son obligatorios.
Autenticación de usuarios	Uno de los siguientes elementos gestiona la autenticación: • Un inicio de sesión local anterior en otro sistema UNIX • Un servicio de directorio de UNIX (NIS o LDAP), que busca el UID/GID del usuario. • Archivos de grupo y contraseñas locales, las cuales buscan el UID/GID del usuario.	Active Directory gestiona la autenticación, la cual busca el SID de un usuario. Esto requiere NTP y DNS.
Reglas de seguridad	Utiliza la credencial de UNIX asociada con el usuario autenticado para consultar los bits de modo (NFSv3) o los derechos de acceso en la ACL de NFSv4.	Utiliza la credencial de Windows asociada con el usuario autenticado para consultar la ACL de acceso de SMB.
Cambie el nombre de la política	Se permite cambiar el nombre de un componente de un archivo abierto.	No se permite cambiar el nombre de un componente de un archivo abierto.

PowerStore admite un entorno combinado de NFS y SMB, lo que proporciona acceso simultáneo a los mismos datos de NFS (v3 y v4) y SMB. La funcionalidad del servidor NAS está determinada por la configuración del protocolo de uso compartido del servidor. Para habilitar el multiprotocolo, seleccione el protocolo de uso compartido SMB y NFS como parte de la configuración del servidor NAS. Cree un sistema de archivos a partir de este servidor NAS y, finalmente, cree ambos recursos compartidos de NFS y SMB en ese sistema de archivos.

Para configurar la funcionalidad multiprotocolo, debe agregar el servidor NAS a un dominio de Windows Active Directory y configurar un servicio de directorio de UNIX (LDAP o NIS) o una contraseña local y archivos de grupo correspondientes al servidor NAS, o ambas opciones. Para usar 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 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.

Los nombres de usuario en un entorno de NFS y en un entorno de SMB deben coincidir carácter por carácter. Si hay discrepancias en los nombres de usuario, puede configurar un archivo de asignación de usuarios (`ntxmap`) para asignar cada nombre de NFS al nombre de SMB correspondiente y viceversa. También puede configurar los nombres predeterminados de cuenta de UNIX y Windows. El sistema utiliza el nombre predeterminado de la cuenta de Windows cuando no puede encontrar una coincidencia de nombre de SMB en NFS y el nombre predeterminado de la cuenta de UNIX cuando no puede encontrar una coincidencia de nombre de NFS en SMB.

NOTA: Cuando varios usuarios utilizan las cuentas predeterminadas, las cuotas pueden verse afectadas.

Cuando configura un sistema de archivos que soporta el acceso multiprotocolo, también debe seleccionar una política de acceso para administrar el control de acceso de usuarios al sistema de archivos. Para obtener información detallada sobre cómo funciona la seguridad y el acceso a archivos en un entorno multiprotocolo, consulte Análisis en profundidad: seguridad del sistema de archivos y acceso en un entorno multiprotocolo.

En las siguientes ilustraciones, se muestran los pasos generales necesarios para configurar el uso compartido de archivos multiprotocolo.

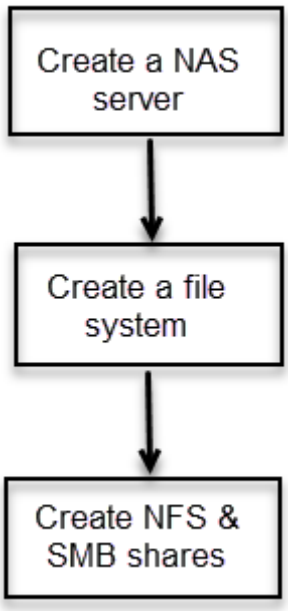

Ilustración 1. Pasos generales para configurar el uso compartido de archivos multiprotocolo

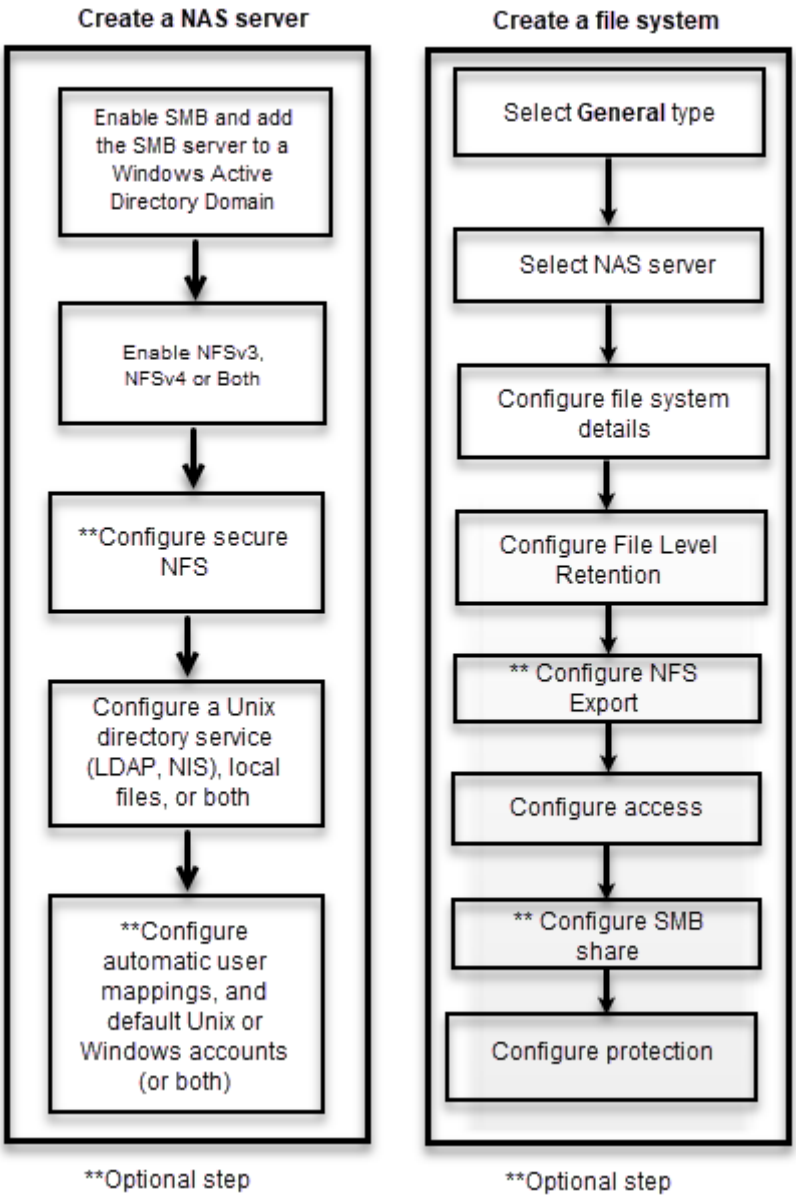

Ilustración 2. Pasos generales para configurar el uso compartido de archivos multiprotocolo (continuación)

2

Análisis en profundidad: seguridad y acceso al sistema de archivos en un entorno multiprotocolo

Este capítulo incluye la siguiente información:

Temas:

Seguridad en los objetos de los sistemas de archivos

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

El ajuste predeterminado de la seguridad nativa mantiene dos conjuntos de permisos por separado por cada archivo y el protocolo que se utiliza para acceder al archivo determina el conjunto de permisos que se consulta. Si se utiliza el protocolo SMB, se consultan las ACL. Si se utiliza el protocolo NFS, se consultan los bits de modo de NFSv3 o la ACL de NFSv4.

NOTA: El acceso del cliente mediante el protocolo SMB1 está deshabilitado de manera predeterminada debido a posibles vulnerabilidades de seguridad. Si se requiere acceso del cliente mediante SMB1, se puede habilitar mediante la modificación del parámetro `cifs.smb1.disabled`. Se recomienda utilizar SMB2 como mínimo para mejorar la seguridad y aumentar la eficiencia.

Modelo de seguridad nativo

El modelo de seguridad nativo corresponde al ajuste predeterminado. Este modelo administra por separado el acceso de cada protocolo con su propia seguridad nativa:

- La seguridad de los recursos compartidos de NFS utiliza los bits de modo de UNIX o la ACL de NFSv4.
- La seguridad de los recursos compartidos de SMB utiliza la lista de control de acceso (ACL) de SMB.

Los dos conjuntos de permisos son independientes y no están sincronizados. Los cambios de permisos de los bits de modo de UNIX de NFSv3 o la ACL de NFSv4 se sincronizan sin cambiar la ACL de SMB. Los cambios en la ACL de SMB no afectan a los bits de modo de UNIX de NFSv3 ni la ACL de NFSv4.

El conjunto de permisos que se aplica depende del protocolo de acceso en uso.

Modelo de seguridad de UNIX

Cuando se selecciona la política de UNIX, se desestiman los intentos de modificación de la seguridad en el nivel de archivos desde el protocolo de SMB, como las modificaciones de las listas de control de acceso (ACL). A los derechos de acceso de UNIX se les denomina los bits de modo de UNIX de NFSv3 o la ACL de NFSv4 de un objeto del sistema de archivos. Una cadena de bits representa los bits de modo. Cada bit equivale a un modo o derecho de acceso otorgado al usuario que posee el archivo, al grupo asociado con el objeto del sistema de archivos y a todos los demás usuarios. Los bits de modo de UNIX se representan como tres conjuntos de triadas rwx (lectura,

escritura y ejecución) concatenadas para cada categoría de usuarios (usuario, grupo u otro). Una ACL es una lista de usuarios y grupos de usuarios mediante la cual se controla el acceso a servicios y la negación de estos.

El modelo de seguridad de UNIX utiliza los bits de modo de UNIX de NFSv3 o la ACL de NFSv4 de ambos protocolos. Cuando se solicita acceso a SMB, la credencial de UNIX que se crea desde el USD o los archivos locales se utiliza para buscar permisos en los bits de modo de NFSv3 o la ACL de NVSv4. Cuando se modifican los bits de modo de UNIX de NFSv3 o las ACL de NFSv4, se actualizan los permisos de ACL de SMB.

Se permiten cambios en los permisos de ACL de SMB a fin de evitar interrupciones, pero estos permisos no se conservan.

Modelo de seguridad de Windows

El modelo de seguridad de Windows se basa principalmente en derechos de objetos, lo cual implica el uso de un descriptor de seguridad (SD) y de su ACL. Cuando se selecciona una política de SMB, se desestiman las modificaciones en los bits de modo en el protocolo NFS.

El acceso a un objeto del sistema de archivos se basa en si los permisos se configuraron en Permitir o Rechazar mediante el uso de un SD. El SD describe el propietario del objeto y los SID de grupo para el objeto, junto con sus ACL. Una ACL es parte del descriptor de seguridad de cada objeto. Cada ACL contiene entradas de control de acceso (ACE). A su vez, cada ACE contiene un único SID que identifica a un usuario, un grupo o una unidad de sistema, y una lista de derechos que se rechazan o permiten en cuanto a ese SID.

El modelo de seguridad de Windows utiliza la ACL de SMB para ambos protocolos. Cuando se solicita acceso a NFS, la credencial de Windows que se crea en la DC/LGDB se utiliza para buscar permisos en la ACL Cuando se modifican los permisos de ACL de SMB, se actualizan los bits de modo de UNIX de NFSv3 o las ACL de NFSv4. Se deniegan los cambios de permisos en los bits de modo de UNIX de NFSv3 y la ACL de NFSv4.

