Dell PowerStore

Configuración de SMB

4.3

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

Diciembre de 2025
Rev. A08

DELL Technologies

Notas, avisos y advertencias

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

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

AVISO: WARNING indica la posibilidad de daños en la propiedad, lesiones personales o la muerte.

Tabla de contenido

Prefacio

Como parte de un esfuerzo por mejorar, se lanzan periódicamente revisiones de software y hardware. Algunas funciones que se describen en este documento no son compatibles con todas las versiones del software o el hardware actualmente en uso. Las notas de la versión del producto proporcionan la información más actualizada acerca de las características del producto. Póngase en contacto con el proveedor de servicio si un producto no funciona correctamente o como se describe en este documento.

Dónde obtener ayuda

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

- **Información del producto**: para obtener documentación o notas de la versión sobre productos y características, visite el Centro de información de PowerStore.
- **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.

Comentarios del cliente

Hay un botón de comentarios en el lado derecho de PowerStore Manager. Si selecciona **Comentarios** , se abre una ventana del navegador en la que puede completar y enviar una encuesta de comentarios.

1

Descripción general

Este capítulo incluye la siguiente información:

Temas:

Compatibilidad con SMB

Modelo PowerStore T y Modelo PowerStore Q soportan de SMB 1 a SMB 3.1.1. Cuando la compatibilidad con SMB está habilitada en el servidor NAS, puede crear sistemas de archivos habilitados para SMB. El servidor NAS con compatibilidad con SMB puede ser independiente o estar unido a un dominio de Active Directory. Los servidores NAS unidos a un dominio se colocan de manera predeterminada en la unidad organizacional OU=Computers, OU=EMC NAS Servers.

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.

Los sistemas de archivos y los recursos compartidos de SMB tienen las siguientes opciones avanzadas para los protocolos:

NOTA: Estas opciones, con excepción de Oplocks Enabled, están deshabilitadas de manera predeterminada.

Tabla 1. Opciones avanzadas del protocolo SMB

Opción de protocolo	Nivel
Escrituras síncronas habilitadas	Sistema de archivos
Bloqueos oportunos habilitados	Sistema de archivos
Notificación en caso de escritura habilitada	Sistema de archivos
Notificación en caso de acceso habilitada	Sistema de archivos
Disponibilidad continua	Recurso compartido
Cifrado de protocolo	Recurso compartido
Enumeración basada en acceso	Recurso compartido
Caché en sucursal habilitada	Recurso compartido
Disponibilidad offline	Recurso compartido

Consideraciones de planificación

Revise la siguiente información antes de configurar servidores NAS y sistemas de archivos:

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

Redes de servidores NAS

Configure lo siguiente antes de configurar servidores NAS con el protocolo SMB:

1. Configure uno o más servidores DNS.

2. Si está uniendo el servidor NAS a Active Directory (AD), configure al menos un servidor NTP en el sistema de almacenamiento para sincronizar la fecha y la hora. Se recomienda configurar un mínimo de dos servidores NTP por dominio para evitar un punto único de falla.

   NOTA: NTP se configura durante la creación de AD.

3. Cree una cuenta de dominio en Active Directory.

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

Escalabilidad

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

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

Requisitos de implementación

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

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

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

Más consideraciones

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

Crear la interfaz de red para el tráfico NAS

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

Crear vinculaciones LACP para el tráfico NAS

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

Sobre esta tarea

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

Pasos

1. Seleccione **Hardware** > **[dispositivo]** > **Puertos**.

2. En la lista de puertos, seleccione de dos a cuatro puertos de la misma velocidad en el nodo en el que desea agregarlos para la vinculación del protocolo de control de agregación de enlaces (LACP) con el fin de gestionar el tráfico NAS.

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

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

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

Crear una red a prueba de errores

Sobre esta tarea

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

Pasos

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

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

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

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

   - BaseEnclosure es constante.
   - Node es el nodo que se muestra en la lista **Nodo-Módulo-Nombre**.
   - nextLACPbondcreated es un valor numérico determinado por el orden en que se creó la vinculación en PowerStore Manager, comenzando con cero para la primera vinculación creada.

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

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

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

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

Creación de recursos compartidos de SMB

Realice lo siguiente antes de poder crear recursos compartidos de SMB en PowerStore:

1. Crear servidores NAS con el protocolo SMB
2. Crear un sistema de archivos para recursos compartidos de SMB

Recursos de documentación

Consulte lo siguiente para obtener información adicional:

Tabla 2. Recursos de documentación

Documento	Descripción	Ubicación
Guía de redes T y Q de PowerStore para servicios de almacenamiento	Proporciona información sobre la planificación y la configuración de la red.	dell.com/powerstoredocs
Guía de configuración de NFS de PowerStore	Proporciona información necesaria para configurar exportaciones de NFS con PowerStore Manager.	
Documentación técnica Funcionalidades de archivos de PowerStore	Se analizan las características, la funcionalidad y los protocolos compatibles con la arquitectura de archivos de Dell PowerStore.	
Ayuda en línea de PowerStore	Proporciona información confidencial contextual para la página que se abre en PowerStore Manager.	Integrada en PowerStore Manager

2

Creación de servidores NAS

Este capítulo incluye la siguiente información:

Temas:

Descripción general de la configuración de servidores NAS

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

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

Crear un servidor NAS para los sistemas de archivos SMB

Crea un servidor NAS antes de crear sistemas de archivos.

