

Dell EMC PowerStore

Configuración de SMB

3.x

Notas, precauciones y avisos

-  **NOTA:** Una NOTA indica información importante que le ayuda a hacer un mejor uso de su producto.
-  **PRECAUCIÓN:** Una PRECAUCIÓN indica la posibilidad de daños en el hardware o la pérdida de datos, y le explica cómo evitar el problema.
-  **AVISO:** Un mensaje de AVISO indica el riesgo de daños materiales, lesiones corporales o incluso la muerte.

Tabla de contenido

Recursos adicionales.....	5
Capítulo 1: Descripción general.....	6
Compatibilidad con SMB.....	6
Consideraciones de planificación.....	6
Redes de servidores NAS.....	6
Requisitos de implementación.....	7
Más consideraciones.....	7
Crear un enlace LACP para el tráfico NAS.....	7
Creación de recursos compartidos de SMB.....	7
Recursos de documentación.....	8
Capítulo 2: Creación de servidores NAS.....	9
Descripción general de la configuración de servidores NAS.....	9
Crear un servidor NAS para los sistemas de archivos SMB (solamente Windows).....	9
Modificación de la configuración de los servidores NAS.....	10
Capítulo 3: Funciones adicionales del servidor NAS.....	12
Configurar el protocolo de uso compartido FTP o SFTP.....	12
Configurar redes de servidores NAS.....	12
Configurar interfaces de archivos para un servidor NAS.....	12
Configurar rutas para la interfaz de archivos para conexiones externas.....	13
Habilitar el respaldo NDMP.....	13
Configurar la seguridad del servidor NAS.....	14
Configurar la seguridad de Kerberos para el servidor NAS.....	14
Comprensión de Common AntiVirus Agent (CAVA).....	14
Capítulo 4: Crear sistemas de archivos y recursos compartidos de SMB.....	17
Crear un sistema de archivos.....	17
Ajustes avanzados del sistema de archivos para SMB.....	18
Crear un recurso compartido de SMB.....	19
Propiedades avanzadas de recursos compartidos de SMB.....	20
Capítulo 5: Más funciones del sistema de archivos.....	22
Retención en el nivel de archivos.....	22
Configurar el servidor DHSM.....	22
Configurar la retención en el nivel de archivos.....	23
Modificar la retención en el nivel de archivos.....	23
Cuotas de sistemas de archivos.....	23
Habilitar cuotas de usuario.....	24
Agregar una cuota de usuario en un sistema de archivos.....	25
Agregar un árbol de cuotas en un sistema de archivos.....	25
Agregar una cuota de usuario en un árbol de cuotas.....	25

Capítulo 6: Replicación del servidor NAS.....	27
Descripción general.....	27
Capítulo 7: Uso de CEPA con PowerStore.....	28
Publicación de eventos.....	28
Crear un pool de publicación.....	28
Crear un publicador de eventos.....	29
Habilitación de un publicador de eventos para un servidor NAS.....	29
Habilitar el publicador de eventos para un sistema de archivos.....	30

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

Dónde obtener ayuda

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

- **Información de productos**

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

- **Solución de problemas**

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

- **Soporte técnico**

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

Descripción general

Este capítulo incluye la siguiente información:

Temas:

- [Compatibilidad con SMB](#)
- [Consideraciones de planificación](#)

Compatibilidad con SMB

Modelo PowerStore T es compatible con 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.

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:

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

Redes de servidores NAS

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 planea crear una VLAN para los servidores NAS, la VLAN no se puede compartir con la administración de Modelo PowerStore T ni con las redes de almacenamiento. Además, asegúrese de trabajar con el administrador de red para reservar los recursos de red y configurar la red en el switch. Para obtener más información, consulte *Guía de redes de PowerStore para modelos PowerStore T*.

Requisitos de implementación

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

Debe haber seleccionado **Unificado** durante la configuración inicial de su dispositivo Modelo PowerStore T. 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 de servicio al cliente debe reinicializar el sistema. Reinicialización del sistema:

- Configura el dispositivo en el estado de fábrica.
- Elimina toda la configuración que se realizó en el sistema a través 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 un enlace LACP para el tráfico NAS

Puede combinar varias interfaces de red en un enlace de red para fines de redundancia y alta disponibilidad.

Sobre esta tarea

La vinculación de red es un proceso en el que se combinan dos o más interfaces de red con una sola interfaz. El uso de la vinculación de red proporciona mejoras de rendimiento y redundancia mediante el aumento del ancho de banda y el rendimiento de la red. Si una de las interfaces combinadas está inactiva, las otras interfaces permiten mantener una conexión estable.

Puede usar la vinculación de red mediante la creación de un grupo agregado de vínculos (LAG) para el tráfico NAS.