File system access

El acceso a archivos se proporciona a través de servidores NAS, los cuales contienen sistemas de archivos en que se almacenan datos. El servidor NAS proporciona acceso a estos datos para los protocolos de archivos NFS y SMB mediante el uso compartido de los sistemas de archivos a través de recursos compartidos SMB y NFS. El servidor NAS permite el uso compartido de los mismos datos entre SMB y NFS, y proporciona acceso simultáneo de SMB y NFS a un sistema de archivos. La asignación de usuarios de Windows a usuarios de UNIX y la definición de reglas de seguridad (bits de modo, ACL e información de identificación) se deben considerar y configurar para el uso compartido multiprotocolo.

Mapeo de usuarios

En un contexto multiprotocolo, se debe hacer coincidir un usuario de Windows con un usuario de UNIX. Sin embargo, un usuario de UNIX se debe mapear a un usuario de Windows solamente cuando la política de acceso es Windows. Esta coincidencia es necesaria para que se pueda aplicar la seguridad del sistema de archivos, incluso si no es nativa para el protocolo.

Los siguientes componentes son parte del mapeo de usuarios:

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

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

Servicios de directorio de UNIX y archivos locales

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

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

Los servicios compatibles son:

- LDAP
- NIS
- Archivos locales

- Ninguno (la única asignación posible se hace a través del usuario predeterminado).

Cuando está habilitado el uso compartido multiprotocolo, debe estar habilitado un UDS, los archivos locales o ambas opciones del servidor NAS. El orden de búsqueda de UDS determina cuál opción se utiliza para la asignación de usuarios.

Solucionadores de Windows

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

- Indicar el nombre de cuenta de Windows correspondiente a un identificador de seguridad (SID) específico.
- Indicar el SID correspondiente a un nombre de cuenta de Windows específico.

Los solucionadores de Windows son:

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

Caché de mapeo seguro

La caché de asignación segura (secmap) es una caché en que se almacenan asignaciones de usuarios que se han conectado al servidor NAS. Por cada usuario, se almacenan el SID, el nombre de usuario y el UID. en secmap solo se almacenan las asignaciones que genera el mecanismo de asignación estándar.

Almacenar asignaciones de SID a UID y GID primario y de UID a SID en una caché local garantiza la coherencia en todos los sistemas de archivos del servidor NAS.

El almacenamiento de asignaciones de usuario en secmap reduce el tráfico de red y aumenta la eficiencia. Una vez que se almacena una asignación de usuarios en secmap, el servidor NAS aprovecha la caché local para futuras búsquedas de asignaciones.

ntxmap

ntxmap es un archivo local opcional que se utiliza para proporcionar traducciones de nombres entre protocolos. Cuando hay alguna incoherencia entre los nombres de usuario, ntxmap se utiliza para asociar una cuenta de Windows a una cuenta de UNIX. Por ejemplo, si hay un usuario con una cuenta denominada Gerald en Windows y una cuenta en UNIX se llama Gerry, se usa ntxmap para establecer la correlación entre ambas cuentas.

ntxmap también se puede utilizar en traducciones avanzadas de nombres, como la conversión de varios nombres de usuario a un solo nombre de usuario y la provisión de conversiones de nombres.

NOTA: ntxmap solo proporciona traducciones de nombres de usuario entre protocolos y no proporciona ningún ID a asignaciones de nombres de usuario.

Mapeo de SID a UID y GID primario

La siguiente secuencia corresponde al proceso que se usa para resolver una asignación de SID a UID con un GID primario:

1. El SID se busca en secmap. Si el SID se encuentra, se resuelven las asignaciones del UID y el GID primario.
2. Si el SID no se encuentra en secmap, se debe buscar el nombre de usuario de Windows relacionado con el SID.
   a. El SID se busca en la base de datos del grupo local (LGDB) para determinar si se trata de un usuario local. Si el SID se encuentra, el nombre de Windows relacionado será `SMB_SERVER\USER`. Dado que este es un usuario local con acceso de solo SMB, no se requiere ninguna asignación de UNIX.
   b. Si el SID no se encuentra en la LGDB, se busca en la DC del dominio. Si el SID se encuentra en el dominio, el nombre relacionado de Windows es `DOMAIN\USER`.
   c. Si el SID no se puede resolver, se niega el acceso. La asignación fallido se agrega a la base de datos persistente de secmap.
3. Si la cuenta predeterminada de UNIX no se utiliza, el nombre de Windows se traduce a un nombre de UNIX mediante ntxmap.
   a. Si el nombre de Windows se encuentra en ntxmap, la entrada se utiliza como el nombre de UNIX.
   b. Si el nombre de Windows no se encuentra en ntxmap o si ntxmap está deshabilitado, el nombre de Windows se utiliza como el nombre de UNIX.
4. El nombre de UNIX se busca en los archivos locales o el UDS para encontrar el UID y el GID primario.
   a. Si se encuentra el nombre de usuario de UNIX, se resuelve la asignación del UID y el GID primario. La asignación correcta se agrega a la base de datos persistente de secmap.

b. Si el nombre de usuario de UNIX no se encuentra, pero la característica de asignación automática de las cuentas de Windows sin asignar está activada, el UID se asigna automáticamente. La asignación correcta se agrega a la base de datos persistente de secmap.
c. Si no se encuentra el nombre de usuario de UNIX, pero hay configurada una cuenta predeterminada de UNIX, el UID y el GID primario se asignan a esta. La asignación fallido se agrega a la base de datos persistente de secmap.
d. Si el nombre de usuario de UNIX no se puede resolver, se niega el acceso. La asignación fallido se agrega a la base de datos persistente de secmap.

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

En el siguiente diagrama, se ilustra el proceso utilizado para resolver una asignación de SID a un UID con GID primario:

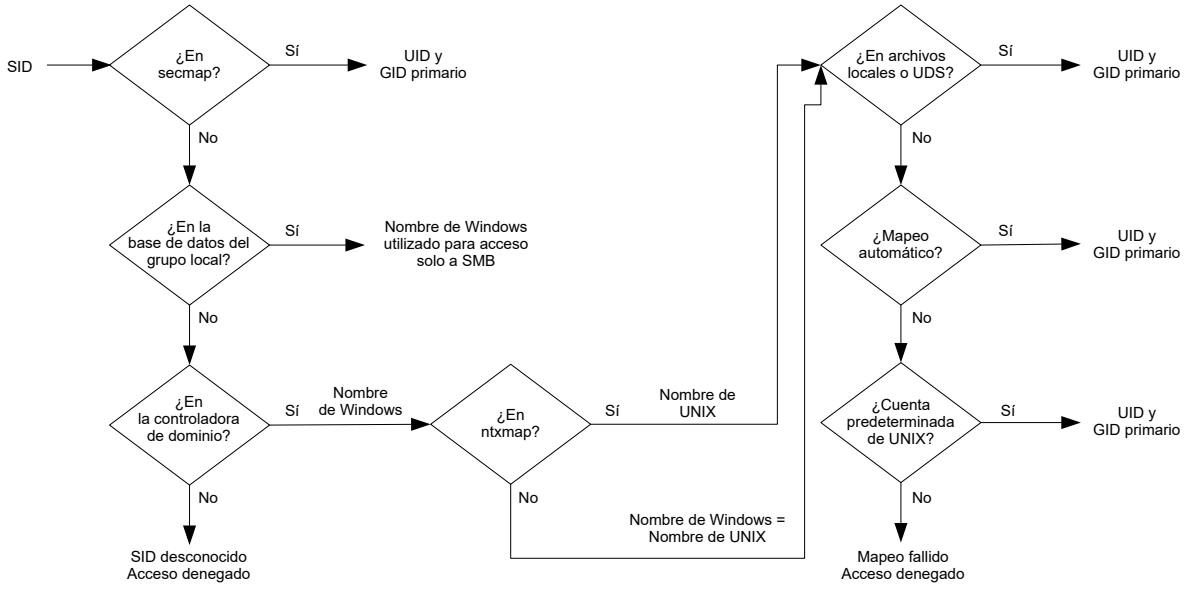

Ilustración 3. Proceso para resolver un mapeo de un SID a un UID, GID primario

Mapeo de UID a SID

La siguiente secuencia corresponde al proceso que se usa para resolver una asignación de UID a un SID:

1. El UID se busca en secmap. Si el UID se encuentra, el mapeo de SID se resuelve.
2. Si el UID no se encuentra en secmap, se debe buscar el nombre de UNIX relacionado con el UID.
   a. El UID se busca en los archivos locales o el UDS. Si el UID se encuentra, el nombre de UNIX relacionado corresponde al nombre de usuario.
   b. Si el UID no se encuentra en el UDS, pero hay una cuenta predeterminada de Windows, el UID se asigna a la cuenta predeterminada de Windows. Si no existe, el usuario predeterminado de Windows se agrega a la base de datos persistente de secmap.
   c. Si el UID no se resuelve, se niega el acceso.
3. Si no se usa la cuenta predeterminada de Windows, el nombre de UNIX se traduce a un nombre de Windows mediante ntxmap.
   a. Si el nombre de UNIX se encuentra en ntxmap, la entrada se utiliza como el nombre de Windows.
   b. Si el nombre de UNIX no se encuentra en ntxmap o si ntxmap está deshabilitado, el nombre de UNIX se utiliza como el nombre de Windows.
4. El nombre de Windows se busca en la DC o la LGDB para encontrar el SID.
   a. El nombre de Windows se busca en la DC. Si el nombre de Windows se encuentra, el mapeo de SID se resuelve.
   b. Si el nombre de Windows contiene un punto (.) y la parte del nombre tras el último punto coincide con un nombre de servidor SMB, se realiza una búsqueda en la LGDB de ese servidor SMB para resolver la asignación de SID. Si el nombre de Windows se encuentra, el mapeo de SID se resuelve.
   c. Si el nombre de Windows no se encuentra, pero hay una cuenta predeterminada de Windows, el SID se mapea al de esa cuenta predeterminada de Windows. Si no existe, el usuario predeterminado de Windows se agrega a la base de datos persistente de secmap.
   d. Si el nombre de Windows no se puede resolver, se niega el acceso.