Requisitos previos

Obtenga la siguiente información:

- Puerto de red, dirección IP, máscara de subred/longitud del prefijo e información de gateway para el servidor NAS.

  NOTA: La dirección IP y la máscara de subred/longitud del prefijo son obligatorias.

- Identificador de VLAN, si el puerto del switch soporta el etiquetado de VLAN.

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

- Si está configurando un servidor NAS independiente, obtenga el grupo de trabajo y el nombre de NetBIOS. A continuación, defina lo que se usará para el administrador local independiente de la cuenta del servidor SMB.
- Si va a unir el servidor NAS a Active Directory (AD), asegúrese de que NTP esté configurado en su sistema de almacenamiento. A continuación, obtenga el nombre de sistema SMB (que se usa para acceder a recursos compartidos SMB), el nombre de dominio de Windows y el nombre de usuario y la contraseña de un administrador o usuario de dominio que tenga un nivel de acceso al dominio suficiente para unirse a AD.

Pasos

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

Pantalla del asistente	Descripción
Detalles	• Nombre del servidor NAS • Descripción del servidor NAS • Interfaz de red: seleccione un grupo de agregación de enlaces o una red a prueba de errores (consulte Crear la interfaz de red para el tráfico NAS). **NOTA:** Si selecciona una red a prueba de errores (FSN), la red primaria no se puede modificar una vez que se configura un servidor NAS con el uso de la FSN. • Información de red: dirección IP, máscara de subred, gateway e ID de VLAN **NOTA:** No puede reutilizar las VLAN que se utilizan para las redes de administración y almacenamiento. • Habilitar reflejo de paquetes: las respuestas del servidor se envían de vuelta al host o enrutador de origen, independientemente de la dirección IP de destino, lo que evita las búsquedas de enrutamiento. **NOTA:** Esta opción no se aplica para la comunicación iniciada por el servidor NAS.
Protocolo de uso compartido	**Select Sharing Protocol** Seleccione **SMB**. **NOTA:** Si selecciona los protocolos SMB y NFS, automáticamente permite que el servidor NAS admita multiprotocolo. La configuración de multiprotocolo no se describe en este documento. **Windows Server Settings** Seleccione **Independiente** para crear un servidor SMB independiente o **Unirse al dominio de Active Directory** para crear un servidor SMB miembro del dominio. Si une el servidor NAS al AD, seleccione opcionalmente **Avanzado** para cambiar el nombre de NetBios predeterminado y la unidad organizacional. **DNS** Si seleccionó **Join to the Active Directory Domain**, es obligatorio agregar un servidor DNS. De manera opcional, habilite DNS si desea usar un servidor DNS para el servidor SMB independiente. **Asignación de usuarios** Se muestra la página **User Mapping** si ha seleccionado unirse al dominio de Active Directory. Mantenga el valor predeterminado **Enable automatic mapping for unmapped Windows accounts/users** para soportar la unión al dominio de Active Directory. Se requiere una asignación automática cuando se una al dominio de Active Directory.
Política de protección	De manera opcional, seleccione una política de protección en la lista.
Política de QoS de archivos	De manera opcional, seleccione una política QoS de archivos en la lista.
Resumen	Revise el contenido y seleccione **Previous** para regresar y realizar las correcciones que sean necesarias.

4. Seleccione **Create NAS Server**.
   Se abre la ventana **Estado** y se lo redirige a la página **Servidores NAS** cuando se crea el servidor.

Siguientes pasos

Una vez que haya creado el servidor NAS para SMB, puede continuar con la configuración de los ajustes del servidor o crear sistemas de archivos.

Seleccione el servidor NAS para continuar con la configuración o modificar sus ajustes.

Cambio de la configuración del servidor NAS

Una vez que haya creado un servidor NAS, puede realizar cambios en la configuración del servidor.

Sobre esta tarea

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

Pasos

1. Seleccione **Storage** > **NAS Servers** > **[nas server]**.
2. En la página **Network**, configure opcionalmente las interfaces de red o las rutas a redes externas, como se describe en Configurar redes de servidor NAS.
3. En la página **Naming Services**, de manera opcional, agregue, modifique o elimine servidores DNS del servidor NAS.

   NOTA: No puede deshabilitar DNS para los servidores NAS compatibles con el uso compartido de archivos de SMB y que están unidos a Active Directory (AD).

