# Dell PowerStore

## Configurar o NFS

4.3

AVISO: Este conteúdo foi traduzido usando inteligência artificial (IA). Ele pode conter erros e é fornecido "no estado em que se encontra", sem qualquer tipo de garantia. Para ver o conteúdo original (não traduzido), consulte a versão em inglês. Em caso de dúvidas ou preocupações sobre este conteúdo, entre em contato com a Dell pelo e-mail Dell.Translation.Feedback@dell.com.

Dezembro 2025
Rev. A08

DELL Technologies

## Notas, avisos e advertências

**NOTA:** NOTA fornece informações importantes para ajudar você a usar melhor o computador.

**CUIDADO: Um AVISO indica possíveis danos ao hardware ou perda de dados e ensina como evitar o problema.**

**ATENÇÃO: Uma ADVERTÊNCIA indica possíveis danos à propriedade, lesões corporais ou risco de morte.**

Copyright © 2020- 2025 Dell Inc. Todos os direitos reservados. Dell Technologies, Dell e outras marcas comerciais são marcas comerciais da Dell Inc. ou de suas subsidiárias. Todas as outras marcas comerciais são marcas comerciais de seus respectivos proprietários.

# Índice

# Prefácio

Como parte de um esforço contínuo de melhorias, lançamos periodicamente revisões de seu software e hardware. Algumas das funções descritas neste documento não são compatíveis com todas as versões de software ou hardware usadas no momento. As notas da versão do produto contêm as informações mais recentes sobre os recursos do produto. Entre em contato com seu fornecedor se um produto não funcionar adequadamente ou conforme descrito neste documento.

**NOTA:** Clientes Modelo PowerStore X: para obter os manuais e guias técnicos de instruções mais recentes para o seu modelo, faça download do *Conjunto de documentação do PowerStore 3.2.x* na página Documentação do PowerStore em dell.com/powerstoredocs.

## Onde obter ajuda

As informações sobre licenciamento, suporte e produtos EMC podem ser obtidas da seguinte maneira:

- **Informações do produto**: para obter a documentação do produto e dos recursos ou as notas da versão, acesse a página de documentação do PowerStore em dell.com/powerstoredocs.
- **Solução de problemas**: para obter informações sobre produtos, atualizações do software, licenciamento e serviços, acesse Suporte Dell e localize a página de suporte ao produto apropriada.
- **Suporte técnico**: para suporte técnico e chamados, acesse Suporte Dell e localize a página **Chamados**. Para abrir um chamado, você deve ter um contrato de suporte válido. Entre em contato com o representante de vendas para saber como obter um contrato de suporte válido ou para tirar dúvidas sobre sua conta.

# 1

# Visão geral

Este tópico contém as seguintes informações:

**Tópicos:**



# Compatibilidade com NFS

O Modelo PowerStore T e o PowerStore modelo Q oferecem suporte a NFSv3 e NFSv4. Esses modelos também oferecem suporte a Secure NFS com Kerberos, proporcionando uma autenticação sólida. Embora o Modelo PowerStore T e o PowerStore modelo Q ofereçam suporte à maioria das funcionalidades de NFSv4 e v4.1 descritas nas RFCs relevantes, não há suporte a pNFS nem à delegação de diretórios. Na PowerStore versão 3.0 e posterior, o suporte básico para NFSv4.2 no modo de compatibilidade também está disponível. A partir da PowerStore versão 4.3, o suporte ao NFSv4.2 é aprimorado com recursos adicionais, incluindo:

- Cópia dentro do servidor - Este recurso permite que os clientes solicitem operações de cópia interna, reduzindo o tráfego de rede desnecessário.
- Suporte a arquivos fragmentados -
  - A operação READ_PLUS pode identificar buracos (regiões preenchidas com zero) em arquivos fragmentados, eliminando a necessidade de transferir dados zero desnecessários e melhorando o desempenho.
  - A operação SEEK permite que os clients determinem o local dos próximos dados ou furos em um arquivo.
- NFS rotulado - esse recurso permite que o servidor NFS com reconhecimento de MAC armazene rótulos de controle de acesso obrigatório (MAC) nos arquivos. Os rótulos são usados para impor controles de acesso aos dados.

O suporte para NFS é ativado em um servidor NAS durante ou após a criação, permitindo criar file systems habilitados para NFS no servidor NAS.

# Sobre NFS seguro

Você pode configurar o NFS seguro quando criar ou modificar um servidor NAS compatível com compartilhamentos UNIX. O NFS seguro fornece autenticação de usuário baseada em Kerberos, o que pode proporcionar integridade de dados de rede e privacidade de dados de rede.

O Kerberos é um serviço de autenticação distribuído projetado para proporcionar autenticação sólida com criptografia de chave secreta. Ele funciona com base em "tíquetes" que permitem que nós se comuniquem em uma rede não segura para provar sua identidade de maneira segura. Quando configurados para atuarem como um servidor NFS seguro, o servidor NAS usa a estrutura de segurança RPCSEC_GSS e o protocolo de autenticação do Kerberos para verificar usuários e serviços.

## Opções de segurança

O seguro de NFS é compatível com as seguintes opções de segurança:

- krb5: autenticação Kerberos
- krb5i: autenticação Kerberos e integridade de dados com a adição de uma assinatura para cada pacote NFS transmitido pela rede
- krb5p: autenticação Kerberos, integridade de dados e privacidade de dados criptografando os dados antes de enviá-los pela rede

  A criptografia de dados exige mais recursos para o processamento do sistema e pode levar a um desempenho mais lento.

Em um ambiente seguro de NFS, o acesso de usuário para file systems NFS é concedido com base nos nomes principais do Kerberos. No entanto, o controle de acesso a compartilhamentos em um file system é baseado em GID e UID do UNIX ou em ACLs.

**NOTA:** O NFS seguro é compatível com credenciais de NFS com mais de 16 grupos, o que equivale à opção de credenciais estendidas do UNIX.

## Configuração de NFS seguro

Se você estiver implementando o NFS seguro, configure o seguinte:

- Deve existir pelo menos um servidor NTP no equipamento PowerStore para que a data e a hora sejam sincronizadas. É recomendável configurar pelo menos dois servidores NTP por domínio para evitar um ponto único de falha.
- Um serviço de diretório UNIX (UDS, UNIX Directory Service)
- Um ou mais servidores DNS
- É preciso adicionar um realm personalizado ou do AD para a autenticação Kerberos
- É preciso carregar um arquivo keytab para o servidor NAS ao usar um realm personalizado em uma configuração Kerberos

# Considerações sobre planejamento

Analise as informações a seguir antes de configurar exportações NFS:

O suporte ao armazenamento em arquivo só está disponível com equipamentos Modelo PowerStore T e PowerStore modelo Q.

## Redes do servidor NAS

A criação de VLANs de rede e endereços IP é opcional para servidores NAS. Se você planeja criar uma VLAN para servidores NAS, ela não poderá ser compartilhada com as redes de armazenamento ou de gerenciamento do Modelo PowerStore T e do PowerStore modelo Q. Além disso, reserve os recursos de rede e configure a rede no switch junto com o administrador de rede. Consulte os detalhes em *Guia de sistema de rede do PowerStore T e Q para Storage Services*.

## Dimensionamento

No PowerStoreOS 3.5 e posterior, há um limite compartilhado para volumes de file systems e vVols. O número total de objetos é determinado de acordo com o limite mais alto dos três tipos de objeto.

Para visualizar o limite de file systems por plataforma, consulte a *Matriz de suporte simples do PowerStore da Dell Technologies* na página da documentação do PowerStore.

## Requisitos de implementação

Os serviços NAS só estão disponíveis em equipamentos Modelo PowerStore T e PowerStore modelo Q.

Você precisa ter escolhido a opção **Unificado** durante a configuração inicial dos equipamentos Modelo PowerStore T e PowerStore modelo Q. Se você escolheu **Otimizado para bloco** durante a execução do Initial Configuration Wizard, os serviços NAS não foram instalados. Para instalar os serviços de NAS, um representante de suporte técnico deve reinicializar o sistema. A reinicialização do sistema:

- Configura o equipamento de volta para o estado de fábrica.
- Remove toda a configuração feita no sistema por meio do **Initial Configuration Wizard**.
- Remove qualquer configuração realizada no PowerStore após a configuração inicial.

## Mais considerações

Para criar um servidor NAS, é preciso que os dois nós no equipamento estejam em funcionamento. Se um dos nós estiver inativo no equipamento, a criação do servidor NAS falhará.

## Criar a interface de rede para o tráfego NAS

É possível configurar uma rede NAS usando vínculos do protocolo de controle de agregação de links (LACP) ou criando uma rede fail-safe para o tráfego de NAS.

## Criar vínculos LACP para o tráfego NAS

Se os switches estiverem configurados com MC-LAG, use a vinculação de rede criando um grupo agregado de links (LAG) para o tráfego NAS.

Quando os switches de topo de rack (ToR) são configurados com uma interconexão MC-LAG, é recomendável configurar a interface NAS em vínculos LACP usando grupos de agregação de links (LAG). A vinculação LACP é um processo em que duas ou mais interfaces de rede são combinadas a uma única interface. O uso dessa vinculação proporciona melhorias de desempenho e redundância, aumentando o throughput da rede e a largura de banda. Se uma das interfaces combinadas estiver inativa, as outras interfaces serão usadas para manter uma conexão estável.

1. Selecione **Hardware** > **[Equipamento]** > **Portas**.
2. Na lista de portas, selecione de duas a quatro portas da mesma velocidade no nó em que você deseja agregar para que o vínculo do protocolo de controle de agregação de links (LACP) atenda ao tráfego NAS.

   **NOTA:** A configuração é simétrica em todo o par do nó.

3. Selecione **Agregação de links** > **Agregar links**.
4. Como opção, especifique uma descrição para o vínculo.
5. Selecione **Agregar**.
6. Percorra a lista de portas e localize o nome do vínculo gerado.

   **NOTA:** Quando criar o servidor NAS, você precisará selecionar o nome do vínculo.

## Criar uma rede à prova de falhas

Uma rede à prova de falhas deverá ser criada quando os switches topo de rack (ToR) não tiverem sido configurados com uma interconexão MC-Lag. Uma FSN estende o failover de link para a rede fornecendo redundância no nível do switch. Uma FSN pode ser configurada em uma porta, em uma agregação de links ou qualquer combinação das duas.