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

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

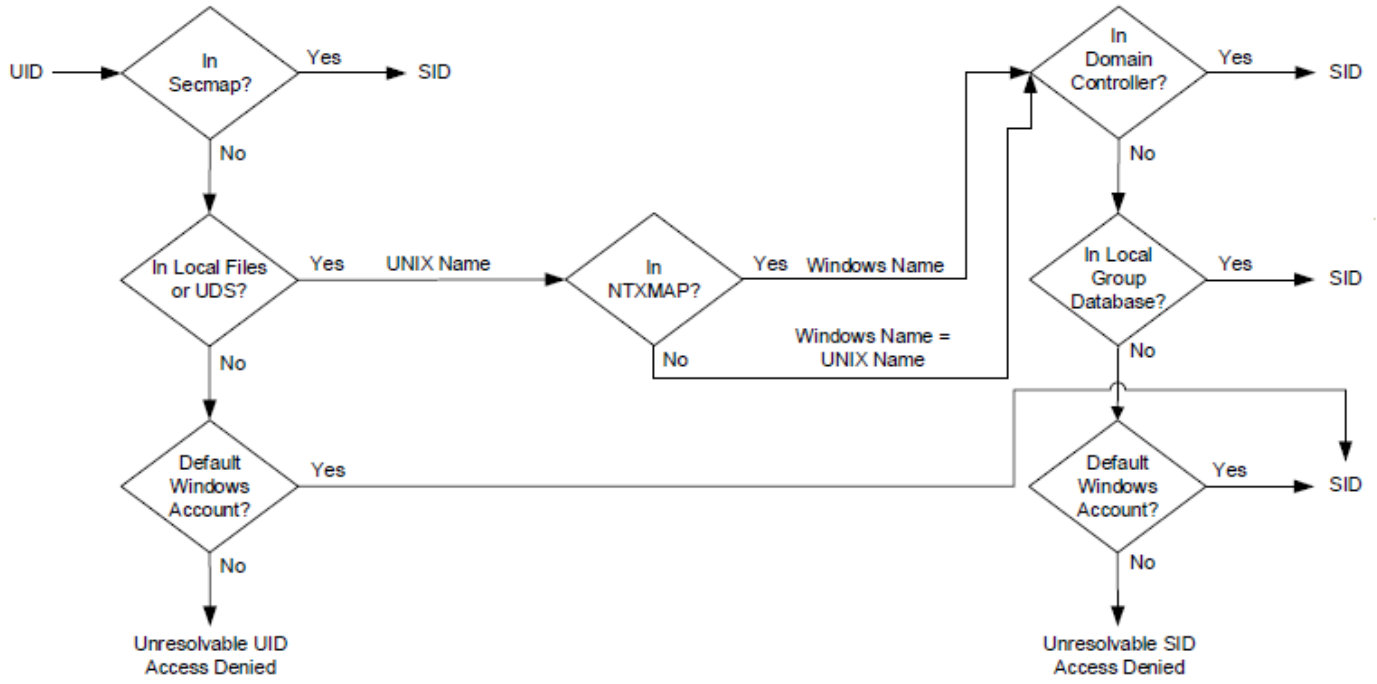

Ilustración 4. Proceso que se utiliza para resolver una asignación de un UID a un SID

Políticas de acceso para NFS, SMB y FTP

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

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

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

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

Tabla 2. Políticas de acceso

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

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

Credenciales para la seguridad en el nivel de archivos

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

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

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

Una caché de credenciales persistente se usa para lo siguiente:

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

Hay una instancia de caché para cada servidor NAS.

Concesión de acceso a usuarios no mapeados

El ambiente multiprotocolo requiere lo siguiente:

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

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

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

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

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

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

Dado que el sistema de archivos de PowerStore se basa en UNIX, todos los datos que se escriben deben estar asociados con un UID y un GID primario válidos. Los usuarios de NFS tienen un UID y un GID primario disponibles de forma nativa. Sin embargo, los usuarios de SMB deben tener un mapeo que convierta su SID nativo a un UID y un GID primario. Se requiere una asignación inversa de UID a SID solo si se aplican permisos de Windows (política de acceso de Windows).

La característica de asignación automática permite tener la capacidad de generar y asignar automáticamente un UID único a usuarios de Windows que no tengan una asignación de UID. Esta característica permite el acceso al recurso compartido a los usuarios sin asignar, en lugar de denegárselos. Dado que cada usuario tiene un UID único, las características basadas en UID, como las cuotas de usuario, de todos modos pueden rastrear correctamente el consumo de cada usuario individual.

La asignación automática viene habilitada de manera predeterminada en servidores NAS de solo SMB y multiprotocolo. Si la característica está habilitada, la capacidad de configurar cuentas predeterminadas se deshabilita. Como el sistema asigna automáticamente cada UID, utilice esta característica solo en entornos en que el UID de estos usuarios no sea crítico. En entornos en que los administradores desean controlar las asignaciones de UID, deshabilite la característica. Si la asignación automática está deshabilitada y no hay otros métodos de asignación disponibles para los usuarios sin asignar, se les niega el acceso al recurso compartido.

Credencial de UNIX para solicitudes NFS

Se debe utilizar una credencial de UNIX para manejar las solicitudes de NFS correspondientes a un sistema de archivos de solo NFS o multiprotocolo con una política de acceso de UNIX o nativa. La credencial de UNIX está siempre incorporada en cada solicitud; sin embargo, está limitada a 16 grupos adicionales.

Para habilitar la propiedad Credenciales extendidas, seleccione **Almacenamiento** > **Servidores NAS** > **[Servidor NAS]** > **Protocolos de uso compartido** > **Servidor NFS** y active la opción **Credenciales extendidas**. Mediante la habilitación de las credenciales extendidas de UNIX, es posible crear una credencial con más de 16 grupos. Si se configura esta opción, se consulta al UDS activo con el UID para obtener el GID primario y todos los GID de grupo a los cuales pertenece. Si el UID no se encuentra en el UDS, se usa la credencial de UNIX integrada en la solicitud.

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

Credencial de UNIX para solicitudes SMB

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

Credencial de Windows para solicitudes SMB

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

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

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

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

Credencial de Windows para solicitudes NFS

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

Ajustes de seguridad del sistema de archivos multiprotocolo

PowerStore ofrece personalización de acceso, cambio de nombre y políticas de bloqueo a un sistema de archivos multiprotocolo.

Políticas de acceso del sistema de archivos

Puede seleccionar una de las siguientes políticas de acceso para un sistema de archivos multiprotocolo:

- Seguridad nativa
- Seguridad de Unix
- Seguridad de Windows

Para obtener información sobre estas políticas de acceso, consulte Políticas de acceso de NFS, SMB y FTP.

Políticas de cambio de nombre del sistema de archivos

Puede seleccionar una de las siguientes políticas de cambio de nombre para un sistema de archivos multiprotocolo. Una política de cambio de nombre controla las circunstancias en que los clientes de NFS y SMB pueden cambiar el nombre de un directorio. El ajuste puede ser uno de los siguientes:

Tabla 3. Políticas de cambio de nombre de un sistema de archivos multiprotocolo

Configuración	Descripción
Todo permitido	Todos los clientes NFS y SMB pueden cambiar el nombre de los directorios sin restricciones.
SMB prohibido	Solo los clientes de NFS pueden cambiar el nombre de los directorios sin restricciones. Si hay al menos un archivo abierto en un directorio o en uno de sus subdirectorios, un cliente de SMB no puede cambiar el nombre del directorio. Por ejemplo, si la ruta de un archivo es C:\Dir1\Dir2\Dir3\File1.txt y un cliente de SMB abre File1, no se puede cambiar el nombre de Dir1, Dir2 ni Dir3.
Todo prohibido	(Opción predeterminada) Si hay al menos un archivo abierto en un directorio o en uno de sus subdirectorios, los clientes de NFS y SMB no pueden cambiar el nombre del directorio.

Políticas de bloqueo del sistema de archivos

SMB y NFS tienen su propia semántica de bloqueo. Las especificaciones del protocolo definen los rangos de bloqueo como obligatorios para SMB, pero pueden ser recomendados para NFS. NFSv3 utiliza un protocolo separado (NLM) que siempre se recomienda. NFSv4 tiene una administración de bloqueo integrada en el protocolo en sí, pero también puede ser recomendada u obligatoria según la implementación.

La propiedad de una política de bloqueo se utiliza para definir el comportamiento. Puede seleccionar una de las siguientes políticas de bloqueo para un sistema de archivos multiprotocolo:

Tabla 4. Políticas de bloqueo de sistemas de archivos

Configuración	Descripción
Obligatorio	Esta política utiliza los protocolos SMB y NFSv4 para administrar los bloqueos de rango de un archivo que está utilizando otro usuario. Si hay acceso simultáneo a los mismos datos bloqueados, una política de bloqueo obligatoria impide el daño de los datos.
Asesoría	(Opción predeterminada) En respuesta a las solicitudes de bloqueo, esta política informa que hay un conflicto de bloqueo de rango, pero no impide el acceso al archivo. Esta política permite que las aplicaciones NFSv3 que no están en conformidad con un bloqueo de rango continúen funcionando, pero los datos se exponen a daños si hay escrituras simultáneas.

3

Configuración de un servidor NAS para el uso compartido de archivos multiprotocolo

Este capítulo incluye la siguiente información:

Temas:

Configuración de servidores NAS para el uso compartido de archivos multiprotocolo

La configuración de un servidor NAS multiprotocolo en la interfaz de usuario requiere que se especifique la siguiente información:

- Información de redes para el servidor NAS (interfaces IP, máscara de red, gateway, VLAN, etc.)
- La dirección IP del servidor DNS y el dominio de DNS para comunicarse con AD.
- La credencial de un usuario de Active Directory (AD) con privilegios para unirse a AD.
- La información del servicio de directorio de UNIX (UDS). Para NIS, esta información incluye el nombre de dominio y la dirección IP de los servidores NIS. Para LDAP, esta información incluye la dirección IP de los servidores LDAP, el DN base e información de autenticación. En el caso de los archivos locales, esta información incluye los archivos passwd y group.

En la siguiente tabla, se describen las configuraciones de servidor NAS disponibles para servidores NAS multiprotocolo:

Tabla 5. Configuraciones de servidor NAS para servidores NAS multiprotocolo

Ambiente operativo:	Función del servidor NAS	Opciones de configuración recomendadas
Entorno equilibrado de UNIX y Windows; es decir, cuando el sistema requiere un mapeo 1:1 de todos los usuarios o la mayoría de estos.	Habilite el acceso de SMB y NFS a los mismos datos de los sistemas de archivos.	1. En el asistente Crear un servidor NAS, realice lo siguiente: • En la pestaña **Protocolos de uso compartido**, seleccione **SMB** junto con **NFSv3** o **NFSv4**. • Una el servidor NAS a un dominio de Windows AD. • Configure un UDS (LDAP o NIS), archivos locales o ambos para administrar las identidades de los usuarios. • Configure DNS. • De manera opcional, configure el mapeo automático de usuarios o las cuentas predeterminadas. • Configure el orden de búsqueda de UDS. 2. De manera opcional, personalice los mapeos entre cuentas de usuario de Windows y cuentas de usuario de UNIX mediante la modificación y la carga de un archivo de mapeo de usuarios con reglas de asignación de nombres avanzadas (ntxmap). Debe optar por esto cuando los nombres de los mismos usuarios sigan diferentes reglas de asignación de nombres en Windows y UNIX.
Entorno UNIX con la capacidad de acceder a datos del sistema de archivos a través de SMB	Habilite el acceso de NFS a datos del sistema de archivos y, de manera opcional, habilite	1. Siga los pasos de la fila Entorno equilibrado de UNIX y Windows para crear un servidor NAS, configurar un servicio de directorio de UNIX o archivos locales y, opcionalmente, personalizar los

Tabla 5. Configuraciones de servidor NAS para servidores NAS multiprotocolo (continuación)

Ambiente operativo:	Función del servidor NAS	Opciones de configuración recomendadas
	el acceso de SMB a los mismos datos del sistema de archivos para algunas cuentas de Windows.	mapeos entre cuentas de usuario de Windows y cuentas de usuario de UNIX. 2. De manera opcional, configure una cuenta de usuario predeterminada de UNIX. Todas las cuentas de Windows no mapeadas se mapean a esta cuenta de usuario. Si opta por usar mapeos automáticos de usuarios, no puede controlar qué UID tiene cada usuario, pero puede usar cuotas. **NOTA:** Si utiliza una cuenta predeterminada de UNIX para los usuarios de SMB, estos usuarios se mapean a un UID. Por lo tanto, se aplica una sola cuota de usuario a todos estos usuarios. 3. Después de crear sistemas de archivos para el servidor NAS, se recomienda especificar una política de acceso al sistema de archivos de UNIX.
Ambiente Windows con la capacidad de obtener acceso a datos del sistema de archivos a través de NFS	Habilite el acceso de SMB a datos del sistema de archivos y, de manera opcional, habilite el acceso de NFS a los mismos datos del sistema de archivos para algunas cuentas de UNIX.	1. Siga los pasos de la fila Entorno equilibrado de UNIX y Windows para crear un servidor NAS y, opcionalmente, use ntxmap para personalizar los mapeos entre cuentas de usuario de Windows y cuentas de usuario de UNIX. 2. De manera opcional, configure una cuenta de usuario predeterminada de Windows. Todas las cuentas de UNIX no mapeadas se mapean a esta cuenta de usuario. **NOTA:** Si utiliza una cuenta predeterminada de Windows para los usuarios de UNIX, estos usuarios se mapean a un SID. Por lo tanto, se aplica una sola cuota de usuario a todos estos usuarios. 3. Después de crear sistemas de archivos para el servidor NAS, se recomienda especificar una política de acceso al sistema de archivos de Windows.