4. En la página **Protocolos de uso compartido**:
   - Seleccione la tarjeta **Servidor SMB** para habilitar o deshabilitar el soporte de recursos compartidos de Windows o cambiar el tipo de búsqueda que usará el servidor de SMB.

     NOTA: Si cambia la opción **Tipo de Windows Server** de **Independiente** a **Unirse al dominio de Active Directory**, debe ir a la pestaña **Mapeo de usuarios** y seleccionar **Habilitar mapeo automático de cuentas/usuarios de Windows sin mapear**.

   - Seleccione la tarjeta **FTP** para habilitar o deshabilitar FTP o SFTP, cambiar las propiedades de FTP o SFTP, y configurar la autenticación de usuario, un directorio principal de usuario y los ajustes de los mensajes de autenticación. Para obtener información detallada, consulte Configurar el protocolo de uso compartido FTP.
   - Seleccione **Asignación de usuarios** para permitir que el servidor use la asignación automática en cuentas/usuarios de Windows no asignados o la cuenta predeterminada de los usuarios de cuentas de Windows no asignados.
5. En la página **Protección y eventos**, habilite o deshabilite NDMP.

   Para obtener información detallada, consulte Habilitar la protección y los eventos de NDMP.
6. En la pestaña **Seguridad y eventos**:
   - Seleccione **Kerberos** con el fin de agregar el dominio de Active Directory (AD) para la autenticación Kerberos o para configurar un dominio personalizado de Kerberos.
   - Seleccione **Antivirus** para habilitar o deshabilitar el servicio de antivirus y recuperar o cargar el archivo de configuración del antivirus.

   Para conocer detalles, consulte Configurar la seguridad del servidor NAS.

Eliminar un servidor NAS

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

Requisitos previos

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

Sobre esta tarea

Pasos

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

3. Seleccione **More Actions** > **Delete**.

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

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

Resultados

Se elimina el servidor NAS seleccionado.

3

Características adicionales del servidor NAS

Este capítulo incluye la siguiente información:

Temas:

Configurar un protocolo de uso compartido FTP o SFTP

Puede configurar FTP o FTP sobre SSH (SFTP) una vez que se haya creado el servidor NAS.

Requisitos previos

FTP en modo pasivo no es compatible.

Sobre esta tarea

El acceso a FTP se puede autenticar con los mismos métodos que SMB. Una vez que se completa la autenticación, el acceso es igual que el de SMB con fines de seguridad y permisos. Si el formato es `domain@user` o `domain\user`, se utiliza la autenticación de SMB. La autenticación de SMB utiliza la controladora de dominio de Windows.

Pasos

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

Configurar redes de servidores NAS

Puede modificar o configurar redes de servidores NAS.

Configure lo siguiente para las redes de servidores NAS:

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

Configurar interfaces de archivos para un servidor NAS

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

Sobre esta tarea

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

Pasos

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

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

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

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

Configurar rutas para la interfaz de archivos para conexiones externas

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

Requisitos previos

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

Sobre esta tarea

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

Siga los pasos a continuación:

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

Pasos

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

Habilitar el respaldo NDMP

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

Sobre esta tarea

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

PowerStore admite:

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

Pasos

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

Siguientes pasos

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

Restauración redirigida de NDMP

PowerStore permite que los usuarios/grupos locales accedan a recursos compartidos SMB en un servidor NAS diferente mediante la ejecución de un comando para modificar las listas de control de acceso (ACL).

La restauración de un respaldo de tipo NDMP en un servidor NAS diferente al original puede causar problemas de acceso. Es posible que los usuarios y grupos locales en el servidor NAS de destino no puedan acceder a los recursos compartidos SMB debido a que las listas de control de acceso (ACL) de los objetos del sistema de archivos contienen identificadores de seguridad (SID) del servidor original.

Para permitir que los usuarios o grupos locales del servidor NAS de destino accedan a los recursos compartidos SMB después de la restauración del servidor NAS, ejecute el siguiente comando antes de restaurar los sistemas de archivos:

```
svc_nas run nas_svc_nas <NAS server name> -param -f PAX -modify honorAdminNDMPPerNasServer
-value 1
```

NOTA: El comando se aplica en el nivel del servidor NAS.

Configuración de la seguridad del servidor NAS

Puede configurar el servidor NAS con seguridad **Kerberos** o **Antivirus**.

La configuración de la seguridad del servidor NAS incluye las siguientes opciones:

- Kerberos
- Antivirus

Configurar la seguridad de Kerberos para el servidor NAS

Puede configurar el servidor NAS con seguridad de Kerberos.

Sobre esta tarea

Asegúrese de agregar el servidor SMB al dominio de AD antes de configurar Kerberos.

Si está configurando el servidor NAS solamente para SMB, no necesita un archivo keytab. El archivo keytab se requiere solamente para la configuración de NFS seguro.