1. Selecione **Hardware** > **[Equipamento]** > **Portas**.
2. Se você planeja usar links agregados para a FSN, primeiro crie os grupos de agregação de links. Para obter mais detalhes, consulte Criar vínculos LACP para tráfego NAS.
3. Na lista, selecione duas portas, duas agregações de links ou uma combinação de uma porta e um grupo de agregação de links que você deseja usar para a FSN no nó A e selecione **FSN** > **Criar FSN**.
4. No painel **Criar FSN**, selecione quais portas ou agregação de links usar como a rede principal (ativa).

   **NOTA:** Não será possível modificar a porta principal depois de usá-la para criar um servidor NAS.

5. Se quiser, você pode adicionar uma descrição da rede à prova de falhas.
6. Clique em **Criar**.

   O PowerStore Manager automaticamente cria um nome para a rede à prova de falhas no seguinte formato: "BaseEnclosure-<Node>-fsn<nextLACPbondcreated>"

   - BaseEnclosure é constante.
   - Node é o nó exibido na lista **Node-Module-Name**.
   - nextLACPbondcreated é um valor numérico determinado pela ordem em que o vínculo foi criado no PowerStore Manager, começando com zero para o primeiro vínculo criado.

   A primeira FSN criada no PowerStore Manager no nó A seria chamada de BaseEnclosure-NodeA-FSN0.

   A mesma FSN é configurada no nó oposto. Por exemplo, se você configurou a FSN no nó A, a mesma FSN seria configurada no nó B.

7. Crie um servidor NAS com a rede à prova de falhas.

   A rede à prova de falhas é aplicada ao servidor NAS durante a criação dele no PowerStore Manager. Consulte Criar um servidor NAS para seu file system NFS.

# Criando exportações NFS

Faça o seguinte para poder criar exportações NFS no PowerStore:

1. Criar servidores NAS com protocolo NFS
2. Criar um file system para exportações NFS

# Recursos de documentação

Consulte o seguinte para obter mais informações:

**Tabela 1. Recursos de documentação**

| Documento | Descrição | Local |
|---|---|---|
| *Guia de sistema de rede do PowerStore T e Q para Storage Services* | O documento fornece informações sobre planejamento e configuração de rede. | dell.com/powerstoredocs |
| *Guia de configuração de SMB do PowerStore* | O documento fornece as informações necessárias para configurar compartilhamentos SMB com o PowerStore Manager. | |
| *White paper de recursos de arquivo do PowerStore* | O documento aborda os recursos, a funcionalidade e os protocolos compatíveis com a arquitetura de arquivo do Dell PowerStore. | |
| *Ajuda on-line do PowerStore* | A ajuda online contém informações contextuais da página aberta no PowerStore Manager. | Incorporado ao PowerStore Manager |

# 2

# Criar servidores NAS

Este tópico contém as seguintes informações:

**Tópicos:**



## Visão geral da configuração de servidores NAS

Para que você possa provisionar o armazenamento de arquivos no sistema de armazenamento, um servidor NAS deve estar em execução no sistema. Um servidor NAS é um servidor de arquivos que usa o protocolo SMB, o protocolo NFS ou ambos para compartilhar dados com hosts da rede. Ele também cataloga, organiza e otimiza as operações de leitura e gravação para os file systems associados.

Este documento descreve como configurar um servidor NAS com o protocolo NFS, onde é possível criar file systems com exportações NFS.

## Criar um servidor NAS para file systems NFS

Crie servidores NAS antes de criar file systems.

Tenha as informações da rede NAS em mãos.

1. Selecione **Armazenamento** > **Servidores NAS**.
2. Selecione **Criar**.
3. Continue trabalhando no assistente **Create NAS Server**.

| Tela Wizard | Descrição |
|---|---|
| Detalhes | • Nome do servidor NAS<br>• Descrição do servidor NAS<br>• Interface de rede — Selecione um grupo de agregação de links ou uma rede à prova de falhas (consulte Criar a interface de rede para tráfego NAS).<br>**NOTA:** Se você selecionar uma rede à prova de falhas (FSN), não será possível modificar a rede primária após um servidor NAS ter sido configurado usando a FSN.<br>• Informações de rede - endereço IP, máscara de sub-rede, gateway e ID da VLAN<br>**NOTA:** Não é possível reutilizar VLANs que estão sendo usadas para as redes de gerenciamento e armazenamento.<br>• Enable Packet Reflect - As respostas do servidor são enviadas de volta para o host ou roteador de origem, independentemente do endereço IP de destino, evitando pesquisas de roteamento.<br>**NOTA:** Essa opção não é aplicada para comunicação iniciada pelo servidor NAS. |
| Protocolos de compartilhamento | **Selecione o protocolo de compartilhamento**<br>Selecione NFSv3, NFSv4 ou ambos. |

| Tela Wizard | Descrição |
| --- | --- |
| | **NOTA:** Se você selecionar SMB e um protocolo NFS, ativará automaticamente o servidor NAS para oferecer suporte a vários protocolos. Para obter detalhes sobre o compartilhamento de arquivos *multiprotocolo, consulte o Guia de configuração de compartilhamento de arquivos multiprotocolo do Dell PowerStore* na PowerStore página Documentação.<br><br>**Unix Directory Services** (Naming Services)<br><br>Você pode configurar os serviços de nomenclatura com uma combinação de arquivos locais e NIS ou LDAP.<br><br>Consulte as seções a seguir para configuração:<br>• Usando arquivos locais<br>• Com NIS<br>• Com LDAP<br><br>Você pode optar por habilitar o NFS seguro aqui.<br><br>O NFS seguro exige o seguinte:<br>• Deve existir pelo menos um servidor NTP no equipamento PowerStore para que a data e a hora sejam sincronizadas. É recomendável configurar pelo menos dois servidores NTP por domínio para evitar um ponto único de falha.<br>• Um serviço de diretório UNIX (UDS, UNIX Directory Service)<br>• Um ou mais servidores DNS<br>• É preciso adicionar um realm personalizado ou do AD para a autenticação Kerberos<br>• É preciso carregar um arquivo keytab para o servidor NAS ao usar um realm personalizado em uma configuração Kerberos<br><br>**DNS**<br><br>As informações do servidor DNS são obrigatórias ao:<br>• Ingressar em um domínio do AD, mas opcional para um servidor NAS independente.<br>• Configuração de NFS seguro<br><br>DNS também pode ser usado para resolver hosts definidos em listas de acesso de exportações de NFS. |
| Política de proteção | Também é possível selecionar uma política de proteção na lista. |
| Política de QoS de arquivo | Também é possível selecionar uma política de QoS na lista. |
| Resumo | Analise o conteúdo e selecione **Previous** para voltar e fazer quaisquer correções. |

4. Selecione **Create NAS Server** para criar o servidor NAS.
   A janela **Status** será aberta e você será redirecionado à página **NAS Servers** assim que o servidor estiver listado na página.

Depois de criar o servidor NAS para NFS, você pode continuar a definir as configurações do servidor.

Se você habilitar o NFS seguro, deverá continuar a configurar o Kerberos.

Selecione o servidor NAS para continuar a configurar ou editar as configurações do servidor NAS.

**NOTA:** Quando há uma conexão com sistema remoto, pode levar até 15 minutos para as alterações de configuração do servidor NAS serem refletidas no servidor NAS remoto.

# Configurar serviços de nomenclatura do servidor NAS

Você pode configurar ou modificar os serviços de nomenclatura de um servidor NAS.

Os serviços de nomenclatura incluem configurar um ou mais dos seguintes:

- DNS
- NIS para Unix Directory Services (UDS)
- LDAP para UDS
- Arquivos locais

# Configurar DNS

Você pode desabilitar o DNS ou habilitar e configurar um servidor NAS para usar DNS.

O DNS também pode ser usado para resolver hosts definidos em listas de acesso da exportação NFS.

O DNS é necessário para:

- NFS seguro
- Ingressar em um domínio do AD.

Não é possível desabilitar o DNS para servidores NAS configurados com:

- Compartilhamento de arquivos multiprotocolo
- Compartilhamento de arquivos SMB associado a um AD (Active Directory)
- NFS seguro

1. Selecione **Storage** > **NAS Servers** > **[nas server]** > **DNS**.
2. Habilite ou desabilite o DNS. Se você habilitou o DNS, especifique as informações do servidor DNS.

# Configurar UNIX Directory Service do servidor NAS para NIS

Você pode configurar o UNIX Directory Service (UDS) do servidor NAS para NIS.

1. Selecione **Storage** > **NAS Servers** > **[nas server]** > **Naming Services** > **UDS**.
2. Se a opção **Disabled** estiver ativada, deslize o botão para mudar para **Enabled**.
3. No menu suspenso **Unix Directory Service**, selecione **NIS**.
4. Especifique um **Domain** NIS e adicione **Addresses** IP para os servidores NIS.
5. Selecione **Aplicar**.

Para solucionar os problemas de configuração de um UDS usando NIS, certifique-se de que os endereços IP informados para o servidor e o domínio do servidor NIS estejam corretos.

# Configurar UNIX Directory Service do servidor NAS usando LDAP

Você pode configurar o UNIX Directory Service (UDS) do servidor NAS usando LDAP.

O LDAP deve aderir aos esquemas IDMU, RFC2307 ou RFC2307bis. Alguns exemplos incluem LDAP AD com IDMU, iPlanet e OpenLDAP. O servidor LDAP deve ser configurado adequadamente para fornecer UIDs a cada usuário. Por exemplo, no IDMU, o administrador deve acessar as propriedades de cada usuário e adicionar um UID à guia Atributos do UNIX.

Você pode configurar o LDAP para usar a autenticação Kerberos anônima e simples. Se estiver usando a autenticação Kerberos, você deverá configurar o seguinte para poder continuar configurando o LDAP com Kerberos:

1. No card **Naming Services**, configure o servidor DNS usado para associar e desassociar um servidor Kerberos a um realm.
2. No card **Security**, adicione o realm Kerberos.
1. Selecione **Storage** > **NAS Servers** > **[nas server]** > **Naming Services** > **UDS**.
2. Se a opção **Disabled** estiver ativada, deslize o botão para mudar para **Enabled**.
3. No menu suspenso **Unix Directory Service**, selecione **LDAP.**
4. Deixe o padrão ou digite outro número de porta em **Port Number**.

   **NOTA:** Por padrão, o LDAP usa a porta 389, e o LDAP sobre SSL (LDAPS) usa a porta 636.

5. Adicione os endereços IP/FQDNs para os servidores LDAP.

   O servidor NAS pode ser configurado para usar a detecção de serviço DNS para obter os endereços IP de servidor LDAP automaticamente.

   **NOTA:** Para que esse processo de detecção funcione, o servidor DNS deve conter indicadores para os servidores LDAP, e os servidores LDAP devem compartilhar as mesmas configurações de autenticação.