Crear un servidor NAS para uso compartido de archivos multiprotocolo (SMB y NFS)

Requisitos previos

Obtenga la siguiente información:

- Información de redes para el servidor NAS (interfaces IP, máscara de red, gateway, VLAN, etc.)
- ID de VLAN, si el puerto del switch es compatible con el etiquetado de VLAN.
- Información de AD, lo que incluye el nombre del sistema SMB (que se utiliza para acceder a recursos compartidos de SMB) y las credenciales del administrador de dominio o de un usuario del dominio con privilegios para unirse a AD. De manera opcional, puede especificar el nombre de NetBIOS y la unidad organizacional. El nombre de NetBIOS cambia a un valor predeterminado para los primeros 15 caracteres del nombre del servidor SMB. La unidad organizacional se configura de manera predeterminada en CN=Computers.
- Información del servicio de directorio de UNIX (UDS) para NIS, LDAP u otros archivos locales. El UDS proporciona el UID y el GID de UNIX para los usuarios de AD.

  NOTA: Puede configurar las asignaciones de algunos usuarios en el UDS y permitir que los demás se asignen a través de la cuenta predeterminada o la asignación automática de usuarios.

- Información del dominio y el servidor DNS.
- Política de protección (opcional).

Sobre esta tarea

Se recomienda balancear el número de servidores NAS en ambos nodos.

En una configuración multiprotocolo, se recomienda unir el servidor SMB a un dominio de Active Directory para resolver SID hacia y desde nombres de usuario de Windows. Cuando se establece una conexión a un sistema de archivos multiprotocolo, los usuarios de dominio realizan la asignación de usuarios para crear una asignación a partir del SID de Windows al UID de UNIX y al GID primario.

Los servidores SMB independientes solo admiten usuarios locales (previstos para el acceso solo a través de SMB y no mapeados) y no tendrían los mapeos necesarios para una configuración multiprotocolo adecuada.

Debido a que es poco probable que el UID del usuario local en el sistema de archivos coincida con el UID configurado en el cliente de UNIX, los dos UID se ven como dos usuarios diferentes desde el punto de vista del servidor NAS. En consecuencia, el mismo usuario tiene permisos incoherentes en diferentes protocolos.

Puede usar una de las siguientes soluciones alternativas:

- Configure manualmente UID para asegurarse de que sean coherentes con el servidor SMB local: cree todos los usuarios locales en un servidor SMB, determine los UID de los usuarios locales y, a continuación, configure los clientes de UNIX para que utilicen esos UID.
- Si la seguridad no representa un problema, puede usar permisos abiertos.
- Si todos pueden acceder a los archivos, no es necesario mantener permisos coherentes entre los protocolos.

Pasos

1. Seleccione **Almacenamiento** > **Servidores NAS**.
2. En la pestaña **Servidores NAS**, haga clic en **Crear**.
3. En la página **Detalles**, especifique el nombre del servidor NAS, la interfaz de red, la dirección IP, la máscara de subred y el ID de la VLAN.
4. Seleccione **Siguiente** para abrir la página **Protocolo de uso compartido**.
5. En la página **Seleccionar protocolo de uso compartido**, seleccione **SMB** y **NFSv3** o **NFSv4** y, luego, **Siguiente**.
6. En la pestaña **Ajustes del servidor de Windows** del campo Tipo de servidor de Windows, seleccione **Unirse al dominio de Active Directory** y complete la información de AD requerida.
7. De manera opcional, seleccione **Opciones avanzadas** para cambiar el nombre de NetBIOS y la unidad organizacional predeterminados. Seleccione **Guardar** y, luego **Siguiente**.
8. En la pestaña **Servicios de directorio de UNIX**, configure uno de los siguientes servicios de directorio:
   - Archivos locales
   - NIS
   - LDAP
   - Los archivos locales y NIS o LDAP
9. De manera opcional, seleccione **NFS seguro** y, a continuación, cambie los **Ajustes de NFS seguro** para habilitar el NFS seguro.
10. En la página **DNS**, seleccione la opción **Habilitar servidor DNS** e indique la siguiente información:
    - Protocolo de transporte DNS: UDP (valor predeterminado), TCP
    - Dominio
    - Dirección IP de los servidores DNS
11. En la página **Política de protección**, puede seleccionar una política de protección para el servidor NAS.
12. En la página **Política de QoS de archivos**, puede seleccionar una política de QoS de archivos para el servidor NAS.
13. Seleccione **Finalizar** para crear el servidor NAS.

Configurar el servicio de directorio de UNIX de un servidor NAS

Cuando configure un servidor NAS que soporta el uso compartido de archivos multiprotocolo, también debe configurar una forma de buscar información de identidad, como UID, GID, grupos de red, etc.

Existen tres maneras de configurar las búsquedas de identidad:

- Utilizar los archivos locales, ya sea solos o con un UDS.
- Configurar un servicio de directorio de UNIX (UDS) mediante NIS.
- Configurar un UDS mediante LDAP.

Si va a crear un servidor NAS, utilice la ventana **Configurar servicio de directorio de UNIX** del asistente **Crear servidor NAS** para configurar las búsquedas de identidad.

Si va a configurar un UDS para un servidor NAS existente, acceda a la pestaña **Servicios de asignación de nombres** para ver las opciones de búsqueda de identidad:

1. En PowerStore Manager, seleccione **Almacenamiento** > **Servidores NAS**.
2. Haga clic en un servidor NAS para seleccionarlo.
3. Seleccione la pestaña **Servicios de asignación de nombres**.

Para especificar el orden de búsqueda de un servidor NAS existente, seleccione la pestaña **Asignación de usuarios** y configure el orden de búsqueda. Los servicios de directorio que haya configurado se pueden seleccionar en el menú desplegable. Las opciones posibles son:

- LDAP
- NIS
- Archivos locales
- Local y, a continuación, NIS
- Local y, a continuación, LDAP

Usar archivos locales

Los archivos de contraseña y grupo locales se pueden utilizar para resolver ID y nombres de usuario. El archivo de contraseña utiliza el mismo formato y nomenclatura que los sistemas operativos basados en UNIX, por lo que también se podría aprovechar un archivo existente de un host para el servidor NAS.

Los elementos relevantes para el servidor NAS son el nombre de usuario, la contraseña con hash (utilizada para la autenticación de FTP), el UID y el GID primario. El resto de los elementos del archivo de contraseña pueden permanecer en blanco.

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

- El archivo se crea con la nomenclatura correcta (se requieren seis signos de dos puntos por cada línea). Consulte la plantilla para conocer más detalles.
- Cada usuario tiene un nombre y UID únicos.

Habilitación de archivos locales para un nuevo servidor NAS

Requisitos previos

Puede descargar la versión actual de los archivos locales desde el servidor NAS, lo que también proporciona la nomenclatura, ejemplos y detalles adicionales. Después de editar el archivo con los detalles del usuario, vuelva a cargarlo en el servidor NAS.

Sobre esta tarea

Realice los siguientes pasos para permitir el uso de archivos locales correspondientes a los servicios de directorio durante la creación de un servidor NAS:

Pasos

1. En la ventana **Servicios de directorio de UNIX** en el asistente **Crear un servidor NAS**, seleccione **Usar archivos locales**.
2. Cree el archivo de contraseña para el UDS. Para ver la plantilla del archivo de contraseña, seleccione **Plantilla de archivo de contraseña**.
3. Para cargar el archivo de contraseña en el servidor NAS, seleccione **Seleccionar archivo de contraseña**.

Habilitación de archivos locales para un servidor NAS existente

Pasos

1. En PowerStore Manager, seleccione **Almacenamiento** > **Servidores NAS**.
2. Seleccione el servidor NAS y, luego la pestaña **Servicios de nomenclatura**.
3. Seleccione la pestaña **Archivos locales**.
4. Haga clic en la flecha hacia abajo del archivo correspondiente para recuperarlo y realice los cambios necesarios.
5. Para cargar los archivos, seleccione **Cargar archivos locales**.

6. Seleccione el tipo de archivo y haga clic en **Seleccionar archivo**.
7. Seleccione el archivo y, a continuación, seleccione **Cargar**.

Configurar un servicio de directorio de UNIX mediante NIS

Puede usar NIS para UDS. Para configurar NIS, proporcione la siguiente información:

- Dominio de NIS
- Direcciones IP del servidor NIS

Si proporciona direcciones de varios servidores NIS, se pueden mover hacia arriba o hacia abajo en la lista de prioridades.

Configuración de un UDS mediante NIS para un servidor NAS nuevo

Pasos

1. En la ventana **Servicios de directorio de UNIX** en el asistente **Crear un servidor NAS**, seleccione **Habilitar un directorio de UNIX con NIS o LDAP**.
2. En la ventana **Servicios de directorio de UNIX**, seleccione **NIS**.
3. Ingrese un dominio de NIS y agregue hasta tres direcciones IP para los servidores NIS.

Configuración de un UDS mediante NIS para un servidor NAS existente

Pasos

1. En PowerStore Manager, seleccione **Almacenamiento** > **Servidores NAS**.
2. Seleccione el servidor NAS y, luego la pestaña **Servicios de nomenclatura**.
3. Seleccione la pestaña **UDS**.
4. En el campo **Servicio de directorio de Unix**, seleccione **NIS**.
5. Ingrese el dominio de NIS y agregue hasta tres direcciones IP para los servidores NIS.
6. Seleccione **Aplicar**.

Configurar un servicio de directorio de UNIX 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.

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

- La configuración de LDAP se adhiera a uno de los esquemas soportados.
- Todos los contenedores especificados en el archivo `ldap.conf` son para contenedores válidos y existentes.
- Cada usuario LDAP está configurado con un UID único.