Pasos

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

Comprensión de Common Anti-Virus Agent (CAVA)

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

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

Para conocer las versiones de CAVA de CEE requeridas por PowerStore, consulte las *Notas de la versión de Common Event Enabler* en el sitio de soporte de Dell Technologies. Para obtener información adicional sobre CAVA, que forma parte de Common Event Enabler (CEE), consulte *Uso de Common Event Enabler en plataformas Windows* en el sitio de soporte de Dell Technologies.

Habilitar Common Anti-Virus Agent (CAVA)

Puede habilitar y configurar CAVA cuando desee agregar protección antivirus a los recursos compartidos de SMB.

Requisitos previos

- Un servidor Windows en ejecución con un producto antivirus compatible. Para obtener más información, consulte eLab CEE_CAVA Support Matrix.
- Instale la aplicación CAVA EMC_CEE_Pack_8_x_x_x de 32 o 64 bits en el servidor del antivirus de Windows.

  NOTA: Después de instalar la aplicación, vaya a la sección Inicio de sesión del servicio CAVA de EMC y asigne una cuenta de usuario administrativo de dominio como el usuario del antivirus. Luego, reinicie el servicio.

- Cree un usuario en Active Directory.
- Verifique que SMB esté habilitado en el servidor NAS.

Sobre esta tarea

A partir de PowerStore Manager 4.x, puede configurar CAVA, asignar privilegios de comprobación de virus, ver la configuración y el estado de CAVA, y realizar análisis del sistema de archivos según demanda mediante PowerStore Manager.

NOTA: También es posible realizar estas acciones mediante la CLI y la API REST.

Pasos

1. En PowerStore Manager, vaya a la pestaña **Almacenamiento** > **Servidores NAS** > **[servidor nas]** > **Seguridad y eventos** > **Antivirus**.
2. Seleccione **Configurar** para abrir el cuadro de diálogo **Configurar ajustes del antivirus**.
3. Configure los siguientes parámetros: la dirección IP, las extensiones de archivo que desee analizar y las extensiones de archivo que desee excluir.
   - Dirección IP: configure la dirección IP o el FQDN del servidor del antivirus de Windows.
   - En el caso de las extensiones de archivo que se deban escanear, use el siguiente formato: *.txt, *.docx o *.exe.
   - Extensiones de archivo que se deben excluir: utilice el mismo formato que para los tipos de archivos escaneados.
4. Seleccione **Opciones avanzadas** para establecer los siguientes parámetros:
   - Tamaño máximo de archivo
   - Tiempo de la encuesta
   - Acción de apagado
   - Parámetro alto
   - Parámetro bajo
   - MSRPC User
   - Puerto HTTP
   - Tiempo de espera agotado de reintento de RPC
   - Tiempo de espera agotado de solicitud de RPC

5. Seleccione **Crear**.
   El servicio antivirus se marca como activo.
6. Seleccione el icono Editar para abrir el cuadro de diálogo **Propiedades**.
7. Seleccione **Habilitar** para habilitar el escaneo antivirus y, a continuación, elija **Aplicar**.
8. Para proporcionar al servidor NAS los derechos de comprobación de virus de EMC, seleccione la pestaña **Privilegios de cuenta** y agregue la cuenta de usuario del antivirus del dominio. Utilice el formato Dominio\nombre de usuario (por ejemplo, Lab\anti-virus).

   NOTA: Esta cuenta es la misma cuenta de usuario que está seleccionada en el servicio CAVA de EMC en el servidor de Windows.

9. Para ver los detalles del software antivirus y el estado en línea, seleccione la pestaña **Información de auditoría**.
10. En la pestaña **Sistemas de archivos que se escanearán**, seleccione los sistemas de archivos que desea escanear y, a continuación, elija **Iniciar** para iniciar el escaneo.
11. Si desea que el escaneo incluya archivos offline, seleccione la opción en el mensaje que se muestra y elija **Iniciar escaneo**.
12. Para monitorear el progreso del escaneo, seleccione la pestaña **Estado**.
13. Cuando se completa el escaneo, aparece un mensaje en que se indica el estado.
14. Para detener un escaneo de un sistema de archivos, seleccione el sistema de archivos, elija **Detener escaneo** y, a continuación, confirme la acción en el mensaje que se muestra.
15. Si desea configurar CAVA mediante un archivo de configuración (viruschecker.conf), puede descargar y modificar el archivo actual o cargar un nuevo archivo de configuración mediante la selección de **Cargar/recuperar configuración** en el cuadro de diálogo **Propiedades**.

    NOTA: Para conocer detalles sobre los parámetros del archivo viruschecker.conf, consulte Parámetros configurables del antivirus.

Parámetros configurables del antivirus

En la siguiente tabla se detallan los parámetros que se pueden configurar en el archivo de configuración `viruschecker.conf` de CAVA. Puede crear el archivo de configuración y, a continuación, cargarlo en PowerStore.

Tabla 3. Parámetros del antivirus

Parámetro	Descripción	Obligatorio	Ejemplo
`addr=`	Configura las direcciones IP del servidor o los servidores CAVA.	Sí	`addr=10.205.20.130`
`masks=`	Configura las extensiones de archivo que se escanean.	Sí	`masks=*.exe:*.docx:*.com`
`excl=`	Enumera las extensiones de archivo que se excluyen durante el escaneo.	No	`excl=pagefile.sys`
`maxsize=<n>`	Entero. Configura el tamaño máximo de los archivos que se comprueban. Los archivos que superan este tamaño no son comprobados.	No	`maxsize=4294967290`
`surveyTime=<n>`	Especifica el intervalo de tiempo (en segundos) que se usa para escanear todos los servidores de AV con el fin de ver si están en línea u offline. Si ningún servidor de AV responde, el proceso de apagado comienza con el uso del parámetro shutdown configurado (consulte la siguiente fila).	No	`surveyTime=600`
`shutdown=`	Especifica la acción de apagado que se llevará a cabo cuando no esté disponible ningún servidor. El valor predeterminado es `Allow Access`.	No	`Allow Access`, `Stop_SMB_Access`, `Disable_Virus_Checker`

Tabla 3. Parámetros del antivirus (continuación)

Parámetro	Descripción	Obligatorio	Ejemplo
`highWaterMark=<n>`	Alerta al sistema cuando la cantidad de solicitudes en curso supera `highWaterMark`.	No	`highWaterMark=200`
`lowWaterMark=<n>`	Alerta al sistema cuando la cantidad de solicitudes en curso es menor que `lowWaterMark`.	No	`lowWaterMark=50`

`msrcpuser=`	Especifica el nombre que se asigna a una cuenta de usuario simple o a una cuenta de usuario que es parte de un dominio bajo el cual se ejecuta el servicio CAVA en la máquina de CEE.	No	Cuenta de usuario:
			`msrpcuser=user1`
			Dominio/cuenta de usuario:
			`msrpcuser=CEE1/user1`

`httpport=`	Especifica el número de puerto HTTP en la máquina de CEE que utiliza el sistema.	No	`httpport=12228`
`RPCRetryTimeout`	Configura el tiempo de espera (en milisegundos) de reintento de RPC.	No	`RPCRetryTimeout=4000 milliseconds`
`RPCRequestTimeout`	Configura el tiempo de espera (en milisegundos) de la solicitud de RPC. Cuando se envía una llamada RPC al servidor CAVA, si el servidor responde después de RPCRetryTimeout, el servidor NAS reintenta la operación hasta que se alcanza RPCRequestTimeout y, a continuación, pasa al siguiente servidor CAVA disponible.	No	`RPCRequestTimeout=20000 milliseconds`
`reference time`	Habilita un escaneo en la primera lectura. Si la hora del último acceso de un archivo es anterior a `reference time`, en el acceso, el archivo se envía al programa antivirus antes de que se le otorgue acceso al cliente.	No	`reference_time=2022-10-27T18:30:00`

4

Crear sistemas de archivos y recursos compartidos de SMB

Este capítulo incluye la siguiente información:

Temas:

Crear un sistema de archivos

Se debe crear un sistema de archivos en el servidor NAS antes de poder crear un recurso compartido de SMB.

Requisitos previos

Asegúrese de que haya un servidor NAS configurado para admitir el protocolo SMB, como se describe en Configuración de servidores NAS.

Pasos

1. Seleccione **Almacenamiento** > **Sistemas de archivos** y haga clic en **Crear**.
2. Continúe trabajando a través del asistente **Create File System**.

Opción	Descripción
Seleccionar tipo	Seleccione **General** como el tipo de sistema de archivos
Select NAS Server	Seleccione un servidor NAS habilitado para SMB.
Advanced SMB Settings	De manera opcional, elija una de las siguientes opciones: • **Escrituras síncronas habilitadas** • **Bloqueos oportunos habilitados** • **Notificar sobre escritura habilitada** • **Notificar sobre un acceso habilitado** • **Habilitar publicación de eventos de SMB** Para obtener información detallada, consulte Ajustes avanzados del sistema de archivos para recursos compartidos de SMB.
File System Details	Proporcione el nombre del sistema de archivos y el tamaño del sistema de archivos. 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 y Modelo PowerStore Q muestran inmediatamente 1,5 GB utilizados. Cuando el sistema de archivos se monta en un host, muestra 98,5 GB de capacidad útil. Esto se debe a que el espacio de metadatos se reserva de la capacidad útil del sistema de archivos.
Retención en el nivel de archivos	De manera opcional, seleccione el tipo de retención de archivos: • Enterprise (FLR-E): protege el contenido de cambios realizados por los usuarios a través de CIFS y FTP. Un administrador puede eliminar un sistema de archivos FLR-E que contiene archivos protegidos.

Opción	Descripción
	• Compliance (FLR-C): protege el contenido de cambios realizados por los usuarios y los administradores y cumple con los requisitos de la norma 17a-4(f) de SEC. El sistema de archivos FLR-C se puede eliminar solo cuando no contiene ningún archivo protegido. **NOTA:** El estado de FLR y el tipo de retención de archivos se configuran en la creación del sistema de archivos y no se pueden modificar. Configure los períodos de retención: • Mínimo: especifica el período más corto durante el cual se pueden bloquear los archivos (el valor predeterminado es 1 día). • Predeterminado: se utiliza cuando un archivo se bloquea y no se especifica ningún período de retención. • Máximo: especifica el período más largo durante el cual se pueden bloquear los archivos.
SMB Share	De manera opcional, configure el recurso compartido SMB inicial. Puede agregar recursos compartidos al sistema de archivos después de la configuración inicial del sistema de archivos. Para obtener información detallada sobre las opciones de recursos compartidos de SMB, consulte Crear un recurso compartido de SMB.
Política de protección	De manera opcional, proporcione una política de protección para el sistema de archivos. PowerStore soporta instantáneas y replicación para la protección del almacenamiento de archivos.
Política de QoS de archivos	De manera opcional, seleccione una política de QoS de archivos para el 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. Vuelva para realizar las actualizaciones necesarias.

3. Haga clic en **Create File System**.
El sistema de archivos se muestra en la lista File System y, si creó un recurso compartido SMB, se muestra en la lista SMB Share.

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 4. 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 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. Esta opción está desactivada de manera 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	(Habilitado de manera predeterminada) Los bloqueos oportunos de archivos (bloqueos oportunos, también conocidos como bloqueos oportunos de nivel 1) permiten que los clientes SMB almacenen localmente en el buffer los datos en archivos antes de enviarlos a un servidor. Los clientes SMB pueden trabajar con los archivos de forma local y comunicar periódicamente los cambios al sistema de almacenamiento en lugar de tener que comunicar cada operación al sistema de almacenamiento a través la red. Esta característica está habilitada de forma predeterminada para los sistemas de archivos Windows (SMB) y multiprotocolo. Salvo que su aplicación maneje datos cruciales o tenga requisitos específicos que anulen este

Tabla 4. Ajustes avanzados del sistema de archivos para SMB (continuación)

Configuración	Descripción
	modo u operación, se recomienda dejar los oplocks activados. 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. El bloqueo oportuno de segundo nivel permite al cliente ejecutar operaciones de lectura y búsquedas de atributos de archivos utilizando la información almacenada en caché o la información local con 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.
Notificación en caso de acceso habilitada	active la notificación cuando se acceda a un sistema de archivos. Esta opción está desactivada de manera predeterminada.
Habilitar publicación de eventos de SMB	Habilite el procesamiento de eventos de SMB para este sistema de archivos.

Crear un recurso compartido de 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 **Storage** > **File System** > **SMB Share**.
2. Haga clic en **Create** y continúe avanzando en el asistente **Create SMB Share**.

Opción	Descripción
Seleccionar sistema de archivos	Seleccione un sistema de archivos que se haya habilitado para SMB.
Seleccione una instantánea del sistema de archivos	De manera opcional, seleccione una de las instantáneas del sistema de archivos en la que cual creará el recurso compartido. Para las políticas de protección del sistema de archivos solamente se admiten las instantáneas. La replicación no es compatible para los sistemas de archivos.
SMB Share Details	Ingrese un nombre 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.

Opción	Descripción
	PowerStore también creó la ruta del recurso compartido de SMB, la que utiliza el host para conectarse al recurso compartido. La ruta de exportación es la dirección IP del sistema de archivos y el nombre del recurso compartido. Los hosts utilizan el nombre de archivo o la ruta del recurso compartido para el montaje del recurso compartido o el mapeo a este desde un host de red.
Advanced SMB Properties	Habilite uno o más de los ajustes avanzados de SMB. ● Disponibilidad continua ● Cifrado de protocolo ● Enumeración basada en acceso ● Caché de sucursal activada Decida qué objetos están disponibles cuando el recurso compartido está offline. Para obtener información detallada, consulte Propiedades avanzadas de SMB.

Siguientes pasos

Una vez que cree 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 5. 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 no cifrado NAS (la ruta de la clave es HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanServer\Parameters\RejectUnencryptedAccess). 1 (valor predeterminado) rechaza el acceso 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.
Disponibilidad offline	Configura el almacenamiento en caché de los archivos offline del lado del cliente: ● **Ninguno**: el almacenamiento en caché del lado del cliente de archivos offline no está configurado (valor predeterminado). ● **Manual**: los archivos se almacenan en caché y están disponibles offline únicamente cuando el almacenamiento en caché se solicita de manera explícita.

Tabla 5. Propiedades avanzadas de SMB (continuación)

Opción	Descripción
	• **Programas**: todos los archivos que abren los clientes desde el recurso compartido están disponibles automáticamente offline. Los archivos ejecutables que se han almacenado en caché localmente con anterioridad se ejecutan desde la copia almacenada en caché, incluso cuando el recurso compartido está disponible. • **Documentos**: todos los archivos que abren los clientes desde el recurso compartido están disponibles automáticamente offline. Cada vez que un usuario accede a un archivo desde un recurso compartido, el contenido se almacena en caché automáticamente a fin de que esté disponible para el usuario en el modo offline. Todos los archivos que se abren continúan almacenándose en caché y estando disponibles para el acceso offline hasta que la caché se llena. El contenido almacenado en caché continúa sincronizándose con la versión del servidor. Los archivos que no se han abierto no están disponibles offline.

Administrar ACL

El cliente de Windows establece y modifica los permisos de acceso de recursos compartidos de SMB (conocidos como listas de control de acceso o ACL) mediante la consola de MMC. Ahora puede administrar las ACL de recursos compartidos SMB en el clúster SDNAS directamente desde PowerStore con el uso de la interfaz de usuario o la API REST.

NOTA: Para conocer detalles sobre el uso de la API REST con el fin de configurar los ACL, consulte la *Guía de referencia de la API REST de Dell PowerStore* en dell.com/powerstoredocs.

NOTA: Los permisos de acceso de archivos y directorios en los recursos compartidos SMB se pueden administrar solo mediante el cliente de Windows.

Para abrir la pantalla Lista de control de acceso a través de PowerStore Manager, seleccione **Almacenamiento** > **Sistemas de archivos** > **Recursos compartidos SMB** > **[SMB share]** > **Más acciones** > **Lista de control de acceso**.

En la pantalla Lista de control de acceso, se muestra la lista de entradas de control de acceso (ACE) definidas para el SMB seleccionado. Para cada ACE, se enumeran el nombre o el ID del elemento de confianza, el nivel de acceso y el tipo de acceso. Puede filtrar la lista por cualquiera de los atributos.

NOTA: La ACE predeterminada otorga permisos completos a todos.

En el cuadro de diálogo Lista de control de acceso, puede realizar lo siguiente:

- Agregar ACE: para obtener detalles, consulte Agregar una entrada de control de acceso.
- Modificar ACE: edite cualquiera de los campos de la ACE seleccionados.
- Eliminar la ACE seleccionada.
- Actualizar ACL (en **Más acciones**): utilice esta opción si modificó la ACL mediante la consola de MMC de Windows o la API REST. La opción Actualizar actualiza la ACL con los cambios.

Agregar una entrada de control de acceso

Sobre esta tarea

Una ACE consta de los siguientes atributos:

- Tipo de elemento de confianza: usuario, grupo, identificador de seguridad (SID) o WellKnown
- Nombre/ID de elemento de confianza: el formato de este campo se determina según el tipo de elemento de confianza:
  - Nombre de usuario: dominio/nombre de usuario
  - Nombre de grupo: dominio/nombre de grupo
  - SID: formato de SID (por ejemplo, S-1-2-34-567890123-456789012-3456789012-34)
  - WellKnown: por ejemplo, “Everyone”
- Nivel de acceso: lectura, cambio o completo
- Tipo de acceso: permitir o denegar

Pasos

1. Seleccione **Almacenamiento** > **Sistemas de archivos** > **Recursos compartidos SMB** > **[SMB share]** > **Más acciones** > **Lista de control de acceso**.

2. En la ventana **Lista de control de acceso**, seleccione **Agregar ACE**.
3. Configure los campos de ACE y haga clic en **Guardar**.
   La nueva ACE se agrega a la ACL.
4. Haga clic en **Apply** para guardar los cambios.

5

Más funciones del sistema de archivos

Este capítulo incluye la siguiente información:

Temas:

Retención de archivos

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

Hay dos tipos de retención en el nivel de archivos:

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

Se aplican las siguientes restricciones:

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

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

Configurar el servidor DHSM

Requisitos previos

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

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

Pasos

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

Configurar la retención en el nivel de archivos

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

NOTA: Los parámetros del período de retención se pueden modificar posteriormente.

Modificar retención en el nivel de archivos

Sobre esta tarea

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

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

Pasos

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

Cuotas de sistemas de archivos

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

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

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

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

Tipos de cuotas

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

Tabla 6. Tipos de cuota

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

Límites de cuota

Tabla 7. Límites máximo y de advertencia

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

Período de gracia de cuota

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

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

Información adicional

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

Habilitar cuotas de usuario

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

Pasos

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

Agregar una cuota de usuario en un sistema de archivos

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

Requisitos previos

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

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

Pasos

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

Agregar un árbol de cuotas en un sistema de archivos

Sobre esta tarea

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

Pasos

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

Agregar una cuota de usuario en un árbol de cuotas

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

Pasos

1. Seleccione **Storage** > **File Systems** > **[file system]** > **Quotas** > **Tree Quotas**.

2. Seleccione una ruta y haga clic en **Add User Quota**.
3. En la pantalla **Add User Quota**, proporcione la información solicitada. Para rastrear el consumo de espacio sin establecer límites, configure los campos **Soft Limit** y **Hard Limit** en 0, lo cual indica que no hay límites.

Calidad de servicio (QoS) de archivos

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

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

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

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

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

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

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

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

Límites de QoS de archivos:

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

QoS y replicación de archivos:

- Cuando el servidor NAS tiene una regla de replicación, la política de QoS asignada se replica en el servidor de destino.
- Cuando modifica las políticas de QoS asignadas al servidor NAS, los cambios se replican en el servidor de destino.
- No es posible modificar la configuración de la política de QoS replicada en el servidor de destino.
- No es posible asignar una política de QoS a un servidor NAS o sistema de archivos en el servidor de destino.
- Después de asignar una política de QoS a un servidor NAS o un sistema de archivos en el servidor de origen, no es posible cancelar la asignación de la política del servidor de destino.
- Después de cancelar la asignación de una política de QoS desde un servidor NAS, la política también se debe cancelar en el destino.
- Después de la conmutación por error, puede asignar, cancelar la asignación y modificar las políticas de QoS replicadas.

Límites de QoS de archivos

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

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

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

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

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

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

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

Sobre esta tarea

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

Pasos

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

Asignación de una política de QoS de archivos

Sobre esta tarea

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

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

Pasos

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

Modificación de una política de QoS de archivos

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

Requisitos previos

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

Pasos

1. Seleccione **Almacenamiento** > **Calidad de servicio (QoS)**.
2. En la tabla **Políticas de QoS de archivos**, seleccione la casilla de verificación junto a la política de QoS que desee modificar.
3. Seleccione **Modify**.

4. En la ventana **Modificar política de QoS**, puede modificar el nombre y la descripción de la política y seleccionar una regla de límite de I/O diferente.
5. Seleccione **Aplicar**.

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

Eliminación de una política de QoS de archivos

Requisitos previos

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

Pasos

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

6

Replicación del servidor NAS

Este capítulo incluye la siguiente información:

Temas:

Descripción general

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

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

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

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

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

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

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

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

Prueba de recuperación ante desastres para servidores NAS en replicación

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

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

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

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

Sobre esta tarea

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

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

Puede elegir cualquiera de las siguientes opciones:

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

Pasos

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

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

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

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

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

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

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

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

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

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

Requisitos y limitaciones

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

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

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

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

Configurar el entorno de pruebas de recuperación ante desastres mediante PSTCLI

Pasos

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

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

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

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

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

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

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

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

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

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

5. Vea la interfaz de archivos:

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

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

Sobre esta tarea

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

Pasos

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

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

Resultados

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

Realizar una conmutación por error planificada

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

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

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

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

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

Los cambios que se descartan:

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

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

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

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

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

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

Existen dos maneras de iniciar una conmutación por error prevista:

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

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

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

Desconexión de red durante una DRT

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

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

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

7

Uso de CEPA con PowerStore

Este capítulo incluye la siguiente información:

Temas:

Publicación de eventos

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

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

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

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

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

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

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

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

Crear un pool de publicación

Requisitos previos

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

Sobre esta tarea

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

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

Pasos

1. Seleccione **Almacenamiento** > **Servidores NAS**.
2. Seleccione **Ajustes de NAS**.
3. En la ventana **Publicación de eventos**, seleccione **Pools de publicación** y, a continuación, seleccione **Crear**.
4. Ingrese un **Nombre del pool**.
5. Ingrese el FQDN del servidor CEPA.
6. En la sección Configuración de evento, haga clic en los tipos de evento y seleccione los que desea agregar al pool.
7. Haga clic en **Aplicar** para crear el pool de publicación de eventos.

Crear un publicador de eventos

Sobre esta tarea

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

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

Pasos

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

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

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

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

Habilitación de un publicador de eventos para un servidor NAS

Sobre esta tarea

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

Pasos

1. Seleccione **Almacenamiento** > **Servidores NAS** > **[nas server]**.

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

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

Habilitar el publicador de eventos para un sistema de archivos

Sobre esta tarea

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

Pasos

1. Seleccione **Almacenamiento** > **Sistemas de archivos** > **[file system]**.
2. En la página **Protección**, seleccione **Publicación de eventos**.
3. Habilite el publicador de eventos para el sistema de archivos y seleccione el protocolo.
4. Haga clic en **Aplicar**.