Dell PowerStore

Protegendo seus dados

Versão 4.4

Este conteúdo pode ter sido traduzido com IA. Para mais informações, consulte o link.

Março 2026
Rev. A10

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

Recursos adicionais ... 6

Capítulo 1: Introdução ... 7
- Proteção de dados ... 7
- Snapshots ... 7
- Replication ... 8
- Políticas de proteção ... 9
- Proteção Metro ... 9
- Backup remoto ... 10

Capítulo 2: Sistemas remotos ... 11
- Visão geral ... 11
  - Considerações sobre replicação e metro ... 11
  - Considerações para backup remoto ... 13
- Adicionar uma conexão de sistema remoto para replicação e Metro ... 13
  - Gerar credenciais temporárias para autenticação ... 14
  - Definir a finalidade da rede de armazenamento ... 14
  - Grupos de rede de replicação ... 15
- Usando quadros jumbo com sistemas remotos ... 16
- Adicionar uma conexão de sistema remoto para backup remoto ... 16

Capítulo 3: Snapshots ... 18
- Criar um snapshot ... 18
  - Criar um snapshot de um volume ... 18
  - Criar um snapshot de um file system ... 19
  - Criar um snapshot de uma máquina virtual ... 19
- Criar um clone dinâmico ... 19
  - Criar um clone dinâmico de um volume ouGrupo de volumes ... 20
  - Criar um clone dinâmico de um file system ... 20
  - Criar um clone dinâmico de um snapshot ... 20
- Usando clones para acessar snapshots somente leitura pelos hosts ... 21
- Atualizar um recurso de armazenamento ... 21
  - Atualizar um volume usando um snapshot ... 21
  - Atualizar um volume de um volume relacionado ... 22
  - Atualizar um snapshot de um file system ... 22
  - Atualizar um clone do servidor NAS ... 22
- Restaurar um recurso de armazenamento de um snapshot ... 23
  - Restaurar um volume ou grupo de volumes a partir de um snapshot ... 23
  - Restaurar um file system a partir de um snapshot ... 23
- Snapshots seguros ... 24

Capítulo 4: Políticas de proteção ... 25
- Regras de snapshot ... 25
  - Criar uma regra de snapshot ... 25
- Regras de replicação ... 26

Criar uma regra de replicação....26
Recovery Point Objective....26
Limite de alerta....26
Regras de backup remoto....27
Criar uma regra de backup remoto....27
Criar uma política de proteção....27
Modificar uma política de proteção....28
Atribuir uma política de proteção....28
Atribuir uma política de proteção a um objeto de armazenamento....29
Atribuir uma política de proteção a vários objetos de armazenamento....29
Alterar a política de proteção atribuída a um objeto de armazenamento....29
Cancelar a atribuição de uma política de proteção....30

Capítulo 5: Replicação....31
Replicação assíncrona....31
Replicação assíncrona para bloco....31
Replicação assíncrona para arquivo....32
Replicação síncrona....32
Replicação síncrona para bloco....33
Replicação síncrona para arquivo....33
Pausar uma sessão de replicação....34
Retomar uma sessão de replicação....34
Failover....34
Realizar um teste de failover....35
Failover planejado....36
Failover não planejado....37
Outras considerações sobre replicação....38
Testando a recuperação de desastres para servidores NAS em replicação....38
Clonar um servidor NAS para testes de recuperação de desastres usando endereços IP exclusivos....39
Clonar um servidor NAS para testes de recuperação de desastres usando uma rede isolada com endereços IP duplicados....39
Replicação de Virtual Volumes....41
Pré-requisitos....42
Criar uma sessão de replicação de Virtual Volume....42
Recuperação de máquinas virtuais....43

Capítulo 6: Proteção Metro....44
Pré-requisitos e limitações....44
Configurar a conectividade do host....45
Testemunha do Metro....46
Implementar a Metro witness....46
Configurar a testemunha do Metro....46
Modificação e recuperação de testemunha....47
Monitorar a testemunha....48
Remover a testemunha....48
Testemunha — Cenários de falha....48
Configurar um volume Metro....49
Configurar um grupo de volumes Metro....49
Definir a função Metro....50
Monitorar recursos Metro....50

Pausar um recurso Metro..... 50
Retomar um recurso Metro..... 51
Promover um recurso Metro..... 52
Rebaixar um recurso Metro..... 52
Encerrar um recurso Metro..... 53
Resumo das ações permitidas em um recurso metro..... 53
Usando políticas de proteção com Metro..... 54
Usando QoS com metro..... 54

Capítulo 7: Backup remoto..... 55
Terminologia..... 55
Pré-requisitos e limites..... 55
Recursos de documentação..... 56
Fluxo de trabalho básico de backup remoto..... 56
Estados da sessão..... 56
Gerenciando sessões de backup remoto..... 57
Recursos..... 57
Sessões de recuperação..... 58
Recuperar um snapshot remoto para o mesmo cluster do PowerStore..... 59
Recuperar um snapshot remoto para um outro cluster..... 59
Recuperação — Considerações adicionais..... 59
Sessões de acesso instantâneo..... 60
Criar uma sessão de acesso instantâneo..... 60
Acesso instantâneo — Considerações adicionais..... 61
Alta disponibilidade..... 61
Alertas de backup remoto..... 61

Capítulo 8: Backup NDMP para servidores NAS..... 62
Ativar o backup de NDMP..... 62

Apêndice A: Resumo da replicação..... 63
Resumo da replicação..... 63

Apêndice B: Casos de uso..... 65
Casos de uso de snapshots e clones thin..... 65
Casos de uso de replicação..... 66
Usando réplicas para tempo de inatividade planejado..... 66
Usando réplicas para recuperação de desastres..... 66
Casos de uso de proteção Metro..... 67
Usando Metro para alta disponibilidade..... 67
Usando Metro para balanceamento de carga..... 67
Usando Metro para migração..... 67

Recursos adicionais

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

Introdução

Este tópico contém as seguintes informações:

Tópicos:

- Proteção de dados
- Snapshots
- Replication
- Políticas de proteção
- Proteção Metro
- Backup remoto

Proteção de dados

O PowerStore oferece vários meios para proteger seus dados:

- Local protection — crie snapshots (cópias point-in-time) de volumes, grupos de volumesmáquinas virtuais ou file systems no PowerStore sistema.
- Proteção remota: Replique dados em um sistema remoto ou espelhando os dados usando volumes Metro para fins de redundância em caso de desastre.
- Backup remoto: Faça backup de volumes e grupos de volumes diretamente do PowerStore para um PowerProtect DD.

O PowerStore permite que você crie políticas de proteção personalizadas, que são conjuntos de regras para criação de snapshots, replicação e backup remoto, e as atribua aos recursos de armazenamento. As políticas de proteção aplicam as regras definidas no recurso de armazenamento, proporcionando proteção, remota e backup remoto.