También puede usar la opción `-ldap` del comando de servicio `svc_nas_tools` para solucionar problemas de LDAP. Este comando puede mostrar diagnósticos avanzados de la conexión al servidor LDAP y puede ejecutar una resolución de nombre de usuario a fin de garantizar que la configuración de LDAP esté correcta.

Configuración de un UDS mediante LDAP para un servidor NAS nuevo

Pasos

1. En la ventana **Servicios de directorio de UNIX** en el asistente **Crear un servidor NAS**, seleccione **Habilitar un directorio de UNIX con NIS o LDAP**.
2. En la ventana **Servicios de directorio de UNIX**, seleccione **LDAP**.
3. Ingrese el número de puerto.

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

4. Ingrese direcciones IP (una sola dirección, varias direcciones separadas por comas o un rango de direcciones) y seleccione **Agregar**.
5. Configure la autenticación con LDAP, tal como se describe en Autenticación con LDAP.
6. Ingrese el DN base en formato X.509.
7. En el caso de un servidor LDAP de iPlanet, ingrese el DN de perfil (opcional).
8. Si desea utilizar un LDAP seguro, seleccione la opción.
9. Seleccione **Confirmar**.

Configuración de un UDS mediante LDAP para un servidor NAS existente

Pasos

1. En PowerStore Manager, seleccione **Almacenamiento** > **Servidores NAS**.
2. Seleccione el servidor NAS y, luego la pestaña **Servicios de nomenclatura**.
3. Seleccione la pestaña **UDS**.
4. En el campo **Servicio de directorio de Unix**, seleccione **LDAP**.
5. Ingrese el número de puerto.

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

6. Ingrese direcciones IP (una sola dirección, varias direcciones separadas por comas o un rango de direcciones) y seleccione **Agregar**.
7. Configure la autenticación con LDAP, tal como se describe en Autenticación con LDAP.
8. Ingrese el DN base en formato X.509.
9. En el caso de un servidor LDAP de iPlanet, ingrese el DN de perfil (opcional).
10. Para cargar un esquema LDAP, seleccione **Cargar nuevo esquema** y, a continuación, **Seleccionar archivo**.
11. Si desea utilizar un LDAP seguro, seleccione la opción.
12. Seleccione **Confirmar**.

Autenticación con LDAP

En la siguiente tabla, se resumen las posibles opciones de autenticación de LDAP:

Tabla 6. Autenticación con LDAP

Opción	Consideraciones
LDAP con autenticación anónima o simple	En el caso de la autenticación anónima, agregue los servidores LDAP y especifique el número de puerto que utilizan estos servidores, el DN base y el DN de perfil del servidor de iPlanet/OpenLDAP. En el caso de la autenticación simple, agregue los servidores LDAP y especifique lo siguiente: ● Si usa AD, LDAP/IDMU: ○ El número de puerto que usan los servidores LDAP ○ La cuenta de usuario en formato de notación de LDAP; por ejemplo, cn=administrator,cn=users,dc=svt,dc=lab,dc=com ○ Contraseña de la cuenta de usuario ○ DN base, que es lo mismo que el nombre de dominio calificado (por ejemplo, svt.lab.com). ● Si usa el servidor de iPlanet/OpenLDAP: ○ La cuenta de usuario 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 del servidor de iPlanet/OpenLDAP
LDAP con autenticación Kerberos	Existen dos métodos para configurar Kerberos: ● Autenticarse en el dominio SMB. Con esta opción, puede autenticarse mediante la cuenta del servidor SMB o hacerlo con otras credenciales.

Tabla 6. Autenticación con LDAP (continuación)

Opción	Consideraciones
	• Configure un dominio personalizado de modo que señale 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 **Seguridad** del servidor NAS. La autenticación de AD del servidor SMB no se utiliza cuando elige esta opción. **NOTA:** Si usa NFS seguro con un dominio personalizado, debe cargar un archivo keytab.

Editar el esquema OpenLDAP de Linux

Es posible que sea necesario cambiar el esquema OpenLDAP de Linux cuando se exportan algunos sistemas de archivos NFS a grupos de red.

Cuando se descarga OpenLDAP en la organización de OpenLDAP, el servidor LDAP viene con un esquema que cumple estrictamente con RFC 2307:

```
( nisSchema.1.14 NAME 'nisNetgroupTriple'
DESC 'Netgroup triple'
SYNTAX 'nisNetgroupTripleSyntax' )
```

El esquema del servidor LDAP también puede cumplir con RFC 2307bis:

```
( 1.3.6.1.1.1.1.14 NAME 'nisNetgroupTriple'
DESC 'Netgroup triple'
EQUALITY caseIgnoreIA5Match
SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )
```

Con PowerStore, se soportan RFC 2307 y RFC 2307bis.

RFC 2307 define que la nomenclatura de tres grupos de red distingue las mayúsculas de las minúsculas, aunque el uso común es que los nombres de host en tres grupos de red no deben distinguir mayúsculas de minúsculas. Si desea hacer coincidir nombres de host con diferentes formatos (por ejemplo, los nombres de host están en mayúsculas en DNS y en minúsculas cada tres grupos de red, según lo definido en el directorio LDAP), se debe cambiar el esquema de LDAP.

Debido a que RFC 2037bis es una versión preliminar y la organización de OpenLDAP no lo reconoce, se debe cambiar el esquema OpenLDAP de Linux a fin de que sea compatible con PowerStore. Por lo tanto, es necesario cambiar el esquema OpenLDAP de PowerStore de la siguiente manera:

En el archivo `/etc/openldap/schema/nis.schema` de su servidor OpenLDAP, busque la siguiente entrada:

```
attributetype ( 1.3.6.1.1.1.1.14 NAME 'nisNetgroupTriple'
DESC 'Netgroup triple'
SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )
```

Edite la entrada para que aparezca de la siguiente manera (agregando la directiva EQUALITY):

```
attributetype ( 1.3.6.1.1.1.1.14 NAME 'nisNetgroupTriple'
DESC 'Netgroup triple'
EQUALITY caseIgnoreIA5Match
SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )
```

Cargar o ver un certificado de CA de LDAPS de un servidor NAS

Sobre esta tarea

NOTA: Este procedimiento solo es necesario si utiliza LDAPS.

Pasos

1. Seleccione **Almacenamiento** > **Servidores NAS**.
2. Seleccione el servidor NAS y, luego la pestaña **Servicios de nomenclatura**.
3. Seleccione la opción **LDAP seguro (usar SSL)** y, a continuación, **Aplicar certificado de autoridad de certificación (CA)**.

   NOTA: Estas opciones están disponibles para la autenticación anónima y simple.

4. Si ya se cargó un certificado de CA, seleccione **Recuperar certificado de CA** para verlo.
5. Seleccione **Cargar certificado de CA**, ubique el certificado que desee cargar y seleccione **Empezar carga**.

Cambiar los ajustes de las credenciales de UNIX del servidor NAS

Pasos

1. Seleccione **Almacenamiento** > **Servidores NAS**.
2. Seleccione el servidor NAS de la lista y, a continuación, seleccione la pestaña **Protocolos de uso compartido**.
3. Seleccione la pestaña **Servidor de NFS**.
4. Realice los cambios necesarios, como se describe en la siguiente tabla.

Tabla 7. Ajustes de la credencial de UNIX del servidor NAS

Tarea	Descripción
Extienda la credencial de UNIX para permitir que el sistema de almacenamiento obtenga más de 16 GID de grupo. **NOTA:** Esto solo es necesario si tiene usuarios con más de 16 GID. **NOTA:** Con NFS seguro, el servidor NAS siempre crea la credencial de UNIX, de modo que esta opción no se aplica.	Habilite o deshabilite las **Credenciales extendidas**. ● Si se habilita esta opción, el servidor NAS usará 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 deshabilita esta opción, la credencial de UNIX de la solicitud de NFS se extrae 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.
Especifique un período de retención de la caché de la credencial de UNIX. Esta opción puede mejorar el rendimiento, ya que reutiliza la credencial de UNIX de la caché en lugar de crearla por cada solicitud.	En el campo **Credential cache retention**, ingrese un período (en minutos) durante el cual las credenciales de acceso se conservan en la caché. El rango es de 1 a 35791394 y el valor predeterminado es de 15 minutos.

Configuración de mapeos de usuario para servidores NAS multiprotocolo

Un ambiente multiprotocolo requiere los siguientes tipos de mapeos de usuarios:

- Para acceder a un sistema de archivos configurado con una política de acceso de UNIX, se debe asignar un nombre de usuario de Windows a un nombre de usuario de UNIX correspondiente. Además, el sistema de almacenamiento debe ser capaz de resolver ese nombre de usuario de UNIX en un UID.
- Se debe asignar un nombre de usuario de UNIX a uno de Windows correspondiente cuando se usa NFS para acceder a un sistema de archivos configurado con una política de acceso de Windows.
- No es necesario que un usuario de UNIX se asigne a un usuario de Windows correspondiente cuando se usa NFS para acceder a un sistema de archivos configurado con una política de acceso de UNIX o nativa.

El sistema crea automáticamente una asignación entre un usuario de Windows y uno de UNIX cuando se define el mismo nombre de usuario en el servicio de directorio de UNIX (UDS) o el archivo de contraseña local, y en Active Directory (AD) de Windows. Los nombres

de usuario de UNIX distinguen mayúsculas de minúsculas. Por ejemplo, User1 de Windows se asignará automáticamente a User1 de UNIX. Si los nombres de usuario son diferentes, puede cargar un archivo de asignación de usuarios personalizado (ntxmap) para crear reglas de asignación personalizadas. Estas reglas pueden ser bidireccionales o asignar usuarios de Windows a usuarios de UNIX o viceversa. Las reglas admiten comodines y sustituciones.

Para permitir que usuarios con nombres de usuario sin asignar accedan a un sistema de archivos, puede configurar la asignación automática de usuarios (la cual habilita cuotas). Otra opción es configurar cuentas predeterminadas de UNIX y Windows para el servidor NAS.

Proceso de asignación automática de usuarios

El proceso de asignación automática de usuarios asigna el UID de UNIX al SID de Windows. Para realizar la asignación, se debe hacer coincidir el nombre de usuario del UDS o los archivos locales con el nombre de usuario del AD.

Mapeo automático de usuarios de Windows

Cuando se modifican los protocolos de uso compartido del servidor NAS, puede dirigir al sistema que genere automáticamente un UID de UNIX por cada usuario de Windows que no esté asignado a una cuenta de UNIX a través de un servicio de directorio (LDAP o NIS) o unos archivos locales.

NOTA: Utilice la asignación automática solo cuando no sea importante qué UID se asigne a cada usuario.

Esta opción está disponible cuando no haya ningún usuario de UNIX predeterminado configurado, y está destinada a la configuración multiprotocolo en que la mayoría de los usuarios son de Windows. El uso de esta opción permite la retención de cuotas del sistema de archivos por cada usuario de Windows no asignado (las cuotas del sistema de archivos se basan en el UID de UNIX). Los UID de UNIX generados automáticamente se encuentran en el rango reservado de 0x80000001 a 0x803FFFFF.

NOTA: Si hay configurado un usuario de UNIX predeterminado, no puede habilitar la asignación automática de los usuarios de Windows.