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 agregar el enlace del protocolo de control agregado de enlaces (LACP) al servicio al 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:** Deberá seleccionar el nombre de enlace cuando cree el servidor NAS.

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
<i>Guía de redes de PowerStore para modelos PowerStore T</i>	Proporciona información sobre la planificación y la configuración de la red.	https://www.dell.com/powerstoredocs
<i>Guía de configuración de NFS de PowerStore</i>	Proporciona información necesaria para configurar exportaciones de NFS con PowerStore Manager.	
<i>Documentación técnica sobre las funcionalidades de archivos de PowerStore de Dell EMC</i>	Analiza las funciones, la funcionalidad y los protocolos compatibles con la arquitectura de archivos de PowerStore de Dell EMC.	
<i>Ayuda en línea de PowerStore</i>	Proporciona información confidencial contextual para la página que se abre en PowerStore Manager.	Integrada en PowerStore Manager

Creación de servidores NAS

Este capítulo incluye la siguiente información:

Temas:

- Descripción general de la configuración de servidores NAS
- Crear un servidor NAS para los sistemas de archivos SMB (solamente Windows)
- Modificación de la configuración de los servidores NAS

Descripción general de la configuración de servidores NAS

Antes de que pueda aprovisionar el almacenamiento de archivos en el dispositivo Modelo PowerStore T, 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 (solamente Windows)

Debe crear 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 es compatible con 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 utilizará para el administrador local independiente de la cuenta del servidor SMB.
- Si está uniendo el servidor NAS a Active Directory (AD), asegúrese de que NTP esté configurado en el sistema de almacenamiento. A continuación, obtenga el nombre de computadora de SMB (que se usa para acceder a recursos compartidos de 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

Pantalla del asistente	Descripción
	- Descripción del servidor NAS - Interfaz de red: si creó una vinculación LACP, selecciónela de la lista (consulte Crear una vinculación LACP para el tráfico NAS). - Información de red
Protocolo de uso compartido	Seleccione Protocolo de uso compartido 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. Ajustes de Windows Server 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 a AD, seleccione de manera opcional Advanced para cambiar el nombre de NetBios y la unidad organizacional predeterminados. DNS Si seleccionó Join to the Active Directory Domain, la adición de un servidor DNS es obligatoria. De manera opcional, habilite DNS si desea usar un servidor DNS para el servidor SMB independiente. Mapeo de usuarios Se muestra la página User Mapping si ha seleccionado unirse al dominio de Active Directory. Conserve la opción predeterminada Enable automatic mapping for unmapped Windows accounts/users para admitir la unión al dominio de Active Directory. Se requiere la asignación automática cuando se une al dominio de Active Directory.
Política de protección	Seleccione una política de protección 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 **Status** y se lo redirige a la página **NAS Servers** cuando se crea el servidor.

Siguientes pasos

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

Modificación de la configuración de los servidores 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 **SMB Server** para habilitar o deshabilitar la compatibilidad con recursos compartidos de Windows y 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 **User mapping** 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 **Protection & Events**, habilite o deshabilite NDMP.

Para obtener información detallada, consulte [Habilitar la protección y los eventos de NDMP](#).

6. En la pestaña **Security**:

- 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 obtener información detallada, consulte [Configurar la seguridad del servidor NAS](#)

Funciones adicionales del servidor NAS

Este capítulo incluye la siguiente información:

Temas:

- [Configurar el protocolo de uso compartido FTP o SFTP](#)
- [Configurar redes de servidores NAS](#)
- [Habilitar el respaldo NDMP](#)
- [Configurar la seguridad del servidor NAS](#)

Configurar el 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 **Apply**.

Configurar redes de servidores NAS

Puede modificar o configurar redes de servidores NAS.

Configure lo siguiente para las redes de servidores NAS:

- [Las interfaces de archivos](#)
- [Rutas a servicios externos, como hosts](#).

Configurar interfaces de archivos para un servidor NAS

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

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 puede reutilizar las VLAN que se utilizan para las redes de administración y almacenamiento.

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

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

Configurar rutas para la interfaz de archivos para conexiones externas

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

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

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 otros fabricantes, como Dell EMC NetWorker, puede detectar el NDMP 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 a través de la DMA a través de una red de área local (LAN) o una red de área extendida (WAN).

- RespalDOS completos e incrementales.

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 **Verify Password**.
5. Haga clic en **Aplicar**.

Siguientes pasos

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

Configurar la seguridad del servidor NAS

Puede configurar el servidor NAS con las opciones de 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 AntiVirus Agent (CAVA)

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

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 CEE CAVA compatibles con PowerStore, consulte *Notas de la versión de PowerStore*. Para obtener información adicional sobre CAVA, que forma parte de Common Event Enabler (CEE), consulte *Uso de Common Event Enabler en plataformas Windows* en <https://www.dell.com/support>.