NOTA: As regras de backup remoto podem ser aplicadas somente a volumes e grupos de volumes.

NOTA: Não é possível atribuir políticas de proteção que incluem uma regra de replicação a volumes metro. Consulte Usando políticas de proteção com metro.

NOTA: No PowerStoreOS 3.x e versões posteriores, políticas de proteção não podem ser aplicadas a máquinas virtuais baseadas em volumes virtuais (vVols). Consulte Replicação de Virtual Volumes.

O PowerStore também possibilita configurar o backup padrão para servidores NAS usando NDMP. Para obter detalhes, consulte Habilitar o backup NDMP.

Snapshots

Os snapshots são cópias point-in-time somente leitura dos dados de um volume,Grupo de volumes, máquina virtual ou sistema de arquivos. A criação de um snapshot salva o estado do recurso de armazenamento nesse momento específico. Com snapshots, você pode proteger seus dados localmente e restaurar um recurso de armazenamento a um estado anterior.

Você pode criar snapshots manualmente a qualquer momento. Também pode configurar regras de snapshot como parte de uma política de proteção e atribuí-las aos recursos de armazenamento. O sistema cria automaticamente snapshots do recurso relevante de acordo com o agendamento especificado na política de proteção.

A partir dePowerStore3.5, você pode criar snapshots seguros que não podem ser excluídos manualmente por um administrador ou invasor e são excluídos automaticamente somente quando atingem o tempo de expiração. Os snapshots seguros oferecem um meio adicional de proteção contra ataques de ransomware.

Se ocorrer corrupção de dados ou os dados forem excluídos acidentalmente, você poderá recuperá-los dos snapshots, restaurar o volume ouGrupo de volumesaté o point-in-time em que o snapshot foi criado.

Em file systems, é possível criar dois tipos de acesso a snapshots de arquivo somente leitura: protocolo e .snapshot. O tipo de acesso padrão é protocolo, que pode ser exportado como compartilhamento SMB, exportação NFS ou ambos. Você pode compartilhar e montar

o snapshot em um client como faria com qualquer outro file system. Nos tipos de acesso .snapshot, você pode acessar os arquivos dentro do snapshot a partir do file system de produção no subdiretório `.snapshot` de cada diretório.

Também pode criar snapshots de volumes que sejam consistentes com aplicativos e com a ordem de gravação:

- Snapshots consistentes com a ordem de gravação —PowerStoremantém todas as gravações noGrupo de volumesmembros para fornecer uma cópia point-in-time uniforme e garantir proteção consistente em todos os volumes membro. Você pode gerar snapshots consistentes com a ordem de gravação a partir doPowerStore Manager.
- Snapshots consistentes com aplicativos — Você pode criar snapshots consistentes com aplicativos de um volume ou de umGrupo de volumesusando o AppSync. Quando você cria um snapshot consistente com aplicativos, toda a E/S recebida referente a um determinado aplicativo é desativada enquanto o snapshot está sendo criado.

Para verificar se um snapshot é consistente com aplicativos ou com **a ordem de gravação** , analise as colunas Write-Order Consistent e **Application Consistent** nas tabelas de snapshot de um volume ouGrupo de volumesnaPowerStore Manager.

NOTA: Se você não conseguir ver essas colunas, poderá adicioná-las usando a opção **Mostrar/ocultar colunas da tabela**.

O mapeamento de snapshots para hosts não é compatível emPowerStore. Para permitir que um host conectado acesse um snapshot, você pode criar um clone dinâmico (uma cópia gravável do snapshot com uso eficiente de espaço) e mapeá-lo para um host. É possível atualizar o clone dinâmico a partir de diferentes snapshots usando a operação de atualização.

Para obter detalhes sobre as possíveis operações relacionadas a snapshots que você pode executar, usando oPowerStore Manager, consulte o capítulo Snapshots .

NOTA: Para obter detalhes sobre os limites de snapshot paraPowerStoreconsulte *a matriz de suporte simples do Dell Technologies PowerStore*

Replication

A replicação de dados é um processo no qual os dados são duplicados para um sistema remoto, o que oferece redundância avançada em caso de falha no sistema de produção principal. A replicação minimiza os custos associados ao tempo de inatividade de uma falha no sistema e simplifica a recuperação após um desastre natural ou um erro humano.

PowerStore é compatível com replicação remota assíncrona e síncrona para volumes, servidores grupos de volumesNAS e Virtual Volumes.

NOTA: Se o cluster de replicação tiver vários equipamentos, recomenda-se que a capacidade dos equipamentos remotos seja a mais semelhante possível. Variações significativas na capacidade dos equipamentos remotos podem levar à alocação desequilibrada de sessões de replicação entre os equipamentos, o que pode afetar o desempenho do cluster. Para equilibrar uma alocação incorreta de sessões de replicação em equipamentos remotos, é recomendável executar a migração do volume de destino.

Para configurar a replicação de volumes e grupos de volumes:

1. Crie uma conexão remota entre os sistemas de origem e de destino.
2. Crie uma política de proteção com uma regra de replicação que atenda melhor às necessidades dos negócios.
3. Atribua uma política de proteção ao volume ou grupos de volumes.

Para configurar a replicação de servidores NAS:

1. Configure e mapeie a rede de mobilidade de arquivos.
2. Crie uma conexão remota entre os sistemas de origem e de destino.
3. Crie uma política de proteção com uma regra de replicação que atenda melhor às necessidades dos negócios.
4. Atribua uma política de proteção ao servidor NAS.

NOTA: Não é recomendável modificar a rede de mobilidade de arquivos quando o par do sistema estiver inacessível. Quando o par do sistema estiver ativo novamente, o resultado poderá ser ambos os servidores NAS no modo de produção.

Para configurar a replicação de Virtual Volumes (vVols):

1. Crie uma conexão remota entre os sistemas de origem e de destino.
2. Os procedimentos de criar políticas de proteção e atribuí-las a Virtual Volumes são feitos no vSphere. Consulte Replicação de Virtual Volumes.

Para replicação de volume e arquivo, PowerStore permite que você controle o failover para o sistema remoto e inverta a direção de uma sessão de proteção remota. O failover pode ser necessário nos casos a seguir:

- Se você quiser migrar dados para um novo sistema e passar a trabalhar nele sem perda de dados. Nesse caso, você pode realizar o failover sem perda de dados.
- Quando não há nenhum acesso aos dados no sistema de origem, é possível alternar para o sistema remoto e continuar a trabalhar usando a última cópia de proteção remota point-in-time. No entanto, a perda de dados poderá ocorrer nessa situação porque a cópia mais recente no sistema remoto não inclui alterações de dados realizadas entre o momento em que essa cópia foi criada e a hora em que os dados no sistema se tornaram inacessíveis.
- Quando os dados no sistema de origem estão acessíveis, mas a integridade deles pode estar comprometida. Nesse caso, é recomendável reverter para a cópia de proteção point-in-time mais recente criada antes de os dados serem comprometidos.
- Você pode realizar um teste de failover no recurso de armazenamento de destino para testar a prontidão da recuperação de desastres do sistema.