Nombres de usuario predeterminados

Al modificar los protocolos de uso compartido del servidor NAS, opcionalmente puede configurar cuentas de usuario predeterminadas para un servidor NAS:

- La cuenta de usuario predeterminada de Unix especifica la cuenta de Unix que se usa para el acceso al sistema de archivos desde una cuenta de Windows no mapeada. Si no especifica una cuenta de UNIX predeterminada, los usuarios de Windows no asignados no podrán acceder al sistema. El usuario de UNIX predeterminado puede ser un nombre de cuenta de UNIX existente y válido o seguir el formato `@uid=xxxx, gid=yyyy@`, en que xxxx e yyyy son los valores numéricos decimales del UID y del GID primario, respectivamente. Cuando configure un usuario de UNIX predeterminado, tenga en cuenta lo siguiente:
  - Si utiliza una cuenta predeterminada de UNIX para los usuarios de Windows, estos usuarios se asignan a un UID. Por lo tanto, se aplica una sola cuota de usuario a todos estos usuarios.
  - El ajuste del usuario predeterminado en un UID de cero o en un usuario que se resolverá en un UID de cero otorga acceso de raíz completo a ese usuario, lo que puede ser peligroso desde un punto de vista de la seguridad.
- Si la política de acceso al sistema de archivos es Windows, la cuenta predeterminada de Windows especifica la cuenta de Windows que se debe usar para el acceso al sistema de archivos desde una cuenta de UNIX no asignada. En el caso de la autenticación de seguridad de Windows, la credencial se crea a partir de la controladora de dominio (DC) de Windows y la base de datos del grupo local (LGDB) del servidor de SMB. Si no se especifica una cuenta de Windows predeterminada y si el usuario de Windows predeterminado no se encuentra en la DC de Windows o la LGDB, un usuario de Unix no asignado no podrá acceder a un sistema de archivos que tenga una política de acceso de Windows. La cuenta de usuario predeterminada de Windows debe ser una cuenta de usuario existente en AD al cual está unido el servidor SMB del servidor NAS. El valor distingue entre mayúsculas y minúsculas.

Personalización del archivo de asignación de usuarios

Después de crear un servidor NAS, puede usar un archivo de asignación de usuarios personalizado (ntxmap) para asignar una o más cuentas de usuario de Windows a una o más cuentas de usuario de UNIX o viceversa (ambas direcciones son válidas). La personalización del archivo de asignación de usuarios permite proporcionar acceso al sistema de archivos en los siguientes casos:

- Si una cuenta de usuario de Windows no tiene una cuenta de usuario de UNIX correspondiente.

- Si la política de acceso al sistema de archivos es de Windows y una cuenta de usuario de UNIX no posee una cuenta de usuario de Windows correspondiente.
- Si existe una cuenta de usuario de Windows y una de UNIX, pero usan reglas de nomenclatura diferentes. Las cuentas de usuario de UNIX distinguen mayúsculas de minúsculas.

El archivo de asignación de usuarios soporta el uso de comodines y secuencias de sustitución.

Para usar un archivo de asignación de usuarios personalizado, seleccione **Almacenamiento** > **Servidores NAS** > **[Servidor NAS]** > **Servicios de nomenclatura** > **Archivos locales** y descargue la plantilla del archivo de Ntxmap. Después de realizar la descarga, personalice el archivo y cárguelo en el sistema.

NOTA: La sintaxis para el archivo de mapeo se muestra en la plantilla de archivo.

Cambiar los mapeos de usuarios del servidor NAS

Sobre esta tarea

Puede cambiar los mapeos de usuarios para servidores NAS multiprotocolo.

Pasos

1. Seleccione **Almacenamiento** > **Servidores NAS**.
2. Seleccione el servidor NAS y, luego la pestaña **Servicios de nomenclatura**.
3. Realice los cambios necesarios como se describe en la siguiente tabla:

Tabla 8. Asignaciones de usuarios del servidor NAS

Tarea	Descripción
Asigne en conjunto las cuentas de UNIX y Windows que tengan nombres de usuario diferentes.	El archivo de configuración de ntxmap permite asignar cuentas de UNIX y Windows con distintos nombres de usuario. La sintaxis para ntxmap se muestra en la plantilla que se puede recuperar mediante estos pasos: a. Seleccione **Archivos locales**. b. En la lista de archivos locales, seleccione el icono de descarga junto a Ntxmap para recuperarlo. **NOTA:** Si no hay ningún archivo de asignación personalizado, el servidor NAS recupera una plantilla para la configuración. c. Use un editor de texto para agregar o cambiar mapeos de cuentas de usuario en el archivo. d. Seleccione **Cargar archivos locales** y, a continuación, seleccione **ntxmap** en las opciones de Tipo de archivo. e. Utilice el navegador para seleccionar el archivo actualizado y, luego **Cargar**.
Genere automáticamente un UID de UNIX para cada usuario de Windows que no esté asignado a una cuenta de UNIX.	a. Seleccione **Asignación de usuario**. b. Seleccione **Habilitar asignación automática de las cuentas/usuarios de Windows sin asignar**. Esta opción está destinada a los ambientes multiprotocolo en los que la mayoría de los usuarios son usuarios de Windows. Cuando seleccione esta opción, el sistema genera un UID de UNIX para los usuarios de Windows que aún no están asignados a una cuenta de UNIX a través de un servicio de directorio (LDAP o NIS) o los archivos locales. Esta funcionalidad permite la retención de cuotas del sistema de archivos para los usuarios de Windows no mapeados.
Habilitar o deshabilitar cuentas predeterminadas de usuarios no mapeados.	a. Seleccione **Asignación de usuario**. b. Marque o desmarque la opción **Habilitar cuenta predeterminada para usuarios sin asignar**.

Tabla 8. Asignaciones de usuarios del servidor NAS (continuación)

Tarea	Descripción
	c. Si habilitó esta opción, configure el usuario predeterminado de UNIX (nombre o UID/GID) y el nombre de usuario predeterminado de Windows. Si habilita esta opción, podrá ingresar cuentas predeterminadas de UNIX y Windows que usará el sistema con el fin de otorgar acceso al sistema de archivos para los usuarios no asignados. El usuario de UNIX predeterminado puede ser un nombre de cuenta de UNIX existente y válido o seguir el formato `@uid=xxxx,gid=yyyy@`, en que xxxx e yyyy son los valores numéricos decimales del UID y del GID primario, respectivamente. **NOTA:** Si utiliza cuentas predeterminadas, los usuarios se asignan a un UID y solo se aplica una cuota de usuario a todos los usuarios.

4

Configuración de un sistema de archivos para el uso compartido de archivos multiprotocolo

Este capítulo incluye la siguiente información:

Temas:

Crear un sistema de archivos

Requisitos previos

- Un servidor NAS configurado para soportar los protocolos de SMB y NFS

Pasos

1. Seleccione **Almacenamiento** > **Sistemas de archivos**.
2. Seleccione **Crear** para abrir el asistente **Crear sistema de archivos**.
3. Configure el sistema de archivos de acuerdo con los pasos del asistente:

Opción	Descripción
Seleccionar tipo	Seleccione el tipo de sistema de archivos **General**
Seleccione el servidor NAS.	Seleccione un servidor NAS habilitado para SMB y NFS. De manera opcional, puede establecer los ajustes avanzados de SMB. Para conocer detalles, consulte Ajustes avanzados del sistema de archivos para SMB.
File System Details	Proporcione el nombre del sistema de archivos, la descripción (opcional) y el tamaño. El tamaño del sistema de archivos puede ser de 3 GB a 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, Modelo PowerStore T muestra inmediatamente 1,5 GB utilizado. Cuando el sistema de archivos se monta en un host, muestra 98,5 GB de capacidad útil. En la capacidad visualizada, se refleja el espacio de metadatos que se reserva de la capacidad útil del sistema de archivos.
Retención en el nivel de archivos	Seleccione un tipo de retención en el nivel de los archivos: • Desactivado: sin retención establecida en el nivel de los archivos. • Enterprise (FLR-E): protege el contenido de cambios realizados por los usuarios a través de SMB, 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 en el nivel de archivos se configuran en la creación del sistema de archivos y no se pueden modificar. Configure los períodos de retención:

Opción	Descripción
	• 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. El valor es ilimitado. • Máximo: especifica el período más largo durante el cual se pueden bloquear los archivos. El valor es ilimitado.
Exportación de NFS (opcional)	Configure un nombre y una descripción de la exportación inicial del sistema de archivos. Puede agregar las exportaciones al sistema de archivos después de realizar la configuración inicial del sistema de archivos.
Configure el acceso	Agregue hosts.

Recurso compartido de SMB (opcional)	Configure el recurso compartido de SMB inicial:
	NOTA: Puede agregar recursos compartidos al sistema de archivos después de la configuración inicial del sistema de archivos.
	• Nombre
	• Descripción (opcional)
	• Disponibilidad offline: configura el almacenamiento en caché del lado del cliente de los archivos offline:
	  ○ Ninguno: el almacenamiento en caché del lado del cliente de archivos offline no está configurado.
	  ○ Manual: los archivos se almacenan en caché y están disponibles offline únicamente cuando el almacenamiento en caché se solicita de manera explícita.
	  ○ Programas: los archivos ejecutables almacenados en la caché localmente se ejecutan desde la copia almacenada en caché en lugar de la copia en el recurso compartido.
	  ○ Documentos: cada vez que un usuario accede a un archivo o un programa desde un recurso compartido, el contenido se almacena en caché automáticamente con el fin de estar disponible en el modo offline. El contenido en la caché continuará sincronizándose con la versión del servidor.
	De manera opcional, configure los ajustes avanzados de SMB de los recursos compartidos de SMB. Para conocer detalles, consulte Propiedades avanzadas de recursos compartidos de SMB.
	• **Disponibilidad continua**
	• **Cifrado de protocolo**
	• **Enumeración basada en el acceso**
	• **Bifurcación de caché habilitada**

Política de protección (opcional)	Proporcione una política de protección correspondiente al sistema de archivos. PowerStore soporta instantáneas y replicación para la protección del almacenamiento de archivos.
Política de QoS de archivos (opcional)	Proporcione una política de QoS correspondiente 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.
Resumen	Revise el resumen. Si es necesario, regrese para realizar cambios.

4. Haga clic en **Create File System**.
El sistema de archivos se visualiza en la lista Sistema de archivos. Si creó una exportación de NFS o un recurso compartido de SMB, se mostrarán en las listas respectivas.

Ajustes avanzados del sistema de archivos para SMB

Puede agregar ajustes avanzados a los sistemas de archivos habilitados para SMB durante la creación de un sistema de archivos.