6. Configure a autenticação LDAP conforme descrito na seguinte tabela:

| Opção | Descrição |
|---|---|
| Anônimo | Especifique o DN base e o DN de perfil do servidor iPlanet/OpenLDAP. |
| Simples | Especifique o seguinte:<br>● Se estiver usando o AD, LDAP/IDMU:<br>○ DN de ligação no formato de notação de LDAP; por exemplo, **cn=administrator,cn=users,dc=svt,dc=lab,dc=com**.<br>○ DN base, no formato X.509 (por exemplo, **dc=svt,dc=lab,dc=com**).<br>○ DN do perfil.<br>● Se estiver usando o servidor iPlanet/OpenLDAP:<br>○ DN de ligação no formato de notação de LDAP; por exemplo, **cn=administrator,cn=users,dc=svt,dc=lab,dc=com**.<br>○ Password<br>○ DN base. Por exemplo, se estiver usando **svt.lab.com**, o DN de base seria **DC=svt,DC=lab,DC=com**.<br>○ DN de perfil (opcional) — Para o servidor iPlanet/OpenLDAP. |
| Kerberos | Configure um realm personalizado para apontar para qualquer tipo de realm Kerberos (Windows, MIT ou Heidmal). Com essa opção, o servidor NAS usa o realm Kerberos personalizado definido na subseção Kerberos da guia **Security** do servidor NAS.<br>**NOTA:** Se você usar NFS seguro com um realm personalizado, deverá fazer upload de um arquivo keytab. |

7. Selecione **Retrieve Current Schema** para fazer download do arquivo ldap.conf.
8. Edite e salve o `ldap.conf` arquivo.
9. Selecione **Upload New Schema** para carregar o arquivo atualizado `ldap.conf` .
10. Como opção, habilite LDAP Secure (Use SSL) e carregue o certificado da CA.

Para solucionar os problemas de configuração de um UDS usando LDAP, certifique-se de que:

- A configuração LDAP segue um dos esquemas compatíveis, conforme descrito anteriormente.
- Os contêineres especificados no arquivo `ldap.conf` apontam para contêineres válidos e existentes.
- Cada usuário do LDAP é configurado com um UID exclusivo.

## Configurar o servidor NAS para usar arquivos locais para serviços de nomenclatura

Você pode configurar os serviços de nomenclatura para usar arquivos locais.

- Os arquivos locais podem ser usados no lugar de, ou também com, serviços de diretório DNS, LDAP e NIS.
- Se você configurar os arquivos locais com um UDS (UNIX Directory Service), o sistema de armazenamento consultará os arquivos locais primeiro.
- Depois de terminar de criar o servidor NFS, você pode voltar e carregar mais arquivos locais.
- Uma vez criado o servidor NAS, habilite os arquivos locais conforme descrito nas seguintes etapas:

1. Selecione **Storage** > **NAS Servers** > **[nas server]** > **Naming Services** > **Local Files**.
2. Para cada tipo de arquivo local, selecione a seta para baixo para fazer download do arquivo atual. Se não houver nenhum arquivo no sistema de armazenamento, o sistema fará download um modelo de arquivo.
3. Atualize o arquivo com as informações do sistema.

   Para usar os arquivos locais para acesso a FTP, o arquivo `passwd` deve conter uma senha criptografada para os usuários. Essa senha é usada para acesso apenas ao FTP. O arquivo `passwd` usa os mesmos formato e sintaxe de um sistema UNIX padrão, por isso você pode aplicar a senha para gerar o arquivo `passwd` local. Em um sistema UNIX, use `useradd` para adicionar um usuário e `passwd` para definir a senha para esse usuário. Em seguida, copie a senha com hash do arquivo `/etc/shadow`, adicione-a ao segundo campo no arquivo `/etc/passwd` e carregue o arquivo `/etc/passwd` no servidor NAS.
4. Salve o arquivo atualizado em sua máquina local.
5. Selecione **Upload Local Files**, navegue até a localização do arquivo editado e selecione o arquivo a ser carregado.
6. Repita a operação para cada tipo de arquivo.

Para solucionar os problemas de configuração de arquivos locais, certifique-se de que:

- O arquivo é criado com a sintaxe adequada. (Seis pontos-e-vírgulas são necessários para cada linha). Consulte o modelo para obter mais detalhes sobre a sintaxe e os exemplos.
- Cada usuário tem um nome e um ID exclusivos.

# Configurar protocolos de compartilhamento do servidor NAS

Você pode configurar ou modificar os protocolos de compartilhamento configurados para um servidor NAS.

O processo de configurar protocolos de compartilhamento para NFS inclui a configuração de uma ou mais das seguintes opções:

- Servidor NFS
- FTP

## Configurar o servidor NFS

Configure o servidor NAS somente para sistemas UNIX ou modifique as configurações do servidor NFS.

O DNS e o NTP devem ser configurados antes de configurar um servidor NFS seguro.

1. Selecione a guia **Storage** > **NAS Servers** > **[nas server]** > **Sharing Protocols** > **NFS Server**.
2. Ative a opção **Linix/UNIX shares** para definir o servidor NAS para suporte do UNIX.
3. Ative **NFSv3**, **NFSv4** ou ambos.
4. Como opção, desative ou ative o NFS seguro.
   As credenciais estendidas do UNIX também são ativadas.
5. **Enable or disable Extend Unix credentials**.

   **NOTA:** O NFS seguro é compatível com credenciais de NFS com mais de 16 grupos, o que equivale à opção de credenciais estendidas do UNIX.

   - Se esse campo estiver selecionado, o servidor NAS usará o ID de usuário (UID) para obter o ID de grupo principal (GID) e todos os GIDs do grupo ao qual ele pertence. O servidor NAS obtém os GIDs do arquivo de senha local ou UDS.
   - Se esse campo ficar em branco, as credenciais do UNIX de solicitação NFS serão extraídas diretamente das informações de rede contidas na estrutura. Esse método tem o melhor desempenho, mas ele está limitado a incluir somente até 16 GIDs de grupos.
6. No campo **Credential Cache Retention**, digite o tempo (em minutos) durante o qual as credenciais de acesso serão mantidas no cache.
7. Clique em **Apply** para aplicar as alterações.

## Configurar o protocolo de compartilhamento FTP ou SFTP

Você pode definir as configurações de FTP ou FTP sobre SSH (SFTP) apenas para um servidor NAS existente.

Não há suporte para o modo FTP passivo.

O acesso ao FTP pode ser autenticado usando os mesmos métodos que o NFS. Uma vez concluída a autenticação, o acesso é o mesmo que NFS para fins de segurança e permissões. Se o formato for algo diferente de `user@domain` ou `domain\user`, será usada a autenticação NFS. A autenticação NFS usa arquivos locais, LDAP, NIS (Network Information Service, Serviço de informação da rede), ou os arquivos locais com LDAP ou NIS.

Para usar os arquivos locais para acesso a NFS e FTP, o arquivo `passwd` deve conter uma senha criptografada para os usuários. Essa senha é usada para acesso apenas ao FTP. O arquivo `passwd` usa o mesmo formato e a mesma sintaxe de um sistema Unix padrão, e você pode aproveitar isso para gerar o arquivo `passwd` local. Em um sistema Unix, use `useradd` para adicionar um usuário e `passwd` para definir a senha desse usuário. Em seguida, copie a senha com hash do arquivo `/etc/shadow`, adicione-a ao segundo campo no arquivo `/etc/passwd` e carregue o arquivo `/etc/passwd` no servidor NAS. Consulte Configurar o servidor NAS para usar arquivos locais em serviços de nomenclatura para obter detalhes sobre o carregamento do arquivo `/etc/passwd`.

1. Selecione a guia **Storage** > **NAS Servers** > **[nas server]** > **Sharing Protocols** > **FTP**.
2. Em **FTP**, se a opção Disabled estiver ativada, deslize o botão até **Enable**.
3. Se preferir, habilite também o FTP SSH. Em **SFTP**, se a opção Disabled estiver ativada, deslize o botão até **Enable**.
4. Em **FTP/SFTP Server Access**, selecione o tipo de usuários autenticados que têm acesso aos arquivos.

5. Como alternativa, veja as opções em **Home Directory and Audit**.
   - Marque ou desmarque as **Home directory restrictions**. Se esta opção estiver desativada, informe o **Default home directory**.
   - Selecione ou desmarque a opção **Enable FTP/SFTP Auditing**. Se marcada, digite a localização do diretório onde os arquivos de auditoria deverão ser salvos e o tamanho máximo permitido para eles.
6. Se preferir, selecione **Show Messages**, digite uma mensagem de boas-vindas padrão em **Welcome message** e a mensagem do dia em **Message of the day**.
7. Como opção, selecione **Show Access Control List** para conceder ou negar acesso a **Filtered Users**, **Filtered Groups** e **Filtered Hosts**.
8. Clique em **Aplicar**.

# Configurar Kerberos para segurança do servidor NAS

Você pode configurar o servidor NAS com Kerberos.

O Kerberos é um serviço de autenticação distribuído projetado para proporcionar autenticação sólida com criptografia de chave secreta. Ele funciona com base em "tíquetes" que permitem que nós se comuniquem em uma rede não segura para provar sua identidade de maneira segura. Quando configurados para atuarem como um servidor NFS seguro, o servidor NAS usa a estrutura de segurança RPCSEC_GSS e o protocolo de autenticação do Kerberos para verificar usuários e serviços.

Se o servidor NAS tiver sido configurado apenas com NFS e você estiver configurando NFS seguro ou LDAP com Kerberos, deverá configurar o Kerberos com um realm personalizado antes de configurar a segurança no PowerStore.

Se o servidor NAS tiver sido configurado com os protocolos NFS e SMB, você terá a opção de usar o Kerberos que é herdado com o AD, desde que o servidor SMB associado ao domínio exista no servidor NAS.

O sistema de armazenamento deve ser configurado com um servidor NTP. Kerberos conta com a sincronização de hora correta entre o Key Distribution Center, servidores e o client na rede.

## Configurando o Kerberos para NFS seguro

Se você estiver configurando o Kerberos para NFS seguro, esteja ciente das seguintes opções:

- Caso esteja configurando o servidor NAS somente para NFS, configure-o com um realm personalizado. Se tiver configurado o servidor NAS com NFS e SMB, use o realm personalizado ou do AD.
- Usar LDAPS ou LDAP com Kerberos é recomendado para maior segurança.
- Um servidor DNS deve ser configurado no nível do servidor NAS. Todos os membros do realm Kerberos, inclusive o Key Distribution Center, o servidor NFS e clients NFS, devem ser registrados no servidor DNS.
- O nome de domínio totalmente qualificado (FQDN) do servidor NAS e o FQDN do nome de host do client NFS devem estar registrados no servidor DNS. Clients e servidores devem ser capazes de resolver qualquer membro dos FQDNs do realm Kerberos para um endereço IP.
- A parte do nome de domínio completo do SPN do client NFS deve estar registrada no servidor DNS.
- É preciso carregar um arquivo keytab para o servidor NAS ao configurar o NFS seguro.