Para obter informações detalhadas sobre procedimentos relacionados à replicação que você pode realizar, consulte o capítulo Replicação.

Para obter informações detalhadas sobre os limites de replicação sincronizada e não sincronizada, consulte a *Matriz de suporte simples do Dell Technologies PowerStore* na página de documentação do PowerStore.

Políticas de proteção

Uma política de proteção consiste em regras de snapshot, de replicação e de backup remoto que você cria para estabelecer proteção de dados consistente entre recursos de armazenamento. Depois de configurada, a política de proteção pode ser atribuída a recursos de armazenamento novos ou existentes.

Uma política de proteção pode incluir uma regra de replicação, uma regra de backup remoto e até quatro regras de snapshot. Todos os tipos de regra podem fazer parte de várias políticas.

As políticas de proteção gerenciam a criação de snapshots, as sessões de replicação e o backup remoto, com base nas regras que contêm. Você pode criar políticas com várias regras que forneçam diferentes níveis de segurança para suas necessidades de proteção local e remota e atribuir uma política a vários recursos de armazenamento para fornecer proteção idêntica a esses recursos.

Você pode criar ou modificar regras e políticas relevantes de acordo com seus privilégios de usuário.

Se quiser criar uma regra, analise os parâmetros e suas necessidades de negócios junto com um administrador antes de continuar. Isso ajuda a alcançar e manter políticas consistentes no sistema inteiro.

Para obter informações detalhadas sobre procedimentos relacionados a políticas de proteção, consulte o capítulo Políticas de proteção.

Proteção Metro

O metro fornece replicação síncrona bidirecional (ativa/ativa) em doisPowerStoreSistemas. Um volume Metro é exposto usando dois sistemas distintos, normalmente localizados em dois data centers diferentes, a até 96 km (60 milhas) de distância, ou em duas localizações distantes dentro do mesmo data center. Os dois sistemas cooperam para expor um único volume Metro aos hosts de aplicativos fornecendo a mesma imagem e dados da SCSI. Os hosts e o aplicativo percebem os dois volumes físicos hospedados pelos dois sistemas como um volume único com vários caminhos.

A proteção Metro permite maior disponibilidade e prevenção de desastres, balanceamento de recursos entre data centers e migração de armazenamento entre doisPowerStoreSistemas.

Quando você configura um volume Metro, o conteúdo dele é replicado para o sistema remoto. Políticas de proteção são usadas para configurar proteção adicional, como snapshots locais.

Uma sessão metro requer duasPowerStoree, opcionalmente, um serviço witness em execução em um host ou VM independente.

Quando você configura um recurso metro, o sistema do qual o recurso metro é configurado é automaticamente definido como preferencial e o outro é configurado como não preferencial. Quando nenhum serviço de testemunha está configurado ou quando o serviço de testemunha está indisponível, essas funções ajudam a orientar o comportamento do sistema em situações de falha. Quando ocorre uma falha (em um dos sistemas ou na conexão entre eles), a sessão Metro é "interrompida" e o sistema não preferencial para de atender à E/S, enquanto o sistema preferencial fornece acesso ao host.

O serviço de testemunha é um terceiro passivo instalado em um host independente.

NOTA: O serviço de testemunha deve ser implementado em um terceiro domínio de falha, que é separado dos doisPowerStoreSistemas que fazem parte da sessão metro. A instalação do serviço testemunha em um sistema separado garante sua disponibilidade se ocorrer falta de energia nos sistemas metro.

A testemunha observa o status dos dois sistemas. Quando ocorre falha, o witness determina qual sistema permanece acessível aos hosts e continua atendendo às E/Ss. Uma testemunha instalada em um terceiro local oferece proteção contra cenários de falha única.

O Metro alterna entre o uso da testemunha e o uso da função do sistema como meio para a recuperação de situações de falha única (quando a testemunha não está configurada ou está indisponível, a recuperação de uma falha única é feita manualmente).

Para obter um resumo dos atributos Metro e a comparação com a replicação síncrona e assíncrona, consulte o Resumo da replicação.

Backup remoto

O backup remoto possibilita fazer backup de volumes e grupos de volumes diretamente do PowerStore para um PowerProtect DD.

O PowerStore é compatível com backup em um equipamento PowerProtect físico ou em um PowerProtect DD Virtual Edition (DDVE).

Um backup remoto cria o snapshot de um volume ou um grupo de volumes no sistema PowerProtect. Os snapshots criados são consistentes em caso de falhas e não há integração de aplicativos.

Depois que estiverem no PowerProtect DD, os backups poderão ser recuperados para um cluster existente ou novo do PowerStore. Você também pode procurar o conteúdo de um backup no DD usando acesso instantâneo e obter acesso temporário rápido aos snapshots de backup sem recuperá-los para o cluster do PowerStore.

Quando um recurso é submetido a backup pela primeira vez, uma cópia completa é criada. Os backups seguintes são incrementais — Somente as alterações a partir do último backup são copiadas para melhorar a eficiência.

Quando você atribui uma política de proteção que inclui uma regra de backup remoto a um volume ou grupo de volumes, uma sessão de backup remoto é criada. Só é possível criar uma sessão de backup remoto por recurso. As sessões de backup remoto são exibidas na guia **Sessões de backup** da página **Backup remoto**.

O backup remoto é iniciado no PowerStore. O fluxo de trabalho do backup remoto é descrito em Fluxo de trabalho básico do backup remoto.

Uma sessão remota acompanha cada uma das operações (backup, recuperação e acesso instantâneo). Você pode monitorar o andamento da sessão e executar ações nas páginas de sessões remotas.