Habilitar Common AntiVirus Agent (CAVA)

Debe habilitar CAVA y cargar el archivo de configuración de CAVA cuando desea agregar protección antivirus a los recursos compartidos de SMB.

Requisitos previos

Para habilitar el escaneo antivirus, debe crear un usuario en Active Directory y, a continuación, otorgarle permisos en el servidor CAVA para realizar escaneos.

Pasos

1. En PowerStore Manager, vaya a la pestaña **Almacenamiento > Servidores NAS > [servidor nas] > Seguridad y eventos > Antivirus**.
2. Si Disabled está activo, deslice el botón para seleccionar **Enabled**.
3. Si no está disponible un archivo de configuración actual de CAVA:
 - a. Haga clic en **Retrieve Current Configuration**.
 - b. Complete la plantilla del archivo de configuración de CAVA.
 - c. Cargue el archivo de configuración CAVA actualizado.
4. Haga clic en **Enabled** y en **Apply** para activar la detección 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 escanearán.	Sí	masks=*.exe;*.docx;*.com
excl=	Enumera las extensiones de archivo que se excluirán durante el escaneo.	No	excl=pagefile.sys
maxsize=<n>	Entero. Configura el tamaño máximo de los archivos que se comprobarán. 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 asignado 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: msrcpuser=user1 Dominio/cuenta de usuario: msrcpuser=CEE1/user1
httpport=	Especifica el número de puerto HTTP en la máquina de CEE que utilizará 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

Crear sistemas de archivos y recursos compartidos de SMB

Este capítulo incluye la siguiente información:

Temas:

- [Crear un sistema de archivos](#)
- [Crear un recurso compartido de SMB](#)

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 avanzando en el asistente **Crear sistema de archivos**.

Opción	Descripción
Seleccionar tipo	Seleccione General como el tipo de sistema de archivos
Seleccionar servidor NAS	Seleccione un servidor NAS habilitado para SMB.
Ajustes avanzados de SMB	De manera opcional, elija entre las siguientes opciones: • Escrituras síncronas habilitadas • Bloqueos oportunos habilitados • Notificación en caso de escritura habilitada • Notificación en caso de acceso habilitada • Habilitar publicación de eventos de SMB Para obtener información detallada, consulte Ajustes avanzados del sistema de archivos para recursos compartidos de SMB.
Detalles del sistema de archivos	Proporcione el nombre y el tamaño del sistema de archivos. El tamaño del sistema de archivos puede ser entre 3 GB y 256 TB.  NOTA: Todos los sistemas de archivos delgados, independientemente del tamaño, tienen 1,5 GB reservados para metadatos después de la creación. Por ejemplo, después de crear un sistema de archivos delgado de 100 GB, Modelo PowerStore T muestra inmediatamente 1,5 GB utilizados. Cuando el sistema de archivos se monta en un host, muestra 98,5 GB de capacidad útil. Esto se debe a que se reserva el espacio de metadatos en la capacidad útil del sistema de archivos.
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.
Recurso compartido de SMB	De manera opcional, configure el recurso compartido de 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 admite instantáneas y replicación para la protección del almacenamiento de archivos.
Resumen	Revise el resumen. Regrese para realizar las actualizaciones que sean necesarias.

3. Haga clic en **Crear sistema de archivos**.

El sistema de archivos se muestra en la lista de sistemas de archivos y, si creó un recurso compartido de SMB, este se muestra en la lista de recursos compartidos de SMB.

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 modo u operación, se recomienda dejar los oplocks activados. Se admiten las siguientes implementaciones de oplocks:

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

Configuración	Descripción
	• 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 oplock de segundo nivel les permite a los clientes ejecutar operaciones de lectura y recuperar atributos de archivos al utilizar la información 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 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 NAS. 1 (valor predeterminado) rechaza el acceso no cifrado y 0 permite a clientes que no son compatibles con el cifrado acceder al sistema de archivos sin cifrado.
Enumeración basada en acceso	Filtra la lista de directorios y archivos disponibles en el recurso compartido para incluir solo los que brinden acceso de lectura al usuario que lo solicita.  NOTA: Los administradores siempre pueden firmar todos los archivos.
Caché en sucursal habilitada	Copia contenido del recurso compartido y lo copia en la memoria caché en las sucursales. Esto permite a los equipos cliente de las sucursales tener acceso al contenido de forma local, en lugar de mediante la WAN. BranchCache se administra desde los hosts de Microsoft.
Disponibilidad offline	Configura el almacenamiento en caché de los archivos offline del lado del cliente: • Manual: los archivos se almacenan en caché y están disponibles offline únicamente cuando el almacenamiento en caché se solicita de manera explícita.