# Criar um realm personalizado para Kerberos

Você pode configurar um realm personalizado para uso com Kerberos.

Um realm Kerberos personalizado permite configurar qualquer tipo de KDC (MIT/Heidmal ou AD). Use esse método quando você não tiver um domínio de servidor SMB configurado no servidor NAS ou se você quiser usar um realm Kerberos diferente daquele configurado para o servidor SMB.

## Criar um realm personalizado para o servidor NFS puro

Para usar um KDC baseado em UNIX, siga estas etapas antes de configurar o Kerberos no PowerStore. As etapas pressupõem que você quer usar myrealm no realm Kerberos linux.dellemc.com como o nome de host do servidor NFS.

1. Execute a ferramenta `kadmin.local`.
2. Crie os principais e as chaves:

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

e/ou

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

3. Coloque a chave do principal no arquivo keytab em myrealm.linux.dellemc.fr:

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

### Criar um realm personalizado para o servidor NAS multiprotocolo (NFS e SMB)

Para usar um KDC baseado em Windows sem usar a conta do servidor SMB no servidor NAS, siga estas etapas antes de configurar o Kerberos no PowerStore. As etapas pressupõem que você quer usar myrealm.windows.dellemc.com como o FQDN para o servidor NFS.

1. Crie a conta myrealm para o servidor NAS no Active Directory (AD) do domínio do Windows windows.dellemc.com.
2. Registre o SPN de serviço na conta do computador que você criou:

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

3. Verificar se o SPN foi criado.

```
C:\setspn myrealm
```

4. Gere um arquivo keytab para o SPN:

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

## Configurar a segurança Kerberos para o servidor NAS

Você pode configurar o servidor NAS com segurança Kerberos.

Se você for configurar a segurança para NFS, o DNS e o UDS deverão ser configurados para o servidor NAS e todos os membros do realm Kerberos deverão estar registrados no servidor DNS.

Se estiver usando um servidor NAS configurado para SMB e NFS, inclua o servidor SMB no domínio do AD.

1. Selecione **Storage** > **NAS Servers** > **[nas server]** > **Security** > **Kerberos**.
2. Se a opção Disabled estiver ativada, deslize o botão para mudar para **Enabled**.
3. Digite o nome do **Realm**.
4. Digite o **Kerberos IP Address** e clique em **Add**.
5. Digite a porta TCP para Kerberos a ser usada. 88 é a porta padrão.
6. Clique em **Apply**.

Se você optar por mudar de um realm do AD para um realm personalizado depois que o servidor NAS for criado com sucesso com NFS seguro, não poderá montar nenhuma exportação NFS até realizar as seguintes operações:

1. Criar um arquivo keytab.
2. Remover o realm do AD do servidor NAS.
3. Digitar o nome de usuário e a senha para o servidor do AD.
4. Digitar o realm personalizado.
5. Carregar o arquivo keytab.

# Excluir um servidor NAS

Exclua um servidor NAS selecionando-o e confirmando a exclusão, garantindo que nenhum file system ou política de proteção esteja associado a ele.

- Certifique-se de que não haja nenhum file system no servidor.
- Certifique-se de que não há políticas de proteção associadas ao servidor.

1. Selecione **Storage** > **NAS Servers** para abrir a lista NAS Servers.

2. Na lista, marque a caixa de seleção ao lado do servidor que você deseja excluir.
3. Selecione **More Actions** > **Delete**.

   **NOTA:** Se o servidor NAS selecionado contiver file systems ou estiver associado a uma política de proteção, a opção Excluir estará indisponível. Passar o mouse sobre a opção Excluir exibe o motivo da inativação.

4. Selecione **Excluir** para confirmar.

O servidor NAS selecionado é excluído.

# 3

# Configurar exportações NFS

Este tópico contém as seguintes informações:

**Tópicos:**



## Visão geral dos file systems e das exportações NFS

Ao criar file systems e exportações NFS, é útil observar os seguintes aspectos:

- Antes de criar um file system, é preciso configurar um servidor NAS para dar suporte ao protocolo NFS.
- Você pode optar por adicionar Exportações NFS na primeira vez que criar o file system ou pode adicionar Exportações NFS a um file system depois de o criar.

## Criar um file system para exportações NFS

Você pode criar um file system para exportações NFS.

Certifique-se de que exista um servidor NAS configurado para oferecer suporte ao protocolo NFS.

1. Selecione **Storage** > **File Systems**.
2. Clique em **Create**.
   O assistente **Create File System** é iniciado.
3. Selecione **Geral** ou **File system VMware** como o tipo de file system.

   **NOTA:** O file system VMware é um file system do PowerStore otimizado para VMware e usado para cargas de trabalho VMware. Essa opção deve ser selecionada somente para datastores VMware NFS. Para todos os outros file systems, selecione **Geral**.

4. Selecione um servidor NAS habilitado para NFS para o file system.
5. Especifique os detalhes do file system, inclusive o nome e o tamanho do file system, o tamanho mínimo é de 3 GB, o tamanho máximo é de 256 TB.

   **NOTA:** Todos os file systems thin, independentemente do tamanho, têm 1,5 GB reservado para metadados após a criação. Por exemplo, depois de criar um file system dinâmico de 100 GB, os modelos Modelo PowerStore T e PowerStore Q exibem uma utilização de 1,5 GB. Quando o file system é montado em um host, ele mostra 98,5 GB de capacidade útil. Isso ocorre porque o espaço de metadados é reservado a partir da capacidade utilizável do file system.

6. Como opção, selecione o tipo de retenção de arquivos (disponível apenas para file systems gerais):
   - Empresarial (FLR-E) — protege o conteúdo contra alterações feitas por usuários por meio de NFS e FTP. Um administrador pode excluir um file system FLR-E que contém arquivos protegidos.
   - Compliance (FLR-C) — Protege o conteúdo contra alterações feitas por usuários e administradores e está em conformidade com os requisitos da regra 17a-4(f) da SEC. Um file system FLR-C só pode ser excluído quando não contém arquivos protegidos.

   **NOTA:** O estado FLR e o tipo de retenção de arquivos são definidos na criação do file system e não podem ser modificados.

   Defina os períodos de retenção:
   - Mínimo — Especifica o período mais curto durante o qual os arquivos podem ficar bloqueados (o valor padrão é 1 dia).
   - Padrão — Usado quando um arquivo é bloqueado e nenhum período de retenção foi especificado.
   - Máximo — Especifica o período mais longo durante o qual os arquivos podem ficar bloqueados.
7. Como opção, configure a exportação inicial do file system.

**NOTA:** Você pode adicionar exportações NFS ao file system posteriormente.

8. Se você configurou a exportação inicial, configure o acesso ao host.

| Opção | Descrição |
|---|---|
| Minimum Security | Selecione **Sys** para permitir que usuários com NFS seguros ou não seguros montem uma exportação NFS no file system. Se você não estiver configurando NFS seguro, selecione esta opção.<br>Caso você esteja criando um file system com NFS seguro, escolha uma das seguintes opções:<br>• **Kerberos** para permitir qualquer tipo de segurança Kerberos para autenticação (krb5/krb5i/krb5p).<br>• **Kerberos com integridade** a fim de permitir Kerberos com integridade e Kerberos com segurança de criptografia para autenticação de usuário (krb5i/krb5p).<br>• **Kerberos com criptografia** a fim de permitir apenas Kerberos com segurança de criptografia para autenticação de usuário (krb5p). |
| Default Access | O tipo de acesso que é aplicado aos hosts por padrão. Como opção, você pode escolher outro tipo de acesso ao host ao adicionar hosts individuais. As opções incluem:<br>• **Sem acesso** — Nenhum acesso é permitido ao recurso de armazenamento ou compartilhamento.<br>• **Leitura/gravação** — os hosts têm permissão para ler e gravar no datastore NFS ou no compartilhamento.<br>• **Somente leitura** — os hosts têm permissão para visualizar o conteúdo do recurso de armazenamento ou do compartilhamento, mas não para gravar neles.<br>**NOTA:** Os hosts do ESXi devem ter acesso de **Leitura/gravação** para montar um datastore NFS usando o NFSv4 com a autenticação **Proprietário Kerberos NFS**.<br>• **Leitura/gravação, permitir raiz** — os hosts têm permissão para ler e gravar no recurso de armazenamento ou no compartilhamento e para conceder permissões de acesso revogadas (por exemplo, permissão para ler, modificar e executar arquivos e diretórios específicos) para outras contas de log-in que acessam o armazenamento. O root do client NFS tem acesso de root ao compartilhamento.<br>**NOTA:** A menos que os hosts sejam parte de uma configuração de cluster compatível, evite a concessão de acesso de leitura/gravação a mais de um host.<br>**NOTA:** Os hosts do ESXi devem ter acesso de **Leitura/gravação, permitir root** para montar um datastore NFS usando o NFSv4 com a autenticação Proprietário NFS:root.<br>• **Read-Only, allow Root** — Os hosts têm permissão para visualizar o conteúdo do compartilhamento, mas não para gravar nele. O root do client NFS tem acesso de root ao compartilhamento. |
| Add Host | Informe hosts individualmente ou adicione hosts carregando um arquivo CSV devidamente formatado. É possível fazer download do arquivo CSV primeiro para obter um modelo. Para fazer download, editar e usar um modelo de arquivo CSV:<br>a. Clique no ícone **Export Hosts**.<br>b. Atualize o arquivo CSV com os hosts e os tipos de acesso que você quer importar.<br>c. Salve o arquivo CSV em sua máquina local.<br>d. Clique em **Import CSV file**.<br>e. Localize o arquivo CSV e clique em **Open** na janela do Explorador de Arquivos da Microsoft.<br>Os hosts do arquivo CSV são exibidos em **Import Host List** com o **Access Type** definido no arquivo CVS. |

9. Com opção, adicione uma política de proteção ao file system.
   Se você estiver adicionando uma política de proteção ao file system, a política deverá ter sido criada antes de criar o file system. A política de proteção selecionada pode incluir regras de snapshot e de replicação.
10. Como opção, adicione uma política de QoS ao file system.

**NOTA:** Se a política selecionada definir uma largura de banda que exceda a largura de banda máxima definida para o servidor NAS, a largura de banda efetiva será a largura de banda máxima do servidor.

11. Analise o resumo e clique em **Create File System**.
    O file system é adicionado à guia **File System**. Se, ao mesmo tempo, você criou uma exportação, ela é exibida na guia **Exportação NFS**.

# Criar uma exportação NFS

É possível criar uma exportação NFS em um file system.

1. Selecione a guia **Storage** > **File Systems** > **NFS Export**.
2. Clique em **Create**.
   O assistente **Create NFS Export** é iniciado.
3. Especifique as informações solicitadas e observe o seguinte:
   - Se você quiser criar uma exportação com base em um snapshot, será necessário criar os snapshots antes de criar a exportação NFS.
   - **Local Path** deve corresponder a um nome de pasta existente dentro do file system criado no lado do host.
   - O valor especificado no campo **Detalhes da exportação NFS**, **Nome**, junto com o IP do servidor NAS, constitui o caminho da exportação.

     **NOTA:** Também é possível montar a exportação usando o IP e o caminho local do servidor NAS.

   - Os nomes das exportações NFS devem ser exclusivos no nível do servidor NAS por protocolo. No entanto, você pode especificar o mesmo nome para um compartilhamento SMB e para exportações NFS.
4. Depois de aprovar as configurações, clique em **Create NFS Export**.
   A exportação NFS será mostrada na página de **NFS Export**.

# Retenção em nível de arquivo

A FLR (File-Level Retention, retenção em nível de arquivo) permite impedir modificações ou a exclusão de arquivos por um período de retenção especificado. A proteção de um file system usando FLR permite criar um conjunto permanente e inalterável de arquivos e diretórios. A FLR garante a acessibilidade e a integridade dos dados, simplifica os procedimentos de arquivamento para administradores e melhora a flexibilidade do gerenciamento de armazenamento.

Há dois tipos de retenção em nível de arquivo:

- Enterprise (FLR-E) — Protege os dados contra alterações feitas por usuários e administradores de armazenamento usando SMB, NFS e FTP. Um administrador pode excluir um file system FLR-E que inclui arquivos bloqueados.
- Compliance (FLR-C) — Protege os dados contra alterações feitas por usuários e administradores de armazenamento usando SMB, NFS e FTP. Um administrador não pode excluir um file system FLR-C que inclui arquivos bloqueados. A FLR-C está em conformidade com a regra 17a-4(f) da SEC.

Aplicam-se as seguintes restrições:

- A FLR está disponível no sistema unificado PowerStore 3.0 ou posterior.
- A FLR não é compatível com file systems VMware.
- A ativação da FLR para um sistema de arquivos e o tipo de FLR são definidos no momento da criação do sistema de arquivos e não podem ser modificados.
- A FLR-C não aceita restauração a partir de um snapshot.
- Ao atualizar usando um snapshot, os dois file systems devem ser do mesmo tipo de FLR.
- Ao replicar um file system, os file systems de origem e destino devem ser do mesmo tipo de FLR.
- Um file system clonado tem o mesmo tipo de FLR que a origem (não pode ser modificado).

O modo FLR é exibido na coluna **FLR Mode** da tabela **File Systems** .

## Configurar o servidor DHSM

A retenção em nível de arquivo exige credenciais de servidor DHSM.

O servidor DHSM também é necessário para hosts do Windows que querem usar FLR e precisam instalar o kit de ferramentas da FLR que permite o gerenciamento de file systems compatíveis com FLR.

1. Selecione **Armazenamento** > **Servidores NAS** > **[servidor NAS]** > **Proteção** > **DHSM**.
2. Se estiver desativado, deslize o botão até **Ativado**.
3. Digite o nome de usuário e a senha do servidor DHSM e verifique a senha.
4. Selecione **Aplicar**.

# Configurar a retenção em nível de arquivo

A retenção em nível de arquivo é configurada na criação do file system. Para obter detalhes, consulte Criar file system.

**NOTA:** A retenção em nível de arquivo e seu nível são determinados na criação do sistema de arquivos e não podem ser modificados, mas os parâmetros do período de retenção podem ser modificados.

# Modificar a retenção em nível de arquivo

Os parâmetros de período de retenção podem ser definidos na criação do file system ou posteriormente e podem ser modificados.

**NOTA:** A modificação dos parâmetros de período de retenção não afeta os arquivos que já estão bloqueados.

1. Selecione **Armazenamento** > **File Systems** > **[file system]** > **Segurança e eventos** > **Retenção em nível de arquivo**.
2. Defina os parâmetros do período de retenção:
   - Período mínimo de retenção — Especifica o período mais curto durante o qual um file system habilitado para FLR pode ser protegido (o valor padrão é um dia).
   - Período de retenção padrão — Usado quando um arquivo está bloqueado e um período de retenção não foi especificado (o valor padrão é um ano).
   - Período máximo de retenção — Especifica o período mais longo durante o qual um file system habilitado para FLR pode ser protegido (o valor padrão é infinito).
3. Opcionalmente, defina as configurações avançadas:
   - Bloqueio automático de arquivos — Você pode especificar se deseja bloquear automaticamente os arquivos em um file system habilitado para FLR e definir um intervalo de política que determine o período entre a modificação do arquivo e o bloqueio automático (o valor padrão do intervalo de política é uma hora).
   - Exclusão automática de arquivos — Você pode especificar se deseja excluir automaticamente os arquivos bloqueados após o vencimento do período de retenção. A primeira varredura para localizar arquivos para exclusão ocorre sete dias após a ativação do recurso.
4. Selecione **Aplicar**.

4

# Recursos adicionais de servidores NAS

Este tópico contém as seguintes informações:

**Tópicos:**



## Definir o UNIX Directory Service preferencial

Depois de criar um servidor NAS, você pode definir a ordem de pesquisa do UNIX Directory Services (UDS) preferencial para acesso de usuário.

1. Selecione **Storage** > **NAS Servers**.
2. Marque a caixa de seleção na coluna **Name** à esquerda do servidor NAS.
3. Clique em **Modificar**.
4. Selecione a ordem de pesquisa preferencial do UDS para uso na lista suspensa **Unix Directory Service Search Order**.
5. Clique em **Apply**.

## Configurar redes do servidor NAS

Você pode modificar ou configurar redes do servidor NAS.

Configure o seguinte para redes do servidor NAS:

- As interfaces de arquivo
- Rotas para serviços externos, como hosts.

### Configurar interfaces de arquivo para um servidor NAS

Você pode configurar as interfaces de arquivo para um servidor NAS depois de adicionar o servidor ao PowerStore.

Você pode adicionar mais interfaces de file e definir qual é a preferencial a ser usada. Além disso, você pode definir qual interface usar para produção e backup ou para IPv4 ou IPv6.

1. Selecione **Storage** > **NAS Servers** > **[nas server]**.
2. Na página **Rede**, clique em **Adicionar** para adicionar outra interface de arquivo ao servidor NAS.
3. Digite as propriedades da interface de file.

   **NOTA:** Não reutilize VLANs que estão sendo usadas para as redes de gerenciamento e de armazenamento.

4. Você pode executar as ações a seguir em uma interface de file selecionando uma interface de file na lista. Selecione:

| Opção | Descrição |
|---|---|
| Modify | Para alterar as propriedades das propriedades da interface de file. |
| Delete | Para excluir a interface de file do servidor NAS. |
| Ping | Para testar a conectividade do servidor NAS com o endereço IP externo. |
| Interface preferencial | Para definir qual interface o PowerStore deve usar como padrão quando várias interfaces de produção e backup tiverem sido definidas. |

## Configurar rotas para a interface de file para conexões externas

Você pode configurar as rotas que o file system usa para conexões externas.

Você pode usar a opção **Ping** no card **File Interface** para determinar se a interface de file tem acesso ao recurso externo.

Geralmente, as interfaces do servidor NAS são configuradas com um gateway padrão, que é usado para rotear as solicitações da interface do servidor NAS para serviços externos.

Execute as seguintes etapas:

- Se você precisar configurar rotas mais específicas para serviços externos.
- Para adicionar uma rota para acessar um servidor a partir de uma interface específica, por meio de um gateway específico.

1. Selecione **Armazenamento** > **Servidores NAS** > **[servidor nas]** > **Rede** > **Rotas para serviços externos**.
2. Clique em **Add** para especificar as informações de rota no assistente **Add Route**.

# Ativar o backup de NDMP

Você pode configurar o backup padrão para os servidores NAS usando NDMP. O protocolo de gerenciamento de dados da rede (NDMP, Network Data Management Protocol) fornece um padrão para fazer backup de servidores de arquivos em uma rede. Quando o NDMP está ativado, um aplicativo de gerenciamento de dados (DMA) de terceiros, como o Dell Networker, é capaz de detectar o NDMP do PowerStore usando o endereço IP do servidor NAS.

O NDMP é realizado após a criação do servidor NAS.

O PowerStore é compatível com:

- NDMP de três vias — Os dados são transferidos pelo DMA por uma Rede Local (LAN) ou WAN.
- Backups completos e incrementais

1. Selecione **Armazenamento** > **Servidores NAS** > **[servidor nas]** > **Proteção** .
2. Em **NDMP Backup**, se a opção **Disabled** estiver ativada, deslize o botão para mudar para **Enabled**.
3. Digite uma senha em **New Password**.
   O nome de usuário sempre é `ndmp`.
4. Digite novamente a mesma senha como a nova senha em **Verificar senha**.
5. Clique em **Aplicar**.

Saia da página NDMP e volte a ela para confirmar se o NDMP está habilitado.

# 5

# Mais recursos de file system

Este tópico contém as seguintes informações:

**Tópicos:**



# Cotas do File system

Você pode controlar e limitar o consumo de espaço em unidade por meio da configuração de cotas para file systems no nível de diretório ou file system. Você pode habilitar ou desabilitar cotas a qualquer momento, mas recomenda-se que você as habilite ou desabilite durante o horário de produção fora de pico para evitar impacto nas operações do file system.

**NOTA:** Você não pode ativar cotas para file systems de somente leitura.

**NOTA:** As cotas não são compatíveis com file systems VMware.

**NOTA:** Quando você cria uma sessão de replicação, as cotas não são visíveis no sistema de destino, mesmo que estejam ativadas no sistema de origem.

## Tipos de cota

Existem três tipos de cota que você pode colocar em um file system.

**Tabela 2. Tipos de cota**

| Type | Descrição |
|---|---|
| Cotas de usuário | Limita o volume de armazenamento que um usuário individual consome ao armazenar dados no file system. |
| Cota de árvore | As cotas de árvore limitam a quantidade total de armazenamento consumida em uma árvore de diretórios específica. Você pode usar cotas de árvore para:<br>● Definir limites de armazenamento de cada projeto. Por exemplo, você pode estabelecer cotas de árvore para um diretório de projeto que possui vários usuários compartilhando e criando arquivos nele.<br>● Controlar o uso do diretório configurando os limites fixos e flexíveis de cota de árvore para 0 (zero).<br>**NOTA:** Se você alterar os limites de uma cota de árvore, as alterações terão efeito imediatamente sem interromper as operações do file system. |
| Cota do usuário em uma árvore de cotas | Limita o volume de armazenamento que um indivíduo consome ao armazenar dados na árvore de cotas. |

## Limites de cota

**Tabela 3. Limites flexíveis e rígidos**

| Type | Descrições |
|---|---|
| Fixo | Um limite rígido é um limite absoluto no uso de armazenamento. |

**Tabela 3. Limites flexíveis e rígidos (continuação)**

| Type | Descrições |
|---|---|
| | Se um limite fixo for atingido para uma cota de usuário em um file system ou árvore de cotas, o usuário não poderá gravar dados para o file system ou a árvore até que mais espaço seja disponibilizado. Se um limite rígido for atingido para uma árvore de cotas, nenhum usuário será capaz de gravar dados na árvore até que mais espaço se torne disponível. |
| Limite flexível | Um limite flexível é um limite preferido na utilização de armazenamento.<br>O usuário tem permissão para usar o espaço até que um período de tolerância tenha sido atingido.<br>O usuário será alertado quando o limite flexível for atingido, até que o período de tolerância acabe. Depois disso, uma condição de falta de espaço é atingida até que o usuário volte para abaixo do limite flexível. |

## Período de tolerância de cota

O período de tolerância das cotas permite definir um período de tolerância específico para cada cota de árvore em um file system. O período de tolerância contabiliza o tempo entre o limite flexível e fixo e alerta o usuário sobre o tempo restante antes que o limite fixo seja atingido. Se o período de tolerância expirar, você não poderá gravar no sistema de arquivos até que mais espaço seja adicionado, mesmo que o limite rígido não tenha sido atingido.

Você pode definir uma data de expiração para o período de tolerância. O padrão é sete dias, mas você pode definir a data de vencimento do período de tolerância para uma quantidade de tempo infinita (de maneira que ele nunca expire) ou para determinado número de dias, horas ou minutos. Depois que a data de expiração do período de tolerância for atendida, o período de tolerância não se aplicará mais ao diretório do file system.

## Informações adicionais

Para obter mais informações sobre cotas, consulte o *white paper sobre recursos de arquivo do Dell PowerStore*.

# Ativar cotas do usuário

Para poder adicionar uma cota de usuário a um file system, é necessário ativar as cotas e definir os valores padrão das cotas de usuário.

1. Selecione **Storage** > **File Systems** > **[file system]** > **Quotas**.
2. Selecione **Storage** > **File Systems** > **[file system]** > **Quotas** > **Properties**.
3. Deslize o botão da posição **Desativado** para **Ativado**.
4. Digite o **Período de carência** padrão para a cota de usuário no file system, o que ativará a contagem regressiva desde o limite flexível até o limite fixo.
5. Digite um **Soft Limit** padrão e um **Hard Limit** padrão e clique em **Update**.

# Adicionar uma cota de usuário a um file system

Crie uma cota de usuário em um file system para limitar ou rastrear a quantidade de espaço de armazenamento que usuários individuais consomem nesse file system. Ao criar ou modificar as cotas de usuário, você pode usar os limites de padrão fixo e flexível, que são definidos no nível do file system.

Você deve ativar a opção Quotas e definir os valores padrão de User Quota para poder adicionar uma cota de usuário a um file system. Consulte Ativar User Quotas.

**NOTA:** Você não pode criar cotas para file systems somente leitura.

1. Selecione **Storage** > **File Systems** > **[file system]** > **Quotas** > **User**.
2. Selecione **Add** na página **User Quota**.
3. No assistente **Add User Quota**, forneça as informações solicitadas. Para monitorar o consumo de espaço sem limites de configuração, defina **Soft Limit** e **Hard Limit** como 0, que indica que não há limite.
4. Selecione **Adicionar**.

## Adicionar uma árvore de cotas a um file system

Crie uma árvore de cotas no nível do diretório de um file system para limitar ou monitorar o espaço de armazenamento total consumido por esse diretório.

1. Selecione **Storage** > **File Systems** > **[file system]** > **Quotas** > **Tree Quotas**.
2. Selecione **Adicionar**.
3. Deslize **Enforce User Quota** para a direita para ativar os valores padrão de User Quota em Tree Quota.
4. Especifique as informações solicitadas.
   - Digite um período de latência em **Grace Period** para iniciar a contagem regressiva entre os limites flexível e rígido. Você começará a receber alertas quando o período de tolerância for atingido.
   - Para monitorar o consumo de espaço sem definir limites, configure os campos **Soft Limit** e **Hard Limit** com 0, que indica que não há limite.
5. Selecione **Adicionar**.

## Adicionar uma cota de usuário a uma árvore de cotas

Crie uma cota de usuário em uma árvore de cotas para limitar ou rastrear a quantidade de espaço de armazenamento que consomem de usuários individuais na árvore. Ao criar cotas de usuário em uma árvore, você pode usar o período de tolerância padrão e os limites rígido e flexível padrão configurados no nível da cota de árvore.

1. Selecione **Storage** > **File Systems** > **[file system]** > **Quotas** > **Tree Quotas**.
2. Selecione um caminho e clique em **Add User Quota**.
3. Na tela **Add User Quota**, forneça as informações solicitadas. Para monitorar o consumo de espaço sem definir limites, configure os campos **Soft Limit** e **Hard Limit** com 0, que indica que não há limite.

# Qualidade de serviço (QoS) de arquivos

Em um sistema que executa cargas de trabalho variadas com demandas imprevisíveis, a qualidade de serviço garante que aplicativos essenciais possam ter prioridade e fornece desempenho previsível para cada aplicativo.

Você pode aplicar políticas de qualidade de serviço (QoS) para definir a largura de banda máxima para servidores NAS e file systems.

Quando você atribui uma política de QoS a um servidor NAS ou file system, o SDNAS aplica a política em serviços NFS/SMB.

Os limites de largura de banda são aplicados com base nos protocolos NFS/SMB e SFTP/FTP.

Se a largura de banda definida exceder a largura de banda máxima definida para o servidor NAS, a largura de banda efetiva será a largura de banda máxima do servidor.

**NOTA:** Pode levar algum tempo para que uma política de QoS entre em vigor.

**NOTA:** A QoS não é suportada com clones de servidor NAS, clones de file system, snapshots, clones de snapshots e atualização de snapshots.

**NOTA:** A largura de banda aplicada a servidores NAS e file systems como parte de uma política de QoS atribuída pode variar dentro de uma margem de 10%.

Limites de QoS de arquivos:

- Uma política de QoS pode incluir uma regra de limite de E/S.
- É possível definir até 100 políticas de QoS de arquivo.
- É possível definir até 100 regras de QoS de arquivo.
- Somente uma política de QoS pode ser aplicada a um servidor NAS ou file system.
- A mesma política de QoS pode ser atribuída a vários servidores NAS e file systems.

QoS e replicação de arquivos:

- Quando o servidor NAS tem uma regra de replicação, a política de QoS atribuída é replicada para o servidor de destino.
- Quando você modifica as políticas de QoS atribuídas ao servidor NAS, as alterações são replicadas para o servidor de destino.
- Não é possível modificar a configuração da política de QoS replicada no servidor de destino.
- Não é possível atribuir uma política de QoS a um servidor NAS ou file system no servidor de destino.

- Depois de atribuir uma política de QoS a um servidor NAS ou file system no servidor de origem, não é possível cancelar a atribuição da política do servidor de destino.
- Depois de cancelar a atribuição de uma política de QoS de um servidor NAS, a política também deverá ser cancelada no destino.
- Após o failover, você pode atribuir, cancelar a atribuição e modificar políticas de QoS replicadas.

## Limites de QoS de arquivo

Você pode criar regras de limite de E/S para servidores NAS e file systems. Uma regra de limite de E/S define a largura de banda máxima permitida.

- Cada servidor NAS ou file system pode ser associado a apenas uma regra de limite.
- Cada política pode incluir apenas uma regra.
- Você pode definir até 100 regras.

**NOTA:** A largura de banda observada pode exceder o valor definido, especialmente em limites definidos inferiores.

As regras de limite de E/S se aplicam somente à E/S de hosts externos e não a operações de replicação síncrona ou assíncrona interna ou E/S de migração.

As regras de limite de E/S não são aplicadas a objetos criados internamente, como backups NDMP atendidos por um servidor NDMP no SDNAS.

Alertas específicos para limites de QoS de arquivo não são suportados. Para saber se os limites definidos exigem um ajuste, você pode monitorar os gráficos de latência, IOPS e largura de banda para cada servidor NAS e file system.

## Criar uma regra e política de limite de largura de banda de qualidade de serviço (QoS)

Você pode criar uma regra de limite de largura de banda e adicioná-la a uma política de QoS.

1. Selecione **Storage** > **Quality of Service (QoS)** > **File I/O Limit Rules**.
2. Selecione **Criar**.
3. No controle deslizante **Create File I/O Limit Rule**, defina o nome da regra e a largura de banda máxima (MB/s).
4. Selecione **Criar**.
   A regra é adicionada à tabela File I/O Limit Rules.
5. Selecione **File QoS Policies**.
6. Selecione **Criar**.
7. No controle deslizante **Create File QoS Policy**, defina o nome da política. Também é possível adicionar uma descrição.
8. Na lista de regras, selecione a regra que você deseja adicionar à política.
9. Selecione **Criar**.
   A política é adicionada à tabela File QoS Policies.

## Atribuir uma política de QoS de arquivo

Depois de definir uma regra de limite de E/S como parte de uma política de QoS de arquivo, você pode atribuí-la a um servidor NAS ou a um file system. Você também pode modificar a política de QoS atribuída.

**NOTA:** Também é possível atribuir uma política de QoS como parte do procedimento para criar um servidor NAS ou um file system.

1. Selecione **Storage** > **NAS Servers** ou **Storage** > **File Systems**.
2. Marque a caixa de seleção ao lado do servidor NAS ou file system relevante.
3. Selecione **More Actions** > **Change QoS Policy**.
4. No painel deslizante **Change QoS Policy**, selecione uma política de QoS de arquivo e, em seguida, selecione **Apply**.
   A política é atribuída. Você pode visualizar o nome da política atribuída na coluna **QoS Policy** nas tabelas NAS Server e File Systems. Você pode visualizar o impacto da política atribuída no desempenho selecionando **Storage** > **NAS Servers** > **[NAS server]** > **Performance** ou **Storage** > **File Systems** > **[file system]** > **Performance**.
   **NOTA:** Você também pode definir a política de QoS selecionando o servidor NAS ou file system relevante e, em seguida, selecionando **Modify**.

# Modificar uma política de QoS de arquivo

Você pode modificar uma política de QoS selecionando uma regra de limite de E/S diferente.

Não é possível modificar uma política atribuída a um servidor NAS ou file system.

1. Selecione **Storage** > **Quality of Service (QoS)**.
2. Na tabela **File QoS Policies**, marque a caixa de seleção ao lado da política de QoS que você deseja modificar.
3. Selecione **Modify**.
4. Na janela **Modify QoS Policy**, você pode modificar o nome e a descrição da política e selecionar uma regra de limite de E/S diferente.
5. Selecione **Aplicar**.

   **NOTA:** Você também pode modificar uma política de QoS na tela **Properties** do recurso de armazenamento.

# Excluir uma política de QoS de arquivo

Certifique-se de que a política de QoS que você deseja excluir não esteja atribuída a um servidor NAS ou file system.

1. Selecione **Storage** > **Quality of Service (QoS)**.
2. A partir da tabela **File QoS Policies**, selecione a política de QoS que você deseja excluir.
3. Selecione **More Actions** > **Delete**.
4. Selecione **Excluir** para confirmar.

# 6

# Replicação de servidores NAS

Este tópico contém as seguintes informações:

**Tópicos:**



## Visão geral

Para ativar a redundância e a recuperação aprimoradas em caso de perda de dados, o PowerStore permite replicar servidores NAS de um sistema local para um sistema remoto.

Por padrão, a replicação ocorre no nível do servidor NAS — todos os file systems do servidor NAS replicado são replicados no sistema remoto. É possível selecionar para adicionar ou excluir file systems do servidor NAS quando ele faz parte de uma sessão de replicação.

Também é possível selecionar a replicação assíncrona, em que os sistemas são sincronizados com base em um RPO definido, ou a replicação síncrona, em que as alterações são replicadas do sistema de origem para o sistema de destino imediatamente quando ocorrem.

Estes são os pré-requisitos para ativar a replicação de arquivos:

- Um file system remoto
- É necessário configurar e mapear uma rede de mobilidade de arquivos (consulte *Guia de sistema de rede do PowerStore T e Q para Storage Services* na página de documentação do PowerStore).
- Uma política de proteção com uma regra de replicação.

Considere as seguintes informações para a replicação do servidor NAS:

- Não é necessário definir políticas de proteção separadas para os servidores NAS. As mesmas políticas de proteção podem ser aplicadas à replicação de bloco e de arquivo.
- E possível excluir file systems do sistema de origem de uma sessão de replicação. Após a exclusão, apenas os file systems restantes são replicados para o destino. O status do sistema destino não é afetado após a exclusão do file system. Se você excluir file systems de um servidor NAS de origem de replicação e, em seguida, fazer failover para o sistema de destino, os file systems que foram excluídos da origem antiga não serão replicados pela nova origem. Se você deseja replicar esses file systems, gere clones que possam ser replicados e exclua os file systems.
- Você pode fazer failover de uma sessão de replicação para o sistema remoto. O failover ocorre para todos os file systems dentro do servidor NAS submetido a failover.
- Quando você cria uma sessão de replicação, as cotas não são visíveis no sistema de destino, mesmo que estejam ativadas no sistema de origem.
- Na replicação assíncrona, o RPO é configurado no nível do servidor NAS e é idêntico em todos os file systems associados.
- Para replicação síncrona, aumentar o tamanho de um file system que está em replicação exige pausar a sessão de replicação primeiro. Reduzir o tamanho de um file system não exige pausar a sessão de replicação.
- No caso de replicação síncrona, não é possível alterar a latência de rede do par de sistemas de replicação para um valor maior do que cinco milissegundos quando sessões de replicação síncrona são definidas.
- Não é possível alternar entre replicação síncrona e assíncrona para a replicação de arquivos.

Para obter informações detalhadas sobre procedimentos de replicação do servidor NAS, consulte o *Guia Protegendo seus* PowerStore dados na página Documentação.

## Testando a recuperação de desastres para servidores NAS em replicação

Um teste de recuperação de desastres executa um plano de recuperação de desastres que permite verificar se o sistema pode recuperar e restaurar os dados e a operação em caso de desastre.

O PowerStore oferece várias opções para testar a capacidade do sistema de se recuperar de um desastre e reaver a funcionalidade:

- Clonar um servidor NAS para testes de recuperação de desastres usando endereços IP exclusivos.
- Clonar um servidor NAS para testes de recuperação de desastres usando uma rede isolada com endereços IP duplicados.
- Realizar um failover planejado.

# Clonar um servidor NAS para testes de recuperação de desastres usando endereços IP exclusivos

Clonar um servidor NAS é a opção recomendada para testar a DR. Você pode clonar o servidor NAS usando o PowerStore Manager e testá-lo sem afetar a produção. Para habilitar o acesso ao servidor NAS recém-clonado, é necessário configurar uma interface de rede nova e exclusiva. O endereço IP configurado não pode estar em uso nos servidores NAS de origem ou destino. Configurações exclusivas também são necessárias para associar o servidor a um domínio do AD.

As alterações feitas nos file systems clonados e nos file systems de produção não afetam umas às outras. Quando o teste de DR estiver concluído, o servidor clonado poderá ser excluído.

Você pode escolher uma das opções a seguir:

- Clone o servidor NAS no sistema de origem, replique-o para o destino e realize um failover planejado no sistema de destino.
- Clone o servidor NAS no sistema de destino e acesse os dados (o failover não é necessário porque os recursos clonados já estão acessíveis no sistema de destino).

1. No PowerStore, selecione **Storage** > **NAS Servers**.
2. Selecione o servidor NAS que deseja clonar e, em seguida, selecione **Repurpose** > **Clone NAS Server**.
3. Na janela **Create Clone**, informe um nome para o clone e selecione os file systems que deseja clonar.
4. Selecione **Criar**.
   O servidor NAS clonado é adicionado à lista de servidores.
5. Selecione o nome do servidor NAS clonado para abrir a janela de detalhes do servidor.
6. Para adicionar uma interface de arquivo:
   a. Selecione a guia **Rede**.
   b. Em **File Interface,** selecione **Add**.
   c. Forneça as informações da interface e selecione **Add**.
7. Para definir o protocolo de compartilhamento:
   a. Selecione a guia **Protocolos de compartilhamento**.
   b. Selecione o protocolo relevante (SMB, NFS ou FTP).
   c. Configure as informações necessárias e selecione **Apply**.
8. Se você clonou o servidor NAS de origem:
   a. Replique o servidor NAS para o sistema de destino. Para obter detalhes, consulte Replicação do servidor NAS.
   b. Realize um failover planejado no destino. Para obter detalhes, consulte Failover planejado.
   c. Verifique se o host pode acessar os dados.
9. Se você clonou o servidor de produção replicado no sistema de destino, o failover não é necessário. Verifique o acesso ao host.

# Clonar um servidor NAS para testes de recuperação de desastres usando uma rede isolada com endereços IP duplicados

É possível testar a recuperação de desastres usando a mesma configuração da produção. O uso de configurações idênticas pode reduzir o risco e aumentar a capacidade de reprodução em um cenário de falha. No entanto, o uso de endereços IP duplicados cria conflitos. A execução do teste de DR em um ambiente isolado do ambiente de produção permite evitar esses conflitos.

No PowerStoreOS 3.6 e posterior, você pode criar um ambiente isolado de teste de recuperação de desastres (DRT) para ajudá-lo a se preparar para um desastre.

Com a criação de um ambiente isolado, é possível usar o mesmo endereço IP e hostname do sistema de produção e executar um DRT para um servidor NAS em replicação sem nenhum impacto sobre a produção.

Para criar um ambiente DRT, você deve configurar uma rede isolada com um roteador DRT separado e criar agregações de links com as portas de E/S de rede.

Usando a PSTCLI ou a API REST, crie um ambiente de rede dedicado no servidor de destino clonando o servidor NAS em replicação no sistema PowerStore de destino. O clone é uma cópia completa do ambiente de produção e de um ambiente de teste dedicado que é isolado da produção. Você pode criar um ambiente de rede isolado e configurar o ambiente de teste com o mesmo endereço IP e hostname que o sistema de produção. O servidor DRT NAS não tem impacto sobre o ambiente de produção e poderá ser executado sem conflitos de endereço IP quando ocorrer failover e failback no servidor NAS de replicação.

Para testar a DR usando um ambiente de teste isolado:

1. Crie o clone do servidor NAS no destino. Use o indicador `is_dr_test`.
2. Crie uma interface de vinculação de usuário para NAS usando o mesmo endereço IP que o servidor NAS de origem.
3. Ingresse o clone ao AD (se necessário).
4. Verifique se os hosts podem acessar os dados.

**NOTA:** Você também pode usar o DRT em servidores NAS independentes.

## Pré-requisitos e limitações

Para criar um ambiente DRT, certifique-se de que os seguintes requisitos sejam atendidos:

- Obtenha as informações da rede privada:
  - Gateway
  - Máscara de rede
  - VLAN ID (opcional)
- Identifique as portas da rede isolada e as portas da rede de produção.

Observe as seguintes limitações ao criar um ambiente DRT:

- A interface de vinculação dedicada ao DRT não pode ser usada para criar outros servidores NAS de produção.
- Um servidor NAS configurado como produção não pode ser reconfigurado como parte do DRT.
- Um servidor NAS configurado como parte do DRT não pode ser reconfigurado como produção.
- Um servidor NAS que não faz mais parte de um DRT não pode ser reconfigurado e deve ser excluído.
- Depois que um servidor NAS estiver ativo e configurado com informações de rede, a configuração adicional (como DNS, CAVA e Kerberos) deverá ser feita manualmente.
- O servidor NAS habilitado para DRT não pode ser replicado.
- A modificação e exclusão do servidor NAS pode ser feita usando o PowerStore Manager.

## Configurar o ambiente de teste de recuperação de desastres usando o PSTCLI

1. Obtenha o nome do servidor NAS no local de destino (a ser clonado):

```
[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 o servidor NAS fornecendo um novo nome para o clone e usando o 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. Localize o ID da porta IP para o vínculo de arquivo NAS conectado à rede isolada:

   **NOTA:** Se o vínculo de arquivo NAS não tiver sido criado, você poderá criá-lo usando o PSTCLI ou 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. Crie a interface do arquivo para o 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. Exiba a interface do arquivo:

```
[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 um servidor NAS em um ambiente DRT usando a API REST

**NOTA:** Se você não estiver usando a API REST, ignore esta seção.

1. Para clonar o servidor NAS no namespace especificado, execute `/nas_server/{id}/clone` e especifique `is_dr_test` como true.
2. Para criar uma interface de rede, execute o comando `/file_interface` e especifique os parâmetros de rede privada.

   **NOTA:** Essa etapa cria a interface de arquivo para o servidor NAS clonado usando o mesmo endereço IP, máscara de rede e gateway que o servidor NAS de produção. Use a interface/IP_Port vinculada associada à rede privada.

O servidor NAS está ativo e pode ser usado para DRT na rede isolada.

# Realizar um failover planejado

Você pode usar o failover planejado para testar a recuperação de desastres. Quando você realiza um failover planejado, a sessão de replicação do servidor NAS faz failover manualmente do sistema de origem para o sistema de destino. Antes do failover, o sistema de destino é sincronizado com o sistema de origem para evitar a perda de dados.

**NOTA:** O failover do servidor NAS de produção para o sistema de destino pode afetar a produção.

Antes de realizar um failover planejado, interrompa as operações de E/S de todos os aplicativos e hosts. Não é possível pausar uma sessão de replicação que está passando por um failover planejado.

Quando a operação está normal, as alterações feitas no servidor NAS e nos file systems durante o teste de DR são preservadas e replicadas de volta para a origem inicial assim que a nova proteção é iniciada (manual ou automaticamente). No entanto, se você não quiser salvar as alterações feitas durante o teste de DR (dados ou configuração), é possível optar por descartar as alterações, usando os comandos da API REST ou da PSTCLI:

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

As alterações que são descartadas:

- Para servidores NAS:
  - Alterações de configuração
- Para file systems:
  - Alterações de configuração
  - Alterações de dados do file system
  - Recursos de snapshot
  - Alterações de tamanho do file system
  - Alterações de cota

- Para exportações e compartilhamentos:
  - Alterações de exportações NFS
  - Alterações de compartilhamentos SMB

**NOTA:** Essa opção somente é compatível com a replicação assíncrona.

Para obter mais detalhes sobre como utilizar a API REST e a CLI para descartar alterações após o failover, consulte o *Guia de referência da API REST do Dell PowerStore* e o *Guia de referência da CLI do Dell PowerStore*, em dell.com/powerstoredocs.

Depois que o servidor NAS for protegido novamente, você poderá iniciar um failover planejado mais uma vez para colocar os recursos on-line no sistema de origem inicial.

**NOTA:** Não realize failover não planejado para fins de recuperação de desastres. O failover não planejado deve ser usado somente quando o sistema de origem está inacessível.

**NOTA:** Para habilitar o acesso não disruptivo aos dados no ambiente SMB, é recomendável configurar a disponibilidade contínua para compartilhamentos SMB e remontar os compartilhamentos após restabelecer a conexão.

Existem duas maneiras de iniciar um failover planejado:

- Em **Proteção** > **Replicação**, selecione a sessão de replicação relevante e escolha **Failover planejado**.
- Na guia **Proteção** do recurso, selecione **Replicação** e escolha **Failover planejado**.

Após um failover planejado, a sessão de replicação fica inativa. Para sincronizar o recurso de armazenamento de destino e retomar a sessão de replicação, use a ação **Reprotect**. Você também pode selecionar a opção de proteção automática antes de fazer failover, o que inicia automaticamente a sincronização na direção oposta (no próximo RPO) após a conclusão do failover e retorna os sistemas de origem e de destino a um estado normal.

**NOTA:** Após o failover, as cotas de usuário não ficarão visíveis no sistema de destino (que se tornou a nova origem). Para visualizar as cotas de usuário, atualize as cotas manualmente selecionando **Armazenamento** > **File systems**, marcando a caixa de seleção ao lado do file system relevante e, em seguida, selecionando **Mais ações** > **Atualizar cotas**.

## Desconexão de rede durante o DRT

Ao executar o DRT, não é recomendável simular uma falha de rede entre os sistemas local e remoto e, então, executar um failover não planejado para o sistema de destino para permitir o acesso ao servidor DR NAS. Como não há comunicação entre os sistemas, PowerStore não é possível garantir que ambos os servidores NAS estejam em um estado compatível. Depois que a conexão é restaurada, os dois servidores NAS ficam no modo de produção (split brain). Como resultado, os dois sistemas alternam para o modo de destino para evitar que os dados sejam gravados em ambos os locais.

Para resolver esse estado, é necessária a intervenção do suporte técnico.

Para obter mais informações, consulte o artigo da base de conhecimento Dell 000215482 (Interrupção da conexão de rede entre locais...).

# 7

# Usando CEPA com o PowerStore

Este tópico contém as seguintes informações:

**Tópicos:**



## Publicação de eventos

O CEE permite que aplicativos de terceiros recebam informações sobre eventos do sistema de armazenamento ao acessar file systems.

O Common Event Enabler (CEE) fornece uma solução de publicação de eventos para clients PowerStore que permite que aplicativos de terceiros sejam registrados para receber notificações de eventos e contexto do sistema de armazenamento ao acessar file systems. Ao receber notificações de eventos, você pode tomar medidas em relação ao armazenamento com base nesses eventos para impedir ameaças de segurança, como ransomware ou acesso não autorizado.

O Common Events Publishing Agent (CEPA) do CEE consiste em aplicativos projetados para processar notificações de eventos de diretório e arquivos SMB e NFS. O CEPA entrega notificações de eventos e o contexto associado ao aplicativo em uma mensagem. O contexto pode consistir em metadados de arquivo ou de diretório que são necessários às decisões sobre a política do setor.

Para ativar o suporte a CEPA do CEE, você deve ativar o CEPA do CEE e criar um pool de publicação de eventos no servidor NAS.

Um pool de publicação de eventos define os servidores CEPA e os eventos específicos que acionam notificações.

Depois de configurar o servidor NAS, você pode ativar a publicação de eventos no file system do qual deseja receber eventos. Quando um host gera um evento no file system por SMB ou NFS, essa informação é encaminhada ao servidor CEPA por meio de uma conexão HTTP. O software CEPA do CEE no servidor recebe o evento e o publica, permitindo que o software de terceiro o processe.

Para usar o Events Publishing Agent, é preciso ter um sistema PowerStore com pelo menos um servidor NAS configurado na rede.

Para obter mais informações sobre o CEPA, que faz parte do Common Event Enabler (CEE), consulte *Usando o Common Event Enabler em plataformas Windows*, no site de suporte da Dell Technologies.

## Criar um pool de publicação

Para criar um pool de publicação de eventos, você deve ter um FQDN de servidor de publicação de eventos (CEPA).

Um pool de publicação de eventos define o servidor CEPA e os eventos específicos que acionam notificações. Defina pelo menos uma das seguintes opções de evento:

- Eventos pré — Eventos enviados ao servidor CEPA para aprovação antes do processamento.
- Eventos pós — Eventos enviados ao servidor CEPA depois que eles ocorrem para fins de log ou auditoria.
- Eventos pós-erro — Eventos de erro são enviados ao servidor CEPA depois que eles ocorrem para fins de log ou auditoria.

1. Selecione **Armazenamento** > **Servidores NAS**.
2. Selecione **Configurações de NAS**.
3. Na janela **Publicação de eventos**, selecione **Pools de publicação** e, em seguida, selecione **Criar**.
4. Digite um **Nome do pool**.
5. Informe o FQDN do servidor CEPA.
6. Na seção Configuração de eventos, clique nos tipos de evento e selecione os eventos que deseja adicionar ao pool.
7. Clique em **Aplicar** para criar o pool de publicação de eventos.

# Criar um editor de eventos

Depois de configurar pools de publicação, crie um editor de eventos para definir a resposta aos diferentes tipos de evento.

**NOTA:** Os editores de eventos são criados no nível do sistema, e um editor de eventos pode ser associado a vários servidores NAS.

1. Selecione **Armazenamento** > **Servidores NAS**.
2. Selecione **Configurações de NAS**.
3. Selecione **Editores de eventos** e, em seguida, selecione **Criar**.
4. Continue trabalhando no assistente **Criar editor de eventos**.

| Tela do assistente | Descrição |
|---|---|
| Selecionar pools de publicação | • Insira um nome.<br>• Selecione até 3 pools de publicação. Para criar um pool de publicação, clique em **Criar**. |
| Configurar editor de eventos | • Política de falha de eventos preliminares — Selecione o comportamento desejado quando todos os servidores CEPA estiverem off-line para eventos preliminares:<br>  ○ Ignorar (padrão) — Suponha que todos os eventos sejam confirmados.<br>  ○ Negar — Negue eventos que exijam aprovação até que os servidores CEPA estejam on-line.<br>• Política de falha de eventos posteriores — Selecione o comportamento desejado quando todos os servidores CEPA estiverem off-line para eventos posteriores:<br>  ○ Ignorar (padrão) — Continue operando. Os eventos que ocorrerem enquanto os servidores CEPA estiverem inativos serão perdidos.<br>  ○ Acumular — Continue operando e salve eventos em um buffer local (até 500 MB).<br>  ○ Garantir — Continue operando e salve eventos em um buffer local (até 500 MB). Negue acesso quando o buffer estiver cheio.<br>  ○ Negar — Negue acesso aos file systems quando os servidores CEPA estiverem off-line.<br>• HTTP/Microsoft RPC<br>• Porta HTTP |

5. Selecione **Aplicar** para criar o Editor de eventos.

# Ativando um editor de eventos para um servidor NAS

Depois de configurar o editor de eventos, ative-o para o servidor NAS e todos os file systems definidos nele.

1. Selecione **Armazenamento** > **Servidores NAS** > **[servidor NAS]**.
2. Na página **Segurança e eventos**, selecione **Publicação de eventos**.
3. Selecione um editor de eventos na lista e ative-o.
4. Indique se você deseja ativar o editor de eventos para todos os file systems definidos no servidor NAS.

   Como alternativa, você pode selecionar a opção para ativar o editor de eventos para file systems específicos. Para obter detalhes, consulte Ativar editor de eventos do file system.
5. Clique em **Aplicar**.

# Ativar o editor de eventos para um file system

Você pode ativar o editor de eventos para file systems selecionados.

1. Selecione **Armazenamento** > **File systems** > **[file system]**.
2. Na página **Proteção**, selecione **Publicação de eventos**.
3. Ative o editor de eventos para o file system e selecione o protocolo.
4. Clique em **Aplicar**.