Tabla 9. Ajustes avanzados del sistema de archivos para SMB

Configuración	Descripción
Escrituras síncronas habilitadas	Cuando se habilita la opción de escrituras síncronas para un sistema de archivos Windows (SMB) o multiprotocolo, el sistema de almacenamiento realiza escrituras síncronas inmediatas para las operaciones de almacenamiento, independientemente de la forma en que el protocolo SMB realiza

Tabla 9. Ajustes avanzados del sistema de archivos para SMB (continuación)

Configuración	Descripción
	las operaciones de escritura. La habilitación de las operaciones de escrituras síncronas permite almacenar y acceder a archivos de base de datos (por ejemplo, MySQL) en recursos compartidos de SMB del sistema de almacenamiento. Esta opción garantiza que todas las escrituras del recurso compartido se realicen sincrónicamente y reduce la posibilidad de que produzcan pérdidas de datos o se dañen archivos en caso de que ocurra algún tipo de error, como una pérdida de la alimentación eléctrica. La opción de escrituras síncronas viene deshabilitada de forma predeterminada. **NOTA:** La opción de escrituras síncronas puede tener un gran impacto en el rendimiento. No se recomienda a menos que desee utilizar los sistemas de archivos Windows para proporcionar almacenamiento para aplicaciones de bases de datos.
Bloqueos oportunos habilitados	Se admiten las siguientes implementaciones de oplocks: ● Bloqueos oportunos de segundo nivel, los cuales informan a un cliente que varios clientes están accediendo a un archivo, pero que ninguno lo ha modificado aún. Un bloqueo oportuno de nivel II permite que el cliente realice operaciones de lectura y capturas de atributos de archivos mediante la información local almacenada en caché o la de lectura anticipada. Todas las solicitudes de acceso a archivos deben enviarse al servidor. ● Bloqueos oportunos exclusivos, los cuales informan a un cliente que es el único que está abriendo el archivo. Un bloqueo oportuno exclusivo permite a un cliente realizar todas las operaciones de archivos utilizando la información en caché o de lectura anticipada hasta que se cierra el archivo, momento en el cual el servidor se debe actualizar con los cambios realizados en el estado del archivo (contenidos y atributos). ● Bloqueos oportunos por lotes, los cuales informan a un cliente que es el único que está abriendo el archivo. Un bloqueo oportuno por lote les permite a los clientes ejecutar todas las operaciones de archivos al utilizar la información en caché o la información local con lectura anticipada (incluida las aperturas y los cierres). El servidor puede mantener un archivo abierto para un cliente incluso si el proceso local en el equipo del cliente cerró el archivo. El mecanismo reduce el tráfico de red al permitirles a los clientes omitir solicitudes extrañas para abrir y cerrar archivos.
Notificación en caso de escritura habilitada	Habilite la notificación cuando se escriba en un sistema de archivos. Esta opción está desactivada de manera predeterminada.
Habilite la notificación sobre un acceso habilitado	active la notificación cuando se acceda a un sistema de archivos. Esta opción está desactivada de manera predeterminada.

5

Configurar recursos compartidos

Este capítulo incluye la siguiente información:

Temas:

Rutas de exportación generales y locales del recurso compartido

En la siguiente tabla, se describen los ajustes de rutas de los recursos compartidos y las exportaciones:

Tabla 10. Ajustes de rutas para recursos compartidos y exportaciones

Configuración	Descripción
Ruta local	Una ruta local constituye aquella ruta al recurso de almacenamiento de sistemas de archivos en el sistema de almacenamiento. Esta ruta especifica la ubicación única del recurso compartido o la exportación en el sistema de almacenamiento. ● Recursos compartidos SMB ○ En un sistema de archivos de SMB, puede crear múltiples recursos compartidos con la misma ruta local. En estos casos, puede especificar distintos controles de acceso del lado del host para diferentes usuarios, pero los recursos compartidos dentro del sistema de archivos obtendrán acceso al contenido común. ○ Un directorio debe existir antes de crear recursos compartidos en él. Si desea que los recursos compartidos de SMB dentro del mismo sistema de archivos accedan a contenido diferente, debe crear en primer lugar un directorio en el host de Windows que esté mapeado al sistema de archivos. A continuación, puede crear los recursos compartidos correspondientes mediante PowerStore. También puede crear y administrar recursos compartidos de SMB desde la consola de administración de Microsoft. ● Exportaciones NFS ○ Cada exportación de NFS debe tener una ruta local única. PowerStore asigna automáticamente esta ruta al recurso de exportación inicial creado dentro de un nuevo sistema de archivos. El nombre de ruta local se basa en el nombre del sistema de archivos. ○ Antes de crear recursos compartidos adicionales dentro de un sistema de archivos NFS, debe crear un directorio para compartir desde un host Linux/UNIX que esté conectado al sistema de archivos. A continuación, puede crear una exportación en PowerStore y configurar permisos de acceso según corresponda.
Ruta de exportación	La ruta que utiliza el host para conectarse al recurso compartido o la exportación. PowerStore crea la ruta de exportación según el

Tabla 10. Ajustes de rutas para recursos compartidos y exportaciones (continuación)

Configuración	Descripción
	nombre del recurso compartido o la exportación y el nombre del sistema de archivos en que reside. Los hosts utilizan el nombre o la ruta de exportación para el montaje o la asignación a la exportación o el recurso compartido en el host de red. Este comportamiento se activa mediante el uso de alias de NFS para los recursos compartidos.

Crear un recurso compartido SMB

Puede crear un recurso compartido de SMB en un sistema de archivos que se haya creado con un servidor NAS habilitado para SMB.

Pasos

1. Seleccione **Almacenamiento** > **Sistema de archivos** > **Recursos compartidos SMB**.
2. Haga clic en **Crear** y complete los pasos del asistente **Crear recurso compartido SMB**.

Página	Descripción
Seleccionar sistema de archivos	Seleccione un sistema de archivos que se haya habilitado para SMB.
Seleccionar instantánea (opcional)	Seleccione una de las instantáneas del sistema de archivos en la que creará el recurso compartido.
SMB Share Details	Ingrese un nombre, una descripción y una ruta local para el recurso compartido. Cuando ingrese la ruta local: ● Puede crear varios recursos compartidos con la misma ruta local en un único sistema de archivos SMB. En estos casos, puede especificar distintos controles de acceso del lado del host para diferentes usuarios, pero los recursos compartidos dentro del sistema de archivos tienen acceso al contenido común. ● Un directorio debe existir antes de crear recursos compartidos en él. Si desea que los recursos compartidos de SMB dentro del mismo sistema de archivos accedan a contenido diferente, debe crear en primer lugar un directorio en el host de Windows que esté mapeado al sistema de archivos. A continuación, puede crear los recursos compartidos correspondientes mediante PowerStore. También puede crear y administrar recursos compartidos de SMB desde la consola de administración de Microsoft. En PowerStore también se muestra la ruta del recurso compartido de SMB, la que utiliza el host para conectarse al recurso compartido. La ruta del recurso compartido es la dirección IP o el nombre del servidor NAS y el nombre del recurso compartido. Los hosts utilizan la ruta del recurso compartido para el montaje o el mapeo del recurso compartido desde un host de red.
Ajustes avanzados de recursos compartidos de SMB	Habilite uno o más de los ajustes avanzados de recursos compartidos de SMB: ● Disponibilidad continua ● Cifrado de protocolo ● Enumeración basada en acceso ● Caché de sucursal habilitada ● Disponibilidad offline (valor predeterminado: ninguna) ● Umask (valor predeterminado: 022)

Siguientes pasos

Cuando crea un recurso compartido, puede modificarlo desde PowerStore o mediante Microsoft Management Console.

Para modificar el recurso compartido desde PowerStore, selecciónelo en la lista de la página **SMB Share** y haga clic en **Modify**.

Propiedades avanzadas de recursos compartidos de SMB

Puede configurar las siguientes propiedades avanzadas de recursos compartidos de SMB cuando crea un recurso compartido SMB o cambia sus propiedades:

Tabla 11. Propiedades avanzadas de SMB

Opción	Descripción
Disponibilidad continua	Otorga a las aplicaciones de host un acceso transparente y continuo a un recurso compartido después de una conmutación por error del servidor NAS en el sistema (con el estado interno del servidor NAS guardado o restaurado durante el proceso de conmutación por error). **NOTA:** Active la disponibilidad continua para un recurso compartido solo cuando desee usar clientes del protocolo Microsoft Server Message Block (SMB) 3.0 con el recurso compartido específico.
Cifrado de protocolo	Habilita el cifrado SMB del tráfico de red a través del recurso compartido. Los clientes SMB 3.0 y superiores son compatibles con el cifrado SMB. De forma predeterminada, el acceso se deniega si un cliente SMB 2 intenta obtener acceso a un recurso compartido con el cifrado de protocolo habilitado. Puede controlar esto mediante la configuración de la clave de registro RejectUnencryptedAccess en el servidor NAS. 1 (valor predeterminado) rechaza el acceso no cifrado y 0 permite a clientes que no son compatibles con el cifrado acceder al sistema de archivos sin cifrado.
Enumeración basada en acceso	Filtra la lista de directorios y archivos disponibles en el recurso compartido para incluir solo los que brinden acceso de lectura al usuario que lo solicita. **NOTA:** Los administradores siempre pueden firmar todos los archivos.
Caché en sucursal habilitada	Copia contenido del recurso compartido y lo copia en la memoria caché en las sucursales. Esto permite a los equipos cliente de las sucursales tener acceso al contenido de forma local, en lugar de mediante la WAN. BranchCache se administra desde los hosts de Microsoft.
Sistema de archivos distribuido (DFS)	(De solo lectura) Le permite agrupar archivos que están en distintos recursos compartidos conectándolos de manera transparente a uno o más espacios de nombres de DFS. Esto simplifica el proceso de trasladar datos de un recurso compartido al otro. Esta opción es de solo lectura en Unisphere debido a que usted administra DFS desde hosts de Microsoft. Para obtener información, consulte la documentación de Distributed File System de Microsoft.
Disponibilidad offline	Configura el almacenamiento en caché de los archivos offline del lado del cliente: ● **Manual**: los archivos se almacenan en caché y están disponibles offline únicamente cuando el almacenamiento en caché se solicita de manera explícita. ● **Programas y archivos abiertos por usuarios**: todos los archivos que abren los clientes desde el recurso compartido se almacenan en caché y están disponibles offline automáticamente. Los clientes abren estos archivos desde el recurso compartido cuando están conectados a él. Esta opción se recomienda para archivos con trabajo compartido. ● **Programas y archivos abiertos por usuarios, optimizar para rendimiento**: todos los archivos que abren los clientes desde el recurso compartido se almacenan en caché y están disponibles offline automáticamente. Los clientes abren estos archivos desde la memoria caché local del recurso compartido, si es posible, incluso cuando están conectados a la red. Esta opción se recomienda para la mayoría de los programas ejecutables. ● **Ninguno**: el almacenamiento en caché del lado del cliente de archivos offline no está configurado.
UMASK	(Se aplica a los recursos compartidos de SMB de un sistema de archivos que admite el acceso multiprotocolo con una política de acceso de UNIX o una política de acceso nativo). Máscara de bits que muestra los permisos de UNIX que se excluyen para los archivos creados en el recurso compartido. Los permisos predeterminados son: ● 666 para los archivos, lo que otorga permisos de lectura y escritura para todos. ● 777 para los directorios, lo que otorga permisos de lectura, escritura y ejecución para todos. Si UMASK se configura en 022, se otorgan los siguientes permisos: ● 644 para los archivos, lo que otorga permisos de lectura y escritura al propietario del archivo y el permiso de lectura para todos los demás. ● 755 para directorios, lo que otorga permisos de lectura, escritura y ejecución a los propietarios del directorio, y de lectura y ejecución para todos los demás.