2

Sistemas remotos

Este tópico contém as seguintes informações:

Tópicos:

- Visão geral
- Adicionar uma conexão de sistema remoto para replicação e Metro
- Usando quadros jumbo com sistemas remotos
- Adicionar uma conexão de sistema remoto para backup remoto

Visão geral

A tabela Sistemas remotos (em **Proteção**) exibe as conexões de sistema remoto configuradas. Na tabela Sistemas remotos, é possível:

- Visualizar informações de sistemas remotos, como o nome e o IP do sistema remoto, o tipo do sistema (de armazenamento ou PowerProtect DD), os recursos compatíveis (visíveis apenas se compatíveis com os dois sistemas) e o status da conexão de dados. A visualização detalhada mostra o status da conectividade IP de todos os iniciadores.
- Para fins de solução de problemas, monitore o status de gerenciamento e conexão de dados.
- Selecione um sistema remoto e, em seguida, selecione **Modificar** para editar seus atributos. Você pode alterar o endereço IP de gerenciamento e a descrição. Para o tipo de conexão TCP, você também pode alterar a latência de rede de uma conexão de sistema remoto.
- Selecione um sistema remoto e, em seguida, selecione **Delete** para removê-lo. Não é possível excluir um sistema remoto nas seguintes instâncias:
  - Quando há sessões ativas de replicação associadas ao sistema remoto.
  - Quando há sessões ativas de backup remoto associadas ao sistema remoto.
  - Quando há uma regra de replicação associada ao sistema remoto.
  - Quando há uma regra de backup remoto associada ao sistema remoto.
  - Quando há sessões Metro.
- Selecione um sistema remoto e clique em **Mais ações** > **Verify and Update** Para verificar e atualizar a conexão com o sistema remoto. A opção Verify and Update detecta alterações nos sistemas locais e remotos e restabelece conexões de dados, levando em consideração as configurações de CHAP (Challenge Handshake Authentication Protocol).
- Para sistemas com o tipo de conexão TCP, selecione um sistema remoto e clique em **Mais ações** > **Gerenciar grupo de rede** Para adicionar, modificar ou excluir grupos de rede.
- Para sistemas remotos PowerProtect DD —
  - Se houver perda de conexão por menos de dez minutos, o sistema remoto se recuperará automaticamente quando a conectividade de rede for restaurada. Se a perda de conexão durar mais de dez minutos, selecione **Mais ações** > **Verify and Update** depois que a conectividade for restaurada, altere o status do sistema remoto para OK.
  - Selecione um sistema remoto e, em seguida, selecione **Mais ações** > **Visualizar detalhes da capacidade** Para visualizar as métricas históricas e de uso desse sistema durante um período selecionado.
  - Se o certificado de um sistema remoto tiver sido renovado, selecione o sistema remoto e, em seguida, selecione **Mais ações** > **Atualizar certificado** Para visualizar e confirmar a atualização do certificado do sistema remoto.
  - Você pode verificar se há problemas de conectividade nas colunas Management/File State e Data Connection da tabela **Remote Systems** .

Considerações sobre replicação e metro

Configure conexões de sistema remoto para replicação e proteção Metro entre dois sistemas, garantindo versões e tipos de conexão compatíveis.

A replicação e a proteção Metro exigem uma conexão de sistema remoto entre doisPowerStoreSistemas. Você deve criar uma conexão de sistema remoto antes de configurar a proteção remota. Para replicação, a conexão de sistema remoto é associada à regra de replicação. Se você estiver usandoPowerStoreManager, você pode criar uma conexão de sistema remoto ao criar uma regra de replicação. Também é possível criar um sistema remoto ao configurar o metro em um volume ou grupo de volumes.

É possível criar uma conexão remota entre sistemas que executem versões diferentes (3.x, 4.x). As versões dos sistemas determinam os recursos compatíveis (tipos de replicação e funcionalidade de proteção remota). Ambos os sistemas devem executar oPowerStoreversão para um recurso nesta versão ser compatível. As seguintes condições para a replicação de objetos de armazenamento devem ser atendidas:

Tabela 1. Replicação de armazenamento - Requisitos

Replication Type	Versões permitidas	Connection Type	Latência de rede	Finalidade da rede de armazenamento (para o tipo de conexão TCP)
Assíncrono — volume	1.x ou posterior	• TCP • FC - Compatível com as versões 4.2 e posteriores	-	Replication
Assíncrono — arquivo	3.x ou posterior	• TCP • FC - Compatível com as versões 4.3 e posteriores	-	Replication
Assíncrono — Virtual Volume	3.x ou posterior	TCP	-	Replication
Metro	3.x ou posterior para suporte a volumes, 4.x ou posterior para suporte a grupos de volumes	• TCP (consulte Pré-requisitos e limitações do Metro) • FC - Compatível com as versões 4.4 e posteriores	Baixa (menos de 5 ms)	Replication
Volume síncrono	4.x ou posterior	• TCP • FC - Compatível com as versões 4.3 e posteriores	Baixa (menos de 5 ms)	Replication
Síncrono — arquivo	4.x ou posterior	• TCP • A replicação síncrona de arquivos usando a replicação metro (com falha automática quando a testemunha é configurada) é compatível com as versões 4.3 e posteriores. • FC - compatível com as versões 4.4 e posteriores.	Baixa (menos de 5 ms)	Replication

- Para o tipo de conexão TCP, verifique se as seguintes condições são atendidas:
  - As redes de armazenamento devem ser configuradas com a finalidade de replicação.
  - A rede deve estar mapeada para pelo menos uma porta.
  - Cada porta deve receber pelo menos dois endereços IP.
- Para replicação usando conexão FC (inclusive metro), todas as conexões FC devem usar switches FC (conexão direta ou ponto a ponto não são compatíveis).
- Não há suporte para modificar o tipo de conexão de dados em um sistema remoto. Para modificar o tipo de conexão de dados, exclua o sistema remoto e crie um novo sistema remoto com o novo tipo de conexão de dados.

  NOTA: Depois de excluir e regenerar o sistema remoto, todos os dados NAS que foram replicados para o sistema remoto se tornam inválidos. Como resultado, todos os dados NAS existentes são copiados para o local remoto. Para replicação de bloco, os dados no local remoto são reutilizados e apenas dados incrementais são copiados para o sistema remoto.

- Os tipos de conexão TCP e FC não podem ser usados simultaneamente para replicar dados entre doisPowerStoreSistemas. É possível replicar dados do sistema A para o sistema B usando o tipo de conexão TCP e do sistema A para o sistema C usando o tipo de conexão FC.

NOTA: Para sistemas remotos com o tipo de conexão TCP, verifique se você configurou a rede de armazenamento com a replicação como finalidade (consulte Definir finalidade do sistema remoto) e a mapeou para pelo menos uma porta.

Considerações para backup remoto

O backup remoto exige uma conexão do sistema remoto entre sistemas PowerStore e PowerProtect DD. A conexão remota está associada a uma regra de backup remoto, e o sistema PowerProtect DD pode ser configurado durante a criação da regra.

Para backup remoto, as seguintes condições devem ser atendidas:

- As redes de armazenamento devem ser configuradas com a finalidade de replicação.
- A rede deve estar mapeada para pelo menos uma porta.
- O sistema PowerStore precisa executar a versão 3.x ou posterior.
- Para obter informações sobre as versões DDOS do PowerProtect suportadas, consulte *Dell Technologies PowerStore Simple Suppport Matrix*.
- A rede de armazenamento do PowerStore precisa ser capaz de se comunicar com a rede de transferência de dados do PowerProtect DD.
- A finalidade da rede de armazenamento deve ser definida como replicação.

Quando existem múltiplas redes de armazenamento com finalidade de replicação, o sistema seleciona uma rede de armazenamento com conectividade máxima ao sistema remoto PowerProtect DD nos seguintes cenários:

- Um sistema remoto é adicionado.
- Verify and Update é executado no sistema remoto.
- A rede de armazenamento é reconfigurada de uma maneira que afeta o sistema remoto PowerProtect DD.

NOTA: Para backup remoto, é recomendável configurar uma rede de armazenamento simétrica dimensionada em todos os equipamentos do cluster.

Adicionar uma conexão de sistema remoto para replicação e Metro

Configurar uma conexão de sistema remoto entre a origem e o destinoPowerStoreSistemas para habilitar a replicação síncrona e assíncrona e a proteção metro.

Pré-requisitos

Antes de criar uma conexão de sistema remoto, verifique se você recebeu os seguintes dados do sistema remoto:

- Endereço IP do sistema
- Credenciais de autenticação do usuário ou credenciais temporárias para conexão ao sistema

Etapas

1. Selecionar **Protection** > **Sistemas remotos**.
2. Na janela **Sistemas remotos**, clique em **Adicionar**.
3. No painel deslizante **Adicionar sistema remoto**, configure estes campos:
   - Tipo de sistema remoto — Selecione **PowerStore**.
   - Endereços IP de gerenciamento
   - Descrição (opcional)
   - Tipo de conexão de dados
     - TCP - Selecionar latência de rede

       NOTA: Se o sistema remoto for usado para replicação síncrona ou Metro, a latência de rede deverá ser definida como baixa.

     - Fibre Channel (SCSI)

       NOTA: Para configurar a replicação via FC, certifique-se de que:
       - As portas para replicação estão configuradas em ambosPowerStore(determine quais portas estão disponíveis para replicação e zoneamento da rede FC.
       - A conectividade de rede é estabelecida entre oPowerStorenas interfaces de gerenciamento.

- Nome de usuário ou ID temporário

4. Clique em **Add**.
5. No painel **Autorização do usuário**, verifique o certificado do sistema remoto e clique em **Confirmar**.

Resultados

A nova conexão de sistema remoto é adicionada à tabela **Remote Systems**. Você pode passar o mouse sobre a coluna **Capability** para visualizar os recursos de proteção remota da nova conexão.

NOTA: Os recursos exibidos são derivados das configurações de rede e das versões de software que estão sendo executadas nos sistemas local e remoto.

Gerar credenciais temporárias para autenticação

Sobre esta tarefa

Quando o CAC/PIV está ativado no PowerStore, a autenticação baseada em um nome de usuário e senha é desativada. Se for necessário informar um nome de usuário e uma senha para autenticação (por exemplo, ao criar uma conexão de sistema remoto), você poderá criar um ID temporário e um segredo usando o PowerStore Manager ou a API REST.

NOTA: As credenciais temporárias expiram após dez minutos.

NOTA: Para usar a API REST para criar as credenciais temporárias, execute o comando generate_temp_credentials.

Para obter detalhes, consulte o *Guia de configuração de segurança do PowerStore* na página da documentação do PowerStore.

Etapas

1. No PowerStore Manager, selecione **Configurações**.
2. Em "Segurança", selecione **Autenticação**.
3. Selecione a guia **Credenciais temporárias**.
4. Clique em **Gerar ID e segredo temporários**.
   Um ID e um segredo temporários são exibidos.

Definir a finalidade da rede de armazenamento

PowerStoreDá suporte à configuração de portas dedicadas ou compartilhadas para replicação e conectividade do host.

Ao criar uma rede de armazenamento, você pode definir a finalidade da rede na etapa **Network Details** do assistente **Create Storage Network** (**Configurações** > **Sistema de rede** > **IPs de rede** > **Armazenamento** > **Criar**).

NOTA: Você pode selecionar uma ou todas as finalidades disponíveis:

- Armazenamento (iSCSI)
- Armazenamento (NVMe/TCP)
- Replication

Para habilitar a replicação ou a proteção Metro entre doisPowerStore, selecione a opção **Replication** .

Para ativar o backup no PowerProtect via TCP, selecione a opção **Replication** .

NOTA: Quando várias redes de armazenamento com vários IPs são configuradas com a finalidade de replicação, a proteção remota pode consumir mais recursos do sistema. Para configurações de rede complexas, é recomendável revisar os requisitos da rede de proteção remota antes de atribuir uma finalidade de replicação.

Para adicionar uma finalidade a uma rede, selecione a rede e, em seguida, selecione **Mais ações** > **Reconfigurar**. Você pode então atribuir a finalidade adicional a portas específicas mapeadas para a rede.

Se uma finalidade estiver habilitada para uma ou mais portas mapeadas para uma rede, você não poderá remover a finalidade dessa rede. Se você quiser remover uma finalidade de uma rede, primeiro desabilite essa finalidade em todas as portas mapeadas para a rede.

Para modificar uma finalidade de uma porta, selecione **Hardware** > **Portas** > **[porta]** > **Mais ações** > **Modificar finalidades atribuídas**. Selecione a rede relevante e, em seguida, selecione ou desmarque as finalidades para adicioná-las ou removê-las da porta, respectivamente.

NOTA: Não é possível remover a finalidade da replicação de uma porta mapeada para uma rede de armazenamento quando há um sistema remoto TCP que esteja usando essa rede.

Quando a rede de armazenamento é selecionada para um mapeamento de porta (na etapa **Mapeamento de equipamento** do assistente **Criar rede de armazenamento**), a finalidade é exibida na coluna "Finalidade atribuída para a porta".

Quando a configuração for concluída, a rede de armazenamento será adicionada à tabela Available Networks e a finalidade será exibida na coluna Purposes.

Para visualizar as redes de armazenamento mapeadas de uma porta e suas finalidades, selecione **Hardware** > **Portas**. A rede de armazenamento mapeada para cada porta é listada na coluna Network Mapped. Se houver mais de uma rede mapeada, o número de redes mapeadas será listado. Selecione o nome da rede ou o número exibido na coluna Network Mapped para exibir a lista de redes mapeadas para a porta.

Grupos de rede de replicação

Cada sistema remoto pode usar diferentes portas e redes de replicação definidas em um grupo de redes de replicação. Um par de sistemas remotos pode usar um ou vários grupos de redes de replicação para tráfego de dados de replicação. Quando você cria uma conexão remota, um grupo de redes de replicação padrão é criado automaticamente para o par de sistemas remotos. O grupo padrão inclui todas as redes que têm uma finalidade de replicação. Você pode adicionar, modificar e excluir grupos de redes de replicação conforme suas necessidades.

Para adicionar, modificar e excluir grupos de redes de replicação, selecione **Protection** > **Remote Systems**. Selecione um sistema remoto na lista e, em seguida, **More Actions** > **Manage Network Groups**.

Para visualizar os detalhes dos grupos de rede configurados para um par de sistemas remotos, selecione o nome do sistema na lista **Remote Systems** (**Protection** > **Remote Systems**) para abrir a janela **Properties** do sistema remoto. A guia Connectivity exibe informações detalhadas sobre a rede de dados de replicação com base na configuração do grupo de rede de replicação.

Adicionar um grupo de redes de replicação

Sobre esta tarefa

Quando você cria um grupo de redes de replicação, a mesma configuração de grupo de redes é criada em ambos os membros do par de sistemas remotos.

NOTA: A configuração do grupo de redes nos dois sistemas PowerStore pode demorar alguns minutos.

Para adicionar um grupo de redes:

Etapas

1. Selecione **Proteção** > **Sistemas remotos** > **[sistema remoto]**.
2. No menu **Mais ações**, selecione **Gerenciar grupos de redes** > **Criar**.
3. Na janela **Criar grupo de redes**, especifique o nome do grupo e selecione as redes locais e remotas nas respectivas listas.
4. Selecione **Aplicar** para criar o grupo.

Modificar um grupo de redes de replicação

Sobre esta tarefa

Talvez você queira mover uma ou mais redes do grupo padrão e formar um grupo separado de redes de replicação de acordo com suas necessidades

Para modificar um grupo de redes de replicação:

Etapas

1. Selecione **Proteção** > **Sistemas remotos** > **[sistema remoto]**.
2. No menu **Mais ações**, selecione **Gerenciar grupos de redes**. A janela **Gerenciar grupos de redes** apresentará os grupos de redes que foram criados para o par de sistemas remotos.
3. Selecione o grupo que você deseja modificar e clique em **Modificar**.
4. Na janela **Modificar grupo de redes**, é possível alterar o nome do grupo e adicionar ou excluir redes locais e remotas do grupo.

5. Quando terminar, selecione **Modificar** para aplicar as alterações.

Excluir um grupo de redes de replicação

Sobre esta tarefa

Para excluir um grupo de redes de replicação:

Etapas

1. Selecione **Proteção** > **Sistemas remotos** > **[sistema remoto]**.
2. No menu **Mais ações**, selecione **Gerenciar grupos de redes**. A janela **Gerenciar grupos de redes** apresentará os grupos de redes que foram criados para o par de sistemas remotos.
3. Selecione o grupo que deseja excluir e clique em **Excluir**.
4. Selecione **Excluir** para confirmar.

Usando quadros jumbo com sistemas remotos

Se você estiver usando quadros jumbo, certifique-se de que eles estão configurados nos dois lados da conexão de sistema remoto (portas do PowerStore e do switch) e em todas as portas entre os dois storage arrays. A disparidade de tamanho da MTU gera uma advertência:

- Ao configurar uma conexão de sistema remoto.
- Ao modificar as configurações da conexão de sistema remoto.
- Ao usar a opção **Verificar e atualizar**.

NOTA: Não é recomendável alterar o tamanho da MTU de uma rede de armazenamento quando há uma sessão de replicação ativa.

NOTA: Se o tamanho da MTU for alterado após a criação do sistema remoto, será obrigatório desativar e ativar (bounce) as portas de rede do switch conectado às portas marcadas para replicação do PowerStore a fim de aplicar a alteração no sistema remoto.

Para alterar o tamanho da MTU:

1. Pause a sessão de replicação.
2. Altere o tamanho da MTU da rede de armazenamento (**Configurações** > **Sistema de rede** > **MTU do cluster**).
3. Execute **Verificar e atualizar** no sistema remoto para confirmar que nenhuma advertência foi emitida.
4. Retome a sessão de replicação.

Adicionar uma conexão de sistema remoto para backup remoto

Configure uma conexão de sistema remoto entre os sistemas PowerStore e PowerProtect DD para ativar o backup remoto.

Pré-requisitos

Antes de adicionar a conexão remota, verifique se você recebeu os seguintes dados do PowerProtect DD:

- Endereço IP do equipamento PowerProtect DD
- Nome da unidade de armazenamento
- Parâmetros de transferência de dados

NOTA: A criação de um sistema remoto com credenciais do usuário inválidas da unidade de armazenamento resulta em perda da conexão de dados. Nesse caso, a coluna Status em **Proteção** > **Sistema remoto** > **[PowerProtect DD]** > **Conectividade** exibe Falha de autenticação. Selecione **Modificar** para o PowerProtect DD e corrija as credenciais inválidas. Para obter mais informações, consulte o artigo 000208506 da base de conhecimento da Dell (Se a senha da conta de usuário do PowerProtect DD for alterada...).

Sobre esta tarefa

NOTA: Você pode adicionar um único equipamento PowerProtect DD ao mesmo cluster do PowerStore várias vezes, usando um ID de unidade de armazenamento diferente a cada vez. Assim, você pode fazer backup de diferentes recursos em diferentes locais em um único sistema PowerProtect DD.

NOTA: Se a unidade de armazenamento for removida do sistema DD, ocorrerá uma perda completa de conexão de dados e as sessões e os snapshots remotos terão que ser limpos. Para obter mais informações, consulte o artigo 000208497 da base de conhecimento da Dell (Se uma unidade de armazenamento for removida do DD...).

Etapas

1. Selecione **Proteção** > **Sistemas remotos**.
2. Na janela **Sistemas remotos**, clique em **Adicionar**.
3. No painel deslizante **Adicionar sistema remoto**, configure estes campos:
   - Tipo de sistema remoto — Selecione **PowerProtect DD**.
   - Endereços IP de gerenciamento
   - Descrição (opcional)
   - Nome de usuário e senha de gerenciamento
   - Nome da unidade de armazenamento
   - Endereço IP, nome de usuário e senha de transferência de dados
4. Defina a opção Ativar criptografia.
   - Quando a criptografia está desativada, a conexão com o PowerStore não usa TLS nem autenticação.
   - Quando a criptografia está ativada, a conexão do PowerStore usa o modo de autenticação de senha bidirecional do DD Boost e negocia o nível de criptografia baseado nas configurações globais de segurança do DD Boost.

   NOTA: É recomendável ativar a criptografia quando o sistema remoto é DDVE na nuvem.
5. Clique em **Add**.
6. No painel **Autorização do usuário**, verifique o certificado do sistema remoto e clique em **Confirmar** para criar a conexão remota.

Resultados

O novo sistema é adicionado à lista **Sistemas remotos**. O tipo de sistema é o PowerProtect DD e o Recurso é Backup remoto.

3

Snapshots

Este tópico contém as seguintes informações:

Tópicos:

- Criar um snapshot
- Criar um clone dinâmico
- Usando clones para acessar snapshots somente leitura pelos hosts
- Atualizar um recurso de armazenamento
- Restaurar um recurso de armazenamento de um snapshot
- Snapshots seguros

Criar um snapshot

Crie um snapshot para salvar o estado de um recurso de armazenamento em um point-in-time específico, permitindo a restauração para um estado anterior.

A criação de um snapshot salva o estado do recurso de armazenamento e todos os arquivos e dados contidos nele em um momento específico. É possível usar snapshots para restaurar todo o recurso de armazenamento a um estado anterior. Você pode criar um snapshot de um volume, Grupo de volumes, file system ou máquina virtual.

Antes de criar um snapshot, considere o seguinte:

- Os snapshots não são cópias completas dos dados originais. Não dependa de snapshots para espelhos, recuperação de desastres ou ferramentas de alta disponibilidade. Como os snapshots são parcialmente derivados de dados em tempo real dos recursos de armazenamento, eles poderão se tornar inacessíveis se o recurso de armazenamento ficar inacessível.
- Embora os snapshots sejam eficientes no espaço, eles consomem a capacidade geral de armazenamento do sistema. Certifique-se de que o sistema tenha capacidade suficiente para acomodar snapshots.
- Ao configurar snapshots, analise a política de retenção de snapshot associada ao recurso de armazenamento. Talvez você queira alterar a política de retenção nas regras associadas ou definir manualmente uma política de retenção diferente, dependendo da finalidade do snapshot.
- Os snapshots manuais criados com PowerStore Manager são mantidos por uma semana após a criação (a menos que configurado de outra forma).
- Se o número máximo de snapshots for atingido, não será possível criar mais nenhum. Nesse caso, para habilitar a criação de novos snapshots, é necessário excluir snapshots existentes.

  NOTA: Para obter informações sobre limites de snapshots, consulte a *Matriz de suporte simples do Dell Technologies PowerStore* na página de documentação do PowerStore.

- Para configurar snapshots seguros (especialmente quando eles são configurados como parte de uma política de proteção local), é recomendável analisar as necessidades de negócios com um administrador antes de continuar. Os snapshots seguros não podem ser excluídos até o final do período de retenção, e é necessário planejar com antecedência para evitar atingir o limite máximo de snapshots. Para obter detalhes sobre snapshots seguros, consulte Snapshots seguros.

Caso você não possa visualizar os snapshots criados para um objeto de armazenamento, adicione a coluna Snapshots à tabela usando a opção **Mostrar/ocultar colunas da tabela**. A coluna Snapshots exibe o número de snapshots criados para cada objeto. Clicar no número abre a janela **Snapshots**, que fornece informações detalhadas de cada snapshot.

Criar um snapshot de um volume

Sobre esta tarefa

Se você deseja criar apenas um snapshot de um volume (e não como parte de uma política de proteção atribuída), use a opção **Criar snapshot**.

NOTA: Você pode usar o mesmo procedimento para criar um snapshot de um grupo de volumes.

Etapas

1. Para abrir a janela **Volumes**, selecione **Armazenamento** > **Volumes**.
2. Clique na caixa de seleção ao lado do volume relevante para selecioná-lo e escolha **Proteger** > **Criar snapshot**.
3. No painel deslizante **Criar snapshot de um volume**, digite um nome exclusivo para o snapshot e defina a **Política de retenção local**.

   NOTA: O período de retenção é definido como uma semana por padrão. É possível definir um período de retenção diferente ou selecionar **Sem exclusão automática** para gerar retenção indefinida.

4. Se você quiser criar um snapshot seguro, defina um período de retenção e selecione a opção **Snapshot seguro**.
5. Clique em **Criar snapshot**.

Criar um snapshot de um file system

Sobre esta tarefa

Se você deseja criar apenas um snapshot de um file system (e não como parte de uma política de proteção atribuída), use a opção **Criar snapshot**.

Etapas

1. Para abrir a janela **File systems**, selecione **Armazenamento** > **File systems**.
2. Clique na caixa de seleção ao lado do file system relevante para selecioná-lo e escolha **Proteger** > **Criar snapshot**.
3. No painel deslizante **Criar snapshot de file system**, digite um nome exclusivo para o snapshot e defina a **Política de retenção local**.

   NOTA: O período de retenção é definido como uma semana por padrão. É possível definir um período de retenção diferente ou selecionar **Sem exclusão automática** para gerar retenção indefinida.

4. Defina o tipo de acesso do snapshot de arquivo.
5. Se a publicação de eventos foi configurada no servidor NAS, você pode selecionar a opção para ativá-la.
6. Clique em **Criar snapshot**.

Criar um snapshot de uma máquina virtual

Sobre esta tarefa

Se você deseja criar um único snapshot de uma máquina virtual (e não como parte de uma política de proteção atribuída), use a opção **Criar snapshot**.

Etapas

1. Para abrir a janela **Máquinas virtuais**, selecione **Computação** > **Máquinas virtuais**.
2. Clique na caixa de seleção ao lado da máquina virtual relevante para selecioná-la e escolha **Proteger** > **Criar snapshot**.
3. No painel deslizante **Criar snapshot de máquina virtual**, digite um nome exclusivo para o snapshot.
4. Opcionalmente, digite uma breve descrição.
5. Clique em **Criar snapshot**.

Criar um clone dinâmico

Clones dinâmicos são cópias graváveis de um snapshot, volume,Grupo de volumes, ou file system que um host pode acessar. Ao contrário de um clone completo, um clone dinâmico é uma cópia com uso eficiente de espaço que compartilha blocos de dados com seu objeto pai e não um backup completo do recurso original. O clone dinâmico pode ser criado diretamente como uma cópia do objeto principal ou por meio de um dos snapshots.

Os clones dinâmicos mantêm o acesso completo de leitura ao recurso original. É possível modificar os dados no clone dinâmico e, ao mesmo tempo, preservar o snapshot original.

Com clones dinâmicos, você pode estabelecer points-in-time hierárquicos para preservar os dados em diferentes estágios de modificações de dados. Se o recurso pai for excluído, migrado ou replicado, o clone dinâmico não será afetado.

NOTA: Se um volume pai for migrado de um equipamento para outro, os clones dinâmicos do volume também serão migrados.

Criar um clone dinâmico de um volume ouGrupo de volumes

Sobre esta tarefa

Você pode executar as seguintes ações em clones dinâmicos de volumes e grupos de volumes:

- Associar clones dinâmicos a diferentes hosts.
- Atualizar o clone dinâmico.
- Restaurar o clone dinâmico a partir de um backup.
- Aplicar políticas de proteção a clones dinâmicos.

Etapas

1. Selecionar **Armazenamento** > **Volumes** ou **Armazenamento** > **Grupos de volumes** para abrir a janela de recursos relevante.
2. Clique na caixa de seleção ao lado do volume relevante ouGrupo de volumese, em seguida, selecione **Reutilizar** > **Criar clone dinâmico**.
3. Na janela deslizante **Create Thin Clone** , faça o seguinte:
   - Digite um nome de clone dinâmico.
   - Digite uma descrição.
   - Defina uma política de QoS.
   - Defina uma política de desempenho (somente para clones dinâmicos criados a partir de volumes).
   - Defina a conectividade do host (somente para clones dinâmicos criados com base em volumes).
   - Defina uma política de proteção.
4. Clique em **Clonar**.

Criar um clone dinâmico de um file system

Sobre esta tarefa

Você pode executar as seguintes ações em clones dinâmicos de volumes e grupos de volumes:

- Associar clones dinâmicos a diferentes hosts.
- Restaurar o clone dinâmico a partir de um backup.
- Aplicar políticas de proteção a clones dinâmicos.

Etapas

1. Selecione **Armazenamento** > **File Systems** para abrir a janela **File Systems**.
2. Clique na caixa de seleção ao lado do file system relevante e selecione **Proteger** > **Clonar file system**
3. Na janela deslizante **Criar clone dinâmico**, defina o nome do clone dinâmico e, opcionalmente, uma descrição
4. Se a publicação de eventos foi configurada no servidor NAS, você pode selecionar a opção para ativá-la.
5. Clique em **Clonar**.

Criar um clone dinâmico de um snapshot

Sobre esta tarefa

Você pode criar um clone dinâmico de um snapshot gerado para um volume, grupo de volumes ou file system.

Etapas

1. Abra a janela relevante do recurso de armazenamento.
2. Clique em um recurso para abrir a janela Overview correspondente.

3. Clique na guia **Proteção**.
4. Clique em **Snapshots** para visualizar a lista de snapshots criados para o recurso.
5. Escolha um snapshot na tabela e selecione **Mais ações** > **Criar clone dinâmico usando snapshot**.

Usando clones para acessar snapshots somente leitura pelos hosts

Não há suporte no PowerStore para mapear e cancelar o mapeamento de snapshots em bloco para hosts. Para permitir que um host conectado acesse um snapshot, crie um clone dinâmico do snapshot e associe-o ao host. Depois de criar o clone dinâmico, você pode usar a operação de atualização para atualizá-lo a partir de diferentes snapshots. Para obter mais informações, consulte Atualizar um recurso de armazenamento.

Os snapshots em arquivo podem ser montados nos hosts diretamente (para permitir acesso somente leitura) ou por meio da criação de um clone dinâmico (para permitir acesso de leitura e gravação). Para montar o file system diretamente, os snapshots podem ser exportados como compartilhamento SMB ou exportação NFS.

Você pode exportar snapshots usando um dos seguintes tipos de acesso:

- Protocolo — O snapshot é exportado com um novo nome de compartilhamento.
- .snapshot — No UNIX/Linux, você pode ver o snapshot no diretório .snapshot do file system e, no Windows, clicando com o botão direito no file system e selecionando a opção **Versão anterior**.

Atualizar um recurso de armazenamento

A operação de atualização é usada para substituir o conteúdo de um recurso de armazenamento pelo conteúdo de um recurso relacionado (um clone ou um snapshot secundário indireto). É possível criar uma duplicata do ambiente de produção para várias finalidades (como teste e desenvolvimento, geração de relatórios etc.). Para manter o ambiente duplicado atualizado, use um recurso de armazenamento que inclua as alterações recentes.

É possível usar a operação de atualização nos seguintes cenários:

- Atualizar um clone dinâmico a partir do volume base.
- Atualizar um recurso de armazenamento ou clone dinâmico a partir de outro clone dinâmico na família.
- Atualizar um recurso de armazenamento ou clone dinâmico a partir do snapshot de um volume base ou clone dinâmico relacionado.

É possível atualizar o snapshot de um file system diretamente com o file system principal correspondente.

Se você atualizar o clone dinâmico de um snapshot que tem snapshots derivativos, esses snapshots permanecerão inalterados e a hierarquia da família continuará intacta. Se você atualizar um Grupo de volumes, a imagem point-in-time em todos os volumes de membros também será atualizada.

Ao atualizar um recurso a partir de um snapshot que foi replicado de um sistema remoto, verifique os valores de hora de criação e hora dos dados de origem para ter certeza de que está usando o snapshot correto. O valor de **Hora dos dados de origem** dos snapshots replicados reflete a hora dos dados de origem, e o valor de **Hora de criação** é atualizado com a hora da replicação.

NOTA: Como a operação de atualização substitui o conteúdo de um recurso de armazenamento, é recomendável obter um snapshot do recurso antes de atualizá-lo. A criação de um backup permite reverter para um point-in-time anterior.

Antes de atualizar snapshots, é obrigatório desligar o aplicativo, desmontar o volume ou o file system que está em execução no host de produção e esvaziar o cache do host para evitar a corrupção dos dados durante a operação de atualização.

Atualizar um volume usando um snapshot

Sobre esta tarefa

Para atualizar um volume usando um snapshot:

Etapas

1. Abra a janela da lista de volumes.
2. Clique no volume em que o snapshot foi obtido para abrir a janela de visão geral correspondente.
3. Clique na guia **Proteção** e depois em **Snapshots**.

4. Na lista de snapshots, selecione aquele que você deseja usar para a operação de atualização.
5. Clique em **Mais ações** > **Atualizar usando snapshot**.
6. No painel deslizante **Atualizar usando snapshot**, selecione o volume ou o clone que deseja atualizar na lista suspensa **Volume que está sendo atualizado**.
7. Indique se você deseja criar um snapshot de backup para o volume atualizado (a opção é selecionada por padrão).
8. Clique em **Atualizar**

Atualizar um volume de um volume relacionado

Sobre esta tarefa

É possível atualizar um volume usando um volume relacionado (um clone ou um snapshot filho indireto).

Etapas

1. Abra a janela da lista de volumes
2. Selecione um volume e, em seguida, selecione **Realocar** > **Atualizar usando um volume relacionado**.
3. No painel deslizante **Atualizar usando um volume relacionado**, clique no botão **Selecionar volume a atualizar em** e selecione o volume de origem.
4. Clique em **Atualizar**.

Atualizar um snapshot de um file system

Sobre esta tarefa

É possível atualizar um snapshot de um file system diretamente com o file system principal correspondente.

Etapas

1. Abra a janela de lista de file systems.
2. Selecione o file system do qual o snapshot foi obtido para abrir a respectiva janela Visão geral.
3. Clique na guia **Proteção** e depois em **Snapshots**.
4. Na lista de snapshots, selecione aquele que você deseja usar na operação de atualização.
5. Clique em **Mais ações** > **Atualizar usando snapshot**.
6. Clique em **Atualizar**