Tabla 5. Propiedades avanzadas de SMB (continuación)

Opción	Descripción
	• Programas y archivos abiertos por usuarios: todos los archivos que abren los clientes desde el recurso compartido se almacenan en caché y están disponibles offline automáticamente. Los clientes abren estos archivos desde el recurso compartido cuando están conectados a él. Esta opción se recomienda para archivos con trabajo compartido. • Programas y archivos abiertos por usuarios, optimizar para rendimiento: todos los archivos que abren los clientes desde el recurso compartido se almacenan en caché y están disponibles offline automáticamente. Los clientes abren estos archivos desde la memoria caché local del recurso compartido, si es posible, incluso cuando están conectados a la red. Esta opción se recomienda para la mayoría de los programas ejecutables. • Ninguno: el almacenamiento en caché del lado del cliente de archivos offline no está configurado.

Más funciones del sistema de archivos

Este capítulo incluye la siguiente información:

Temas:

- [Retención en el nivel de archivos](#)
- [Cuotas de sistemas de archivos](#)

Retención en el nivel de archivos

La retención en el nivel de archivos (FLR) permite evitar modificaciones o la eliminación de archivos bloqueados 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 de datos y su accesibilidad, simplifica los procedimientos de archivado para los administradores y mejora la flexibilidad de la administración del almacenamiento.

Hay dos niveles 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:

- La retención en el nivel de archivos está disponible en el sistema PowerStore 3.0 o superior unificado.
- La FLR no se admite en sistemas de archivos VMware.
- La habilitación de una retención en el nivel de archivos para un sistema de archivos y el nivel 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 tener el mismo nivel de FLR.
- Cuando se replica un sistema de archivos, los sistemas de archivos de origen y destino deben tener el mismo nivel de FLR.
- Un sistema de archivos clonado tiene el mismo nivel de FLR que el origen (no se puede modificar).

El modo de FLR se muestra en la pantalla **Sistemas de archivos**.

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 más adelante.

Modificar la 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. La modificación del parámetro 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 especificó 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 configurar 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 **Aplicar**.

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.

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 que almacena datos en el sistema de archivos.

Tabla 6. Tipos de cuota (continuación)

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

Límites de cuotas

Tabla 7. Límites máximo y de advertencia

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

Período de gracia de cuotas

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

Puede establecer una fecha de vencimiento para el período de gracia. El valor predeterminado es de 7 días. De manera alternativa, puede configurar la fecha de vencimiento del período de gracia en una cantidad infinita de tiempo y el período de gracia nunca vencerá, o en una cantidad determinada de días, horas o minutos. Cuando se alcanza la fecha de vencimiento del período de gracia, el período de gracia ya no se aplica al directorio del sistema de archivos.

Información adicional

Para obtener más información sobre las cuotas, consulte la *Documentación técnica sobre las funcionalidades de archivos de PowerStore de Dell EMC*.

Habilitar cuotas de usuario

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

Pasos

1. Seleccione **Storage > File Systems > [file system] > Quotas**.
2. Seleccione **Storage > File Systems > [file system] > Quotas > Properties**.
3. Deslice el botón **Disabled** hacia la derecha hasta que se seleccione **Enabled**.
4. Ingrese el valor predeterminado de **Grace Period** para la cuota de usuario en el sistema de archivos, el cual contará el tiempo de inactividad después de que se cumpla el límite mínimo hasta que se alcance el límite máximo.
5. Ingrese un valor predeterminado de **Soft Limit** y **Hard Limit**, y haga clic en **Update**.

Agregar una cuota de usuario en un sistema de archivos

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

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.

Replicación del servidor NAS

Este capítulo incluye la siguiente información:

Temas:

- [Descripción general](#)

Descripción general

PowerStore le permite replicar servidores NAS de manera asíncrona entre un sistema local y un sistema remoto. La replicación se produce en el nivel del servidor NAS: todos los sistemas de archivos dentro del servidor NAS replicado se replican al sistema remoto. El RPO se configura en el nivel del servidor NAS y es idéntico en todos los sistemas de archivos asociados.

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 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.

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

- Un sistema remoto de archivos
- Una red de movilidad de archivos que esté configurada y mapeada (consulte *Guía de redes para modelos PowerStore T* en la página Documentación de PowerStore en <https://www.dell.com/powerstoredocs>).
- Una política de protección que incluya una regla de replicación.

Para obtener información detallada sobre los procedimientos de replicación del servidor NAS, consulte *Protección de sus datos* en la página Documentación de PowerStore en <https://www.dell.com/powerstoredocs>.

Uso de CEPA con PowerStore

Este capítulo incluye la siguiente información:

Temas:

- [Publicación de eventos](#)
- [Crear un pool de publicación](#)
- [Crear un publicador de eventos](#)
- [Habilitación de un publicador de eventos para un servidor NAS](#)
- [Habilitar el publicador de eventos para un sistema de archivos](#)

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 Windows Platforms* en <https://www.dell.com/support>.

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**.