Tabla 11. Propiedades avanzadas de SMB (continuación)

Opción	Descripción
	NOTA: Si la herencia de ACL de NFSv4 está presente, tiene prioridad sobre la configuración de UMASK. • Para cambiar los permisos excluidos, haga clic en **Modificar** y seleccione o deseleccione los permisos. • Para establecer la máscara de bits en el valor predeterminado (022), haga clic en **Set default**. Un valor de 022 solo le permite escribir los datos, pero permite que cualquier persona los lea. Para obtener más información, consulte la documentación de UNIX.

Crear una exportación de NFS

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

Pasos

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**.

6

Habilitar el uso compartido de archivos multiprotocolo en un servidor NAS existente

Este capítulo incluye la siguiente información:

Temas:

Habilitar el uso compartido de archivos multiprotocolo en un servidor NAS habilitado para NFS existente

Sobre esta tarea

Cuando configura el multiprotocolo, todos los sistemas de archivos existentes se habilitan con la política de acceso de seguridad nativa.

Pasos

1. Seleccione **Almacenamiento** > **Servidores NAS**.
2. Seleccione el servidor NAS pertinente y, a continuación, seleccione la pestaña **Servicios de nomenclatura**.
3. Configure uno de los siguientes servicios de directorio en caso de que no se haya configurado el servicio de directorio de UNIX (UDS) del servidor NAS o si los archivos locales no están configurados:
   - NIS
   - LDAP
   - Archivos locales
   - Los archivos locales y NIS o LDAP

   Puede configurar LDAP de modo que use autenticación anónima, simple y Kerberos. También puede configurar LDAP con SSL (LDAP seguro) e imponer el uso del certificado de una autoridad de certificación para la autenticación.
4. Seleccione la pestaña **Asignación de usuarios** y configure el orden de búsqueda. Los servicios de directorio que haya configurado se pueden seleccionar en el menú desplegable.
5. Seleccione la pestaña **Asignación de usuarios** y habilite la asignación automática o la cuenta predeterminada para los usuarios no asignados. Si seleccionó habilitar la cuenta predeterminada, especifique las cuentas predeterminadas de Windows y UNIX. También puede usar **`ntxmap`** (que se encuentra en la pestaña **Archivos locales**) para asignar usuarios de Windows y UNIX.
6. Seleccione la página **Protocolos de uso compartido** y, a continuación, **Servidor de SMB**.
7. En la pestaña **Servidor de SMB**, realice lo siguiente:
   - Habilite el servidor de SMB.
   - Una el servidor NAS al dominio de Active Directory (AD).
   - De manera opcional, seleccione **Opciones avanzadas** para especificar el nombre del NetBIOS y la unidad organizacional. El nombre de NetBIOS cambia a un valor predeterminado para los primeros 15 caracteres del nombre del servidor SMB. La unidad organizacional se configura de manera predeterminada en CN=Computers.

Habilitar el uso compartido de archivos multiprotocolo en un servidor NAS habilitado para SMB existente

Sobre esta tarea

Las siguientes consideraciones se aplican a la habilitación del uso compartido de archivos multiprotocolo en un servidor NAS habilitado para SMB existente:

- Cuando configura el multiprotocolo, todos los sistemas de archivos existentes se habilitan con la política de acceso de seguridad nativa. Con esta política, la seguridad de Windows se usa para el acceso de NFS y SMB a los archivos. Esta política usa la credencial de Windows nativa en todos los protocolos y solo aplica la ACL de SMB a todos ellos. Además, el sistema actualiza automáticamente la propiedad de todos los archivos con información de UID de UNIX. El proceso de actualización puede tardar, pero los datos siguen siendo accesibles. Si es necesario, puede cambiar esta política de acceso.
- Los clientes con asignaciones incorrectas recibirán un mensaje de acceso denegado hasta que la configuración de la asignación sea la correcta.

Pasos

1. Seleccione **Almacenamiento** > **Servidores NAS**.
2. Seleccione el servidor NAS pertinente y, a continuación, seleccione la pestaña **Servicios de nomenclatura**.
3. Configure uno de los siguientes servicios de directorio:
   - NIS
   - LDAP
   - Archivos locales
   - Los archivos locales y NIS o LDAP

   Puede configurar LDAP de modo que use autenticación anónima, simple y Kerberos. También puede configurar LDAP con SSL (LDAP seguro) e imponer el uso del certificado de una autoridad de certificación para la autenticación.
4. Seleccione la pestaña **Asignación de usuarios** y configure el orden de búsqueda. Los servicios de directorio que haya configurado se pueden seleccionar en el menú desplegable.
5. En la pestaña **Asignación de usuarios**, configure el modo de asignación para los usuarios no asignados. Si desea asignaciones automáticas de UID, habilite la opción **Habilitar asignación automática de cuentas/usuarios de Windows no asignados**. Otra opción es habilitar la opción **Habilitar cuenta predeterminada para usuarios no asignados**, en cuyo caso especifique las cuentas predeterminadas de Windows y Unix.

7

Configurar los enlaces amplios y el sistema de archivos distribuido

Este capítulo incluye la siguiente información:

Temas:

Acerca del sistema de archivos distribuidos

El sistema de archivos distribuidos (DFS) de Microsoft permite agrupar sistemas de archivos (carpetas compartidas) que residen en diferentes servidores en un espacio de nombres del DFS lógico. Un espacio de nombres del DFS constituye una vista virtual de estos sistemas de archivos que se muestran en una estructura de árbol de directorios. Mediante DFS, puede agrupar sistemas de archivos en un espacio de nombres de DFS lógico y hacer que las carpetas que se distribuyan entre varios servidores aparezcan a los usuarios como si residieran en una ubicación de la red. Los usuarios pueden navegar por el espacio de nombres sin necesidad de conocer los nombres de los servidores ni los sistemas de archivos en que se alojan los datos.

Cada estructura de árbol del DFS tiene un destino raíz, que corresponde al servidor host que tiene en ejecución el servicio de DFS y hospeda el espacio de nombres. Una raíz de DFS contiene enlaces de DFS que conducen a los sistemas de archivos (un recurso compartido y cualquier directorio debajo de este en la red). Los sistemas de archivos se ven como objetivos del DFS. Microsoft ofrece servidores raíz del DFS independientes y basados en dominio. El servidor del DFS basado en dominios almacena la jerarquía del DFS en AD. El servidor raíz del DFS independiente almacena la jerarquía del DFS de manera local. PowerStore proporciona la misma funcionalidad que un servidor raíz del DFS independiente con Windows 2000 o Windows Server 2003.

Configuración de raíces de DFS

Puede configurar las raíces de soporte de sistemas de archivos distribuidos (DFS) en un recurso compartido de SMB en PowerStore. Complete las siguientes tareas antes de configurar una raíz de DFS en un recurso compartido de SMB:

1. Configure un servidor NAS que soporte SMB.
2. En el servidor NAS recién creado, configure un sistema de archivos en el que se deba crear la raíz de DFS.

NOTA: No establezca una raíz de DFS en un objeto del sistema de archivos con una política de comprobación de acceso de UNIX, ya que ninguno de los componentes de enlace de DFS se creará con derechos de UNIX.

Existen dos maneras de crear una raíz de DFS en un recurso compartido de SMB:

- Cree una raíz de DFS mediante dfsutil.exe.
- Cree una raíz de DFS independiente mediante la MMC de DFS.

Para obtener más información sobre la configuración de DFS, consulte la documentación de Microsoft.

Acerca de los enlaces anchos

Los enlaces anchos hacen que los enlaces simbólicos tradicionales de UNIX en los sistemas de archivos de usuario sean útiles para los clientes de SMB. Cuando un cliente de NFS encuentra un enlace simbólico en un sistema de archivos, resuelve el destino del propio enlace. El desafío es que, si bien la ruta de destino del enlace simbólico es significativa para los clientes de NFS, lo más probable es que no sea de utilidad para los clientes de SMB. Este desafío se aborda mediante la configuración de una raíz DFS local de Microsoft Windows en el servidor NAS que aloja los sistemas de archivos de usuario, que incluyen enlaces simbólicos de UNIX que se deben traducir para los clientes de SMB. Las entradas se agregan a la raíz de DFS para que el servidor NAS pueda traducir las rutas de UNIX.

Por ejemplo, suponga que widelink1 se ve de la siguiente manera para un cliente de NFS:

```
$ ls -l widelink1
lrwxr-xr-x 1 cstacey ENG\Domain Users 30 23 JUS 17:33
widelink1 -> /net/nfsserver42/export1/target1
```

$ ls -l widelink1

A continuación, la entrada en la raíz de DFS debe ser:

```
net/nfsserver42/export1/target1 ->
\\nfsserver42\<share-name>\<path-to-target1>
```

8

Solución de problemas de una configuración multiprotocolo

Este capítulo incluye la siguiente información:

Temas:

Comandos de servicio para solucionar problemas de una configuración multiprotocolo

Los siguientes comandos de servicio son útiles para solucionar problemas de acceso en una configuración multiprotocolo. Para obtener información detallada sobre los comandos de servicio, consulte las *Notas técnicas de los comandos de servicio*.

Tabla 12. Comandos de servicio para solucionar problemas de una configuración multiprotocolo

Caso de uso	Comando de servicio
Obtenga información sobre la conectividad de red con las controladoras de dominio, los derechos de acceso, las credenciales, los registros de acceso, etc.	`svc_nas_cifssupport --server <NAS_Server_Name>`
Audite la conexión actual entre el cliente de SMB y la controladora de dominio.	`svc_nas_cifssupport --server <NAS_Server_Name> --args="-builtinclient"`
Realice una prueba interna para ayudarse a detectar la causa raíz de posibles errores de configuración o de entorno.	`svc_nas_cifssupport --server <NAS_Server_Name> --args="-checkup"`
Solucione problemas de control de acceso de usuarios; para ello, indique las credenciales de usuario como se ven en la caché del servidor de SMB.	`svc_nas_cifssupport --server <NAS_Server_Name> --args="-cred"`
Obtenga información sobre los objetos de política global que se aplican al servidor de SMB.	`svc_nas_cifssupport --server <NAS_Server_Name> --args="-gpo"`
Habilite un registro de intentos de inicio de sesión del usuario o de la máquina.	`svc_nas_cifssupport --server <NAS_Server_Name> --args="-logontrace"`
Consulte la autenticación de un usuario determinado en un servidor de SMB.	`svc_nas_cifssupport --server <NAS_Server_Name> --args="-lsarpc"`
Ponga a prueba el inicio de sesión de red en un servidor de SMB.	`svc_nas_cifssupport --server <NAS_Server_Name> --args="-nltest"`
Muestre información de la controladora de dominio correspondiente a un servidor de SMB determinado.	`svc_nas_cifssupport --server <NAS_Server_Name> --args="-pdcdump"`
Intente conectarse a la controladora de dominio de SMB desde un servidor de SMB determinado.	`svc_nas_cifssupport --server <NAS_Server_Name> --args="-pingdc"`
Obtenga la membresía de grupo de un usuario determinado en la controladora de dominio de SMB.	`svc_nas_cifssupport --server <NAS_Server_Name> --args="-samr"`
Acceda a la base de datos de asignación segura que actúa como un mecanismo de caché para relacionar los SID de Windows con los UID de UNIX.	`svc_nas_cifssupport --server <NAS_Server_Name> --args="-secmap"`