Dell PowerStore

Configurar o SMB

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.

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 o provedor de serviços se um produto não funcionar adequadamente ou não funcionar conforme descrito neste documento.

Onde obter ajuda

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

- **Informações sobre**o produto — Para obter a documentação do produto e de recursos ou as notas da versão, acesse o Hub de informações do PowerStore.
- **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.

Feedback do cliente

Um botão de feedback está localizado no lado direito do PowerStore Manager. Selecionar **Feedback** abre uma janela do navegador onde você pode preencher e enviar uma pesquisa de feedback.

1

Visão geral

Este tópico contém as seguintes informações:

Tópicos:

Suporte do SMB

O Modelo PowerStore T e o PowerStore modelo Q oferecem suporte do SMB 1 ao SMB 3.1.1. Quando o suporte para SMB está habilitado no servidor NAS, você pode criar file systems habilitados para SMB. O servidor NAS com suporte para SMB pode ser independente ou associado a um domínio do Active Directory. Por padrão, os servidores NAS associados a um domínio são colocados em uma unidade organizacional OU=Computers, OU=EMC NAS Servers.

NOTA: O acesso do client usando o protocolo SMB1 é desativado por padrão, devido a possíveis vulnerabilidades de segurança. Se o acesso do client usando SMB1 for necessário, será possível ativá-lo modificando o parâmetro `cifs.smb1.disabled`. Recomenda-se a utilização no mínimo do SMB2 para proporcionar maior segurança e eficiência.

Os file systems e compartilhamentos SMB têm as seguintes opções avançadas de protocolo:

NOTA: Estas opções, com exceção de Oplocks ativados, ficam desabilitadas por padrão.

Tabela 1. Opções avançadas do protocolo SMB

Opção de protocolo	Nível
Gravação síncrona ativada	File system
Oplocks ativados	File system
Notificar durante gravação ativada	File system
Notificar durante acesso ativada	File system
Disponibilidade contínua	Compartilhamento
Criptografia do protocolo	Compartilhamento
Enumeração com base em acesso	Compartilhamento
Branch Cache habilitado	Compartilhamento
Disponibilidade off-line	Compartilhamento

Considerações sobre planejamento

Analise as seguintes informações antes de configurar servidores NAS e file systems:

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

Redes do servidor NAS

Configure o seguinte antes de configurar servidores NAS com o protocolo SMB:

1. Configure um ou mais servidores DNS.

2. Se você estiver associando o servidor NAS ao AD (Active Directory), configure pelo menos um servidor NTP no sistema de armazenamento para sincronizar a data e a hora. É recomendável configurar pelo menos dois servidores NTP por domínio para evitar um ponto único de falha.

   NOTA: O NTP é configurado durante a criação do AD.

3. Crie uma conta de domínio no Active Directory.

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.

Sobre esta tarefa

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.

Etapas

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

Sobre esta tarefa

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.

Etapas

1. Selecione **Portas de hardware** > .
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 **Create**.

   PowerStore O Manager cria automaticamente um nome para a rede à prova de falhas usando o 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 gerenciador no nó A será denominada 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 do servidor NAS no PowerStore Manager. Consulte Criar um servidor NAS para o file system SMB.

Criando compartilhamentos SMB

Faça o seguinte para poder criar compartilhamentos SMB no PowerStore:

1. Criar servidores NAS com protocolo SMB
2. Criar um file system para compartilhamentos SMB

Recursos de documentação

Consulte o seguinte para obter mais informações:

Tabela 2. Recursos de documentação

Documento	Descrição	Local
Guia de sistema de rede do PowerStore T e Q para Storage Services	Contém informações sobre planejamento e configuração de rede.	dell.com/powerstoredocs
Guia de configuração de NFS do PowerStore	Contém as informações necessárias para configurar o recurso de exportações NFS com o PowerStore Manager.	
White paper de recursos de arquivo do PowerStore	Aborda os recursos, a funcionalidade e os protocolos compatíveis com a arquitetura de arquivo do Dell PowerStore.	
Ajuda on-line do PowerStore	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 em arquivo no cluster do PowerStore, um servidor NAS precisa estar em execução no sistema. Um servidor NAS é um servidor de arquivos que dá suporte ao protocolo SMB, ao protocolo NFS ou a ambos para compartilhar dados com os clients do host. 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 SMB, onde é possível criar file systems com compartilhamentos SMB.

Criar um servidor NAS para file systems SMB

Crie um servidor NAS antes de criar file systems.

Pré-requisitos

Obtenha as seguintes informações:

- Porta de rede, endereço IP, máscara de sub-rede/comprimento de prefixo, informações de gateway do servidor NAS.

  NOTA: O endereço IP e a máscara de sub-rede/comprimento de prefixo são obrigatórios.

- Identificador de VLAN, se a porta de switch der suporte à marcação de VLAN.

  NOTA: Não é possível reutilizar VLANs que estão sendo usadas para as redes de gerenciamento e armazenamento.

- Se você estiver configurando um servidor NAS independente, obtenha o grupo de trabalho e o nome NetBIOS. Em seguida, defina o que usar para o administrador local independente da conta do servidor SMB.
- Se você estiver associando o servidor NAS ao AD (Active Directory), certifique-se de que o NTP esteja configurado em seu sistema de armazenamento. Em seguida, obtenha o nome do sistema SMB (usado para acessar compartilhamentos de SMB), o nome de domínio do Windows e o nome de usuário e a senha de um administrador do domínio ou um de usuário do domínio que tenha um nível de acesso suficiente para associar ao AD.

Etapas

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

Tela Wizard	Descrição
Detalhes	• Nome do servidor NAS • Descrição do servidor NAS

Tela Wizard	Descrição
	• 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). **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. • Informações de rede - endereço IP, máscara de sub-rede, gateway e ID da VLAN **NOTA:** Não é possível reutilizar VLANs que estão sendo usadas para as redes de gerenciamento e armazenamento. • 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. **NOTA:** Essa opção não é aplicada para comunicação iniciada pelo servidor NAS.
Protocolos de compartilhamento	**Selecione o protocolo de compartilhamento** Selecione **SMB**. **NOTA:** Se você selecionar tanto o protocolo SMB quanto o NFS, habilitará automaticamente o servidor NAS para dar suporte a vários protocolos. A configuração multiprotocolo não está descrita neste documento. **Configurações do Windows Server** Selecione **Independente** para criar um servidor SMB independente ou **Ingressar no domínio do Active Directory** para criar um servidor SMB membro do domínio. Se você associar o servidor NAS ao AD, opcionalmente, selecione **Avançado** para alterar o nome padrão do NetBios e a unidade organizacional. **DNS** Se você selecionou **Join to the Active Directory Domain**, é obrigatório adicionar um servidor DNS. Opcionalmente, habilite o DNS se quiser usar um servidor DNS para seu servidor SMB independente. **Mapeamento do usuário** A página **User Mapping** será exibida se você tiver optado por ingressar no domínio do Active Directory. Mantenha o padrão **Enable automatic mapping for unmapped Windows accounts/users**, para oferecer suporte à associação ao domínio do Active Directory. O mapeamento automático é necessário ao ingressar no domínio do Active Directory.
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**.
   A janela **Status** é aberta, e você é redirecionado para a página **Servidores NAS** depois da criação do servidor.

Próximas etapas

Depois de criar o servidor NAS para SMB, você pode continuar a definir as configurações do servidor ou criar file systems.

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

Alterar as configurações do servidor NAS

Depois de criar um servidor NAS, você pode fazer alterações na configuração dele.

Sobre esta tarefa

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.

Etapas

1. Selecione **Storage** > **NAS Servers** > **[nas server]**.
2. Na página **Network**, você pode configurar as interfaces de rede ou as rotas para redes externas, conforme descrito em Configurar redes de servidor NAS.
3. Na página **Naming Services**, você tem a opção de adicionar, modificar ou excluir servidores DNS do servidor NAS.

   NOTA: Não é possível desabilitar o DNS para servidores NAS compatíveis com o compartilhamento de arquivos SMB e que estão associados a um AD (Active Directory).

4. Na página **Protocolos de compartilhamento**:
   - Selecione o cartão **Servidor SMB** para ativar ou desativar o suporte a compartilhamentos do Windows ou para alterar o tipo de pesquisa que o servidor SMB usa.

     NOTA: Se você alterar **Windows Server Type** de **Standalone** para **Join to the Active Directory Domain**, será necessário acessar a guia **User Mapping** e selecionar **Enable automatic mapping for unmapped Windows accounts/users**.

   - Selecione o card **FTP** para habilitar ou desabilitar o FTP ou SFTP, alterar as propriedades de FTP ou SFTP, configurar a autenticação de usuário e um diretório base de usuário e para definir as configurações de mensagem de autenticação. Para obter detalhes, consulte Configurar o protocolo de compartilhamento FTP.
   - Selecione **Mapeamento do usuário** para permitir que o servidor use o mapeamento automático para contas/usuários não mapeados do Windows ou a conta padrão para usuários não mapeados de contas do Windows.
5. Na página **Proteção**, ative ou desative o NDMP.

   Para obter detalhes, consulte Habilitar a proteção e eventos de NDMP.
6. Na guia **Proteção e eventos**:
   - Selecione **Kerberos** para adicionar o realm do AD (Active Directory) para autenticação Kerberos ou para configurar um realm Kerberos personalizado.
   - Selecione **Antivirus** para ativar ou desativar o serviço de antivírus e para recuperar ou carregar o arquivo de configuração do antivírus.

   Para obter detalhes, consulte Configurar a segurança do servidor NAS.

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.

Pré-requisitos

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

Sobre esta tarefa

Etapas

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.

Resultados

O servidor NAS selecionado é excluído.

3

Recursos adicionais de servidores NAS

Este tópico contém as seguintes informações:

Tópicos:

Configurar um protocolo de compartilhamento FTP ou SFTP

Você pode configurar o FTP ou FTP sobre SSH (SFTP) depois que o servidor NAS tiver sido criado.

Pré-requisitos

Não há suporte para o modo FTP passivo.

Sobre esta tarefa

O acesso ao FTP pode ser autenticado usando os mesmos métodos que o SMB. Uma vez concluída a autenticação, o acesso é o mesmo que SMB para fins de segurança e permissões. Se o formato for `domain@user` ou `domain\user`, será usada a autenticação SMB. A autenticação SMB usa o controlador de domínio do Windows.

Etapas

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. 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** e digite uma mensagem de boas-vindas padrão e a mensagem do dia.
7. Como opção, exiba a **Access Control List** e adicione uma lista de usuários, grupos e hosts que podem acessar o FTP ou que têm acesso negado.
8. Selecione **Aplicar**.

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.

Sobre esta tarefa

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.

Etapas

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.

Pré-requisitos

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

Sobre esta tarefa

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.

Etapas

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.

Sobre esta tarefa

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

Etapas

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**.

Próximas etapas

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

Restauração redirecionada do NDMP

PowerStore permite que usuários/grupos locais acessem compartilhamentos SMB em um servidor NAS diferente executando um comando para modificar listas de controle de acesso (ACLs).

A restauração de um backup NDMP para um servidor NAS diferente do original pode causar problemas de acesso. Talvez usuários e grupos locais no servidor NAS de destino não consigam acessar compartilhamentos SMB porque as listas de controle de acesso (ACLs) de objetos do file system contêm SIDs (identificadores de segurança) do servidor original.

Para permitir que os usuários/grupos locais do servidor NAS de destino acessem os compartilhamentos SMB após a restauração do servidor NAS, execute o seguinte comando antes de restaurar os file systems:

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

NOTA: O comando é aplicado no nível do servidor NAS.

Configurar a segurança do servidor NAS

Você pode configurar o servidor NAS com segurança de **Kerberos** ou **Antivírus**.

A configuração de segurança do servidor NAS inclui as seguintes opções:

- Kerberos
- Antivírus

Configurar a segurança Kerberos para o servidor NAS

Você pode configurar o servidor NAS com segurança Kerberos.

Sobre esta tarefa

Adicione o servidor SMB ao domínio do AD antes de configurar Kerberos.

Se você estiver configurando o servidor NAS somente para SMB, não precisará de um arquivo keytab. O arquivo keytab só é necessário para a configuração do Secure NFS.

Etapas

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 endereço IP para Kerberos e clique em **Add**.
5. Digite a porta TCP a ser usada para Kerberos. 88 é a porta padrão.
6. Clique em **Apply**.

Noções básicas do Common Anti-Virus Agent (CAVA)

O CAVA (Common Antivirus Agent) fornece uma solução de antivírus a clients que usam um servidor NAS. Ele usa um protocolo SMB padrão do setor em um ambiente do Microsoft Windows Server. O CAVA usa software antivírus de terceiros para identificar e eliminar vírus conhecidos antes que eles infectem os arquivos no sistema de armazenamento.

O software antivírus é importante porque o sistema de armazenamento é resistente à invasão de vírus devido à sua arquitetura. O servidor NAS tem acesso aos dados em tempo real com um sistema operacional incorporado. Não é possível executar programas com vírus neste sistema operacional. Embora o software do sistema operacional seja resistente a vírus, clients Windows que acessam o sistema de armazenamento também necessitam de proteção contra vírus. A proteção contra vírus em clients reduz a possibilidade de os clients armazenarem arquivos infectados no servidor e oferece proteção em caso de abertura de arquivos infectados. Essa solução antivírus consiste em uma combinação de software de sistema operacional, agente CAVA e um mecanismo antivírus de terceiros. O software CAVA e o mecanismo antivírus de terceiros devem ser instalados em um Windows Server no domínio.

Para obter as versões CAVA do CEE exigidas pelo PowerStore, consulte as *Notas da versão do Common Event Enabler* no site Suporte Dell Technologies. Para obter mais informações sobre o CAVA, que faz parte do Common Event Enabler (CEE), consulte *Usando o Common Event Enabler em plataformas Windows*, no site de suporte da Dell Technologies.

Ativar o Common Anti Virus Agent (CAVA)

É possível ativar e configurar o CAVA quando você quer adicionar proteção antivírus aos compartilhamentos SMB.

Pré-requisitos

- Um servidor Windows em execução com um produto A/V compatível. Para obter detalhes, consulte a Matriz de suporte de CEE_CAVA do eLab.
- Instale o aplicativo EMC_CEE_Pack_8_x_x_x 32 ou CAVA de 64 bits no servidor A/V do Windows.

  NOTA: Depois de instalar o aplicativo, acesse o serviço EMC CAVA, seção Log On e atribua uma conta de usuário administrativo do domínio como o usuário antivírus. Em seguida, reinicie o serviço.

- Crie um usuário no Active Directory.
- Verifique se o SMB está habilitado no servidor NAS tem o SMB habilitado.

Sobre esta tarefa

A partir do PowerStore Manager 4.x, é possível configurar o CAVA, atribuir privilégios de verificação de vírus, visualizar a configuração e o status do CAVA e realizar verificações sob demanda do file system usando o PowerStore Manager.

NOTA: Também é possível realizar essas ações usando a CLI e a API REST.

Etapas

1. No PowerStore Manager, vá para a guia **Armazenamento** > **Servidores NAS** > **[servidor nas]** > **Segurança e eventos** > **Antivírus**.
2. Selecione **Configure** para abrir a caixa de diálogo **Configure Antivirus Settings**.
3. Defina os seguintes parâmetros: o endereço IP, as extensões de arquivo que você deseja verificar e as extensões de arquivo que você deseja excluir.
   - IP address — Defina o Endereço IP ou FQDN do servidor A/V do Windows.
   - Extensões de arquivo para verificação — use o seguinte formato: *.txt, *.docx, *.exe.
   - Extensões de arquivo para exclusão — use o mesmo formato dos tipos de arquivo para verificação.
4. Selecione **Opções avançadas** para definir os seguintes parâmetros:
   - Tamanho máximo do arquivo
   - Hora da pesquisa

- Ação de desligamento
- Limite superior da marca d'água
- Limite inferior da marca d'água
- MSRPC User
- Porta HTTP
- Tempo de espera excedido para repetição de RPC
- Tempo de espera excedido para solicitação de RPC

5. Selecione **Criar**.
   O serviço antivírus será marcado como ativo.
6. Selecione o ícone de edição para abrir a caixa de diálogo **Properties**.
7. Selecione **Enable** para ativar a varredura antivírus e, em seguida, **Apply**.
8. Para oferecer ao servidor NAS os direitos de verificação de vírus da EMC, selecione a guia **Privilégios da conta** e adicione a conta de usuário antivírus do domínio. Use o formato Domínio\nome de usuário (por exemplo, Lab\antivírus).

   NOTA: Esta é a mesma conta de usuário selecionada no serviço EMC CAVA no Windows Server.

9. Para visualizar detalhes do software antivírus e o status on-line, selecione a guia **Audit Info**.
10. Na guia **File Systems to be Scanned**, selecione os file systems que você deseja examinar e, em seguida, **Start** para iniciar a varredura.
11. Se quiser que a varredura inclua arquivos off-line, selecione a opção na mensagem exibida e **Start Scan**.
12. Para monitorar o progresso da varredura, selecione a guia **Status**.
13. Após a conclusão da varredura, será exibida uma mensagem indicando o status.
14. Para interromper uma varredura de um file system, selecione o file system, **Stop Scan** e confirme na mensagem exibida.
15. Se você quiser configurar o CAVA usando um arquivo de configuração (viruschecker.conf), poderá fazer download e modificar o arquivo atual ou carregar um novo arquivo de configuração selecionando **Carregar/recuperar configuração** na caixa de diálogo **Propriedades**.

    NOTA: Para obter detalhes sobre os parâmetros do arquivo viruschecker.conf, consulte Parâmetros antivírus configuráveis.

Parâmetros de antivírus configuráveis

A tabela a seguir detalha os parâmetros que podem ser configurados no arquivo de configuração `viruschecker.conf` do CAVA. Você pode criar o arquivo de configuração e, depois, carregá-lo no PowerStore.

Tabela 3. Parâmetros do antivírus

Parâmetro	Descrição	Obrigatório	Exemplo
`addr=`	Define os endereços IP do(s) servidor(es) CAVA.	Sim	`addr=10.205.20.130`
`masks=`	Configura as extensões de arquivo que serão verificadas.	Sim	`masks=*.exe:*.docx:*.com`
`excl=`	Relaciona as extensões de arquivo que serão excluídas durante a verificação.	Não	`excl=pagefile.sys`
`maxsize=<n>`	Inteiro. Define o tamanho máximo de arquivos que serão verificados. Arquivos que excedem esse tamanho não são verificados.	Não	`maxsize=4294967290`
`surveyTime=<n>`	Define o intervalo de tempo (em segundos) para verificar todos os servidores de AV e saber se eles estão on-line ou off-line. Se nenhum servidor de AV responder, o processo de desligamento será iniciado usando o parâmetro de desligamento configurado (consulte a próxima linha).	Não	`surveyTime=600`

Tabela 3. Parâmetros do antivírus (continuação)

Parâmetro	Descrição	Obrigatório	Exemplo
`shutdown=`	Especifica a ação de desligamento quando nenhum servidor está disponível. O valor padrão é `Allow Access`.	Não	`Allow Access`, `Stop_SMB_Access`, `Disable_Virus_Checker`
`highWaterMark=<n>`	Alerta o sistema quando o número de solicitações em andamento excede `highWaterMark`.	Não	`highWaterMark=200`
`lowWaterMark=<n>`	Alerta o sistema quando o número de solicitações em processo é menor que `lowWaterMark`.	Não	`lowWaterMark=50`
`msrcpuser=`	Especifica o nome atribuído a uma conta de usuário simples ou uma conta de usuário que faz parte de um domínio que o serviço CAVA está executando na máquina CEE.	Não	Conta de usuário: `msrpcuser=user1` Domínio/conta de usuário: `msrpcuser=CEE1/user1`
`httpport=`	Especifica o número da porta HTTP na máquina CEE que o sistema usa.	Não	`httpport=12228`
`RPCRetryTimeout`	Define o tempo de espera excedido (em milissegundos) de repetição da chamada a RPC.	Não	`RPCRetryTimeout=4000 milliseconds`
`RPCRequestTimeout`	Define o tempo de espera excedido (em milissegundos) da solicitação de RPC. Quando uma chamada a RPC é enviada ao servidor CAVA, se o servidor responde após RPCRetryTimeout, o servidor NAS tenta novamente até atingir RPCRequestTimeout e, então, passa para o próximo servidor CAVA disponível.	Não	`RPCRequestTimeout=20000 milliseconds`
`reference time`	Permite uma verificação na primeira leitura. Se a hora do último acesso de um arquivo for anterior a `reference time`, no acesso, o arquivo será enviado ao antivírus antes que o client receba acesso.	Não	`reference_time=2022-10-27T18:30:00`

4

Criar file systems e compartilhamentos SMB

Este tópico contém as seguintes informações:

Tópicos:

Criar um file system

Um file system deve ser criado no servidor NAS antes que você possa criar um compartilhamento SMB.

Pré-requisitos

Certifique-se de que existe um servidor NAS configurado para dar suporte ao protocolo SMB, como descrito em Configurando servidores NAS.

Etapas

1. Selecione **Storage** > **File Systems** e clique em **Create**.
2. Continue trabalhando no assistente **Create File System**.

Opção	Descrição
Selecionar tipo	Selecione o tipo de file system **Geral**
Selecionar NAS Server	Selecione um servidor NAS habilitado para SMB.
Advanced SMB Settings	Como opção, escolha uma das seguintes opções: • **Gravação síncrona ativada** • **Oplocks ativados** • **Notificar durante gravação ativada** • **Notificar durante acesso ativada** • **Habilitar publicação de eventos SMB** Para obter detalhes, consulte Configurações avançadas de file system para compartilhamentos SMB.
Detalhes do sistema de arquivos	Informe o nome do file system e o tamanho do file system. O tamanho do file system pode ser de 3 GB a 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, o Modelo PowerStore T e o PowerStore modelo Q exibem imediatamente 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.
Retenção em nível de arquivo	Como opção, selecione o tipo de retenção de arquivo: • Empresarial (FLR-E) — protege o conteúdo contra alterações feitas por usuários por meio de CIFS e FTP. Um administrador pode excluir um file system FLR-E que contém arquivos protegidos. • Conformidade (FLR-C) — protege o conteúdo contra alterações feitas por usuários e administradores e cumpre os requisitos da regra 17a-4(f) da SEC. Um file system FLR-C só pode ser excluído quando não contém arquivos protegidos.

Opção	Descrição
	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.
Compartilhamento SMB	Como opção, configure o compartilhamento SMB inicial. Você pode adicionar compartilhamentos ao file system após a configuração inicial do file system. Para obter detalhes sobre as opções de compartilhamento SMB, consulte: Criar um compartilhamento SMB.
Política de proteção	Opcionalmente, forneça uma política de proteção para o file system. O PowerStore é compatível com proteção de armazenamento em arquivo de snapshots e replicação.
Política de QoS de arquivo	Como opção, selecione uma política de QoS de arquivo para o 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.
Resumo	Analise o resumo. Volte para fazer as atualizações necessárias.

3. Clique em **Create File System**.
   O file system é exibido na lista File System e, se você criou um compartilhamento SMB, ele é exibido na lista SMB Share.

Configurações avançadas de file system para SMB

Você pode adicionar configurações avançadas a file systems habilitados para SMB ao criar um file system.

Tabela 4. Configurações avançadas de file system para SMB

Configuração	Descrição
Gravação síncrona ativada	Quando você habilita a opção Gravações síncronas para um file system multiprotocolo do Windows (SMB), o sistema de armazenamento executa gravações síncronas imediatas para operações de armazenamento, independentemente de como o protocolo executa operações de gravação. Habilitar operações de gravações síncronas permite armazenar e acessar arquivos de banco de dados (por exemplo, MySQL) nos compartilhamentos SMB do sistema de armazenamento. Essa opção garante que qualquer gravação feita no compartilhamento seja feita de maneira síncrona e reduz as chances de perda de dados ou de corrupção de arquivo em vários cenários de falha, por exemplo, perda de energia. Por padrão, está opção é desabilitada. **NOTA:** A opção de gravações síncronas pode ter um impacto considerável no desempenho. Isso não é recomendado, a menos que você pretenda usar file systems do Windows para fornecer armazenamento para aplicativos de banco de dados.
Oplocks ativados	(Habilitado por padrão) Os bloqueios de arquivos oportunistas (oplocks, também conhecidos como oplocks de nível 1) permitem que os clients SMB armazenem file data em buffer localmente antes de enviá-los ao servidor. Os clients SMB podem trabalhar com arquivos localmente e comunicar periodicamente as alterações ao sistema de armazenamento em vez de ter de comunicar cada operação na rede ao sistema de armazenamento. Esse recurso é habilitado por padrão para file systems multiprotocolo do Windows (SMB). A menos que seu aplicativo controle dados críticos ou tenha requisitos específicos que tornem esse modo ou essa operação inviável, é recomendável manter os oplocks habilitados. As seguintes implementações de oplocks são compatíveis: • Oplocks nível II, que informa a um client que vários clients estão acessando um arquivo no momento, mas que nenhum client o modificou ainda. Um oplock nível II permite que o client execute operações de leitura e buscas de atributo de arquivo usando informações locais em cache ou leitura antecipada. Todas as outras solicitações de acesso ao arquivo devem ser enviadas para o servidor.

Tabela 4. Configurações avançadas de file system para SMB (continuação)

Configuração	Descrição
	• Oplocks exclusivo, que informa um client que ele é o único client abrindo o arquivo. Um oplock exclusivo permite que um client realize todas as operações de arquivo usando informações em cache ou de leitura antecipada até que ele feche o arquivo, que é quando o servidor deve ser atualizado com as alterações feitas no estado do arquivo (conteúdo e atributos). • Oplocks em lote, que informa um client que ele é o único client abrindo o arquivo. Um oplock em lote permite que um client execute todas as operações de arquivo usando informações em cache ou de leitura antecipada (incluindo aberturas e fechamentos). O servidor pode manter um arquivo aberto para um client mesmo que o processo local na máquina client tenha fechado o arquivo. Esse mecanismo reduz a quantidade de tráfego de rede permitindo que os clients ignorem as solicitações de abertura e fechamento incorretas.
Notificar durante gravação ativada	Habilite a notificação quando houver gravação para um file system. Por padrão, está opção é desabilitada.
Notificar durante acesso ativada	Habilite a notificação quando um file system for acessado. Por padrão, está opção é desabilitada.
Habilitar publicação de eventos SMB	Habilite o processamento de eventos SMB (Server Message Block) para esse file system.

Criar um compartilhamento SMB

Você pode criar um compartilhamento SMB em um file system que tenha sido criado com um servidor NAS habilitado para SMB.

Etapas

1. Selecione **Storage** > **File System** > **SMB Share**.
2. Clique em **Create** e continue trabalhando no assistente **Create SMB Share**.

Opção	Descrição
Select File System	Selecione um file system que tenha sido habilitado para SMB.
Select a snapshot of the file system	Como opção, selecione um dos snapshots do file system onde o compartilhamento deverá ser criado. Somente os snapshots são compatíveis com as políticas de proteção do file system. A replicação não é compatível com file systems.
SMB Share Details	Digite um nome e um caminho local para o compartilhamento. Ao digitar o caminho local: • Você pode criar vários compartilhamentos com o mesmo caminho local em um único file system SMB. Nesses casos, você pode especificar controles de acesso do host diferentes para usuários diferentes, mas todos os compartilhamentos existentes no file system têm acesso ao mesmo conteúdo. • Deve haver um diretório antes que você possa criar compartilhamentos nele. Se quiser que os compartilhamentos SMB presentes no mesmo file system acessem um conteúdo diferente, você precisará criar primeiro um diretório no host do Windows associado ao file system. Em seguida, você poderá criar os compartilhamentos correspondentes usando o PowerStore. Você também pode criar e gerenciar compartilhamentos SMB no Console de Gerenciamento Microsoft. O PowerStore também criou o caminho de compartilhamento SMB, que usa o host para se conectar ao compartilhamento. O caminho de exportação é o endereço IP do file system e o nome do compartilhamento. Os hosts usam o nome do arquivo ou o caminho do compartilhamento para montar ou associar o compartilhamento a partir de um host da rede.
Propriedades de SMB avançadas	Habilite uma ou mais das configurações de SMB avançadas. • Disponibilidade contínua • Criptografia do protocolo • Enumeração com base em acesso • Branch Cache habilitado

Opção	Descrição
	Decida quais objetos estarão disponíveis quando o compartilhamento está off-line. Para obter detalhes, consulte Propriedades de SMB avançadas.

Próximas etapas

Depois de criar um compartilhamento, você pode modificá-lo no PowerStore ou usando o Console de Gerenciamento Microsoft.

Para modificar o compartilhamento no PowerStore, selecione o compartilhamento na lista na página **SMB Share** e clique em **Modify**.

Propriedades de compartilhamento SMB avançadas

Você pode configurar as seguintes propriedades avançadas de compartilhamento SMB ao criar um compartilhamento SMB ou alterar suas propriedades:

Tabela 5. Propriedades de SMB avançadas

Opção	Descrição
Disponibilidade contínua	Permite o acesso contínuo e transparente dos aplicativos host a um compartilhamento após um failover do servidor NAS no sistema (com o estado interno do servidor NAS salvo ou restaurado durante o processo de failover). **NOTA:** Permita a disponibilidade contínua para o compartilhamento somente quando quiser usar clients de protocolo do SMB 3.0 (Microsoft Server Message Block) com o compartilhamento específico.
Criptografia do protocolo	Permite a criptografia SMB do tráfego de rede no compartilhamento. A criptografia de SMB é aceita por clients SMB 3.0 e posterior. Por padrão, o acesso é negado se um client SMB 2 tenta acessar um compartilhamento com a criptografia de protocolo habilitada. Controle essa opção configurando a chave de registro RejectUnencryptedAccess no servidor não criptografado NAS (o caminho da chave é HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanServer\Parameters\RejectUnencryptedAccess). 1 (padrão) rejeita o acesso e 0 permite que os clients não compatíveis com criptografia acessem o file system sem criptografia.
Enumeração com base em acesso	Filtra a lista de arquivos e diretórios disponíveis em um compartilhamento para incluir apenas aqueles aos quais o usuário solicitante tem acesso de leitura. **NOTA:** Os administradores sempre podem listar todos os arquivos.
Branch Cache habilitado	Copia conteúdo do compartilhamento, armazenando-o em filiais. Isso permite que os computadores client nas filiais acessem localmente o conteúdo em vez de usar a WAN. O BranchCache é gerenciado a partir de hosts da Microsoft.
Disponibilidade off-line	Configura o armazenamento em cache no client de arquivos off-line: • **None**: No lado do client, o armazenamento em cache de arquivos off-line não está configurado (padrão). • **Manual**: os arquivos são armazenados em cache e disponibilizados off-line apenas quando o armazenamento em cache é explicitamente solicitado. • **Programs**: Todos os arquivos que os clients abrem no compartilhamento ficam automaticamente disponíveis off-line. Os arquivos executáveis que anteriormente eram armazenados em cache localmente são executados a partir da cópia em cache mesmo quando o compartilhamento está disponível. • **Documents**: Todos os arquivos que os clients abrem no compartilhamento ficam automaticamente disponíveis off-line. Quando um usuário acessa um arquivo de um compartilhamento, o conteúdo é automaticamente armazenado em cache para ficar disponível ao usuário no modo off-line. Todos os arquivos abertos continuarão sendo armazenados em cache e disponíveis para acesso off-line até que o cache fique cheio. O conteúdo em cache continua sendo sincronizado com a versão do servidor. Os arquivos que não foram abertos não estarão disponíveis off-line.

Gerenciar ACLs

O client Windows define e modifica as permissões de acesso dos compartilhamentos SMB (conhecidas como listas de controle de acesso ou ACLs) usando o console do MMC. Agora você pode gerenciar ACLs de compartilhamentos de SMB no cluster SDNAS diretamente do PowerStore, usando a interface do usuário ou a API REST.

NOTA: Para obter detalhes sobre como usar a API REST para definir ACLs, consulte o *Guia de referência da API REST do Dell PowerStore*, em dell.com/powerstoredocs.

NOTA: As permissões de acesso de arquivos e diretórios nos compartilhamentos de SMB só podem ser gerenciadas usando o client do Windows.

Para abrir a tela Lista de controle de acesso usando o PowerStore Manager, selecione **Armazenamento** > **File Systems** > **Compartilhamentos de SMB** > **[Compartilhamento de SMB]** > **Mais ações** > **Lista de controle de acesso**.

A tela Lista de controle de acesso exibe a lista das entradas de controle de acesso (ACEs) definidas para o SMB selecionado. Para cada ACE, o nome ou ID do trustee, o nível de acesso e o tipo de acesso são listados. Você pode filtrar a lista por qualquer um dos atributos.

NOTA: O ACE padrão concede permissão total a todos.

Na caixa de diálogo Lista de controle de acesso, é possível:

- Adicionar um ACE — Para obter detalhes, consulte Adicionar uma entrada de controle de acesso.
- Modificar um ACE — Edite qualquer um dos campos do ACE selecionado.
- Excluir o ACE selecionado.
- Atualizar a ACL (em **Mais ações**) — Use esta opção se você tiver modificado a ACL usando o console MMC do Windows ou a API REST. A opção Atualizar incorpora as alterações na ACL.

Adicionar uma entrada de controle de acesso

Sobre esta tarefa

Uma entrada de controle de acesso consiste nos seguintes atributos:

- Tipo de trustee — Usuário, grupo, identificador de segurança (SID) ou WellKnown
- ID/nome do trustee — O formato deste campo é determinado de acordo com o tipo de trustee:
  - Nome de usuário — Nome de usuário/domínio
  - Nome do grupo — Nome do grupo/domínio
  - SID — Formato do SID (por exemplo, S-1-2-34-567890123-456789012-3456789012-34)
  - WellKnown — Por exemplo, "Everyone"
- Nível de acesso — Leitura, alteração ou total
- Tipo de acesso — Permitir ou negar

Etapas

1. Selecione **Armazenamento** > **File Systems** > **Compartilhamentos de SMB** > **[Compartilhamento de SMB]** > **Mais ações** > **Lista de controle de acesso**.
2. Na janela **Lista de controle de acesso**, selecione **Adicionar ACE**.
3. Defina os campos de ACE e clique em **Salvar**.
   Uma nova ACE é adicionada à ACL.
4. Clique em **Apply** para salvar as alterações.

5

Mais recursos de file system

Este tópico contém as seguintes informações:

Tópicos:

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

Pré-requisitos

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.

Etapas

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 um file system.

NOTA: É possível modificar os parâmetros do período de retenção posteriormente.

Modificar a retenção em nível de arquivo

Sobre esta tarefa

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.

Etapas

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**.

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 6. Tipos de cota

Type	Descrição
Cotas de usuário	Limita o volume de armazenamento que um usuário individual consome ao armazenar dados no file system.

Tabela 6. Tipos de cota (continuação)

Type	Descrição
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: • 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. • Controlar o uso do diretório configurando os limites fixos e flexíveis de cota de árvore para 0 (zero). **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 7. Limites flexíveis e rígidos

Type	Descrições
Fixo	Um limite rígido é um limite absoluto no uso de armazenamento. 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. O usuário tem permissão para usar o espaço até que um período de tolerância tenha sido atingido. 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.

Etapas

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.

Pré-requisitos

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.

Etapas

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

Sobre esta tarefa

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.

Etapas

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.

Etapas

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)

Sobre esta tarefa

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

Etapas

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

Sobre esta tarefa

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.

Etapas

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.

Pré-requisitos

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

Etapas

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

Pré-requisitos

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

Etapas

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

Sobre esta tarefa

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).

Etapas

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

Etapas

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

Sobre esta tarefa

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

Etapas

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.

Resultados

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

Pré-requisitos

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

Sobre esta tarefa

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.

Etapas

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

Sobre esta tarefa

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.

Etapas

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. • 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:
	  ○ Ignorar (padrão) — Suponha que todos os eventos sejam confirmados.
	  ○ Negar — Negue eventos que exijam aprovação até que os servidores CEPA estejam on-line.
	• Política de falha de eventos posteriores — Selecione o comportamento desejado quando todos os servidores CEPA estiverem off-line para eventos posteriores:
	  ○ Ignorar (padrão) — Continue operando. Os eventos que ocorrerem enquanto os servidores CEPA estiverem inativos serão perdidos.
	  ○ Acumular — Continue operando e salve eventos em um buffer local (até 500 MB).
	  ○ Garantir — Continue operando e salve eventos em um buffer local (até 500 MB). Negue acesso quando o buffer estiver cheio.
	  ○ Negar — Negue acesso aos file systems quando os servidores CEPA estiverem off-line.
	• HTTP/Microsoft RPC
	• Porta HTTP

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

Ativando um editor de eventos para um servidor NAS

Sobre esta tarefa

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

Etapas

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

Sobre esta tarefa

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

Etapas

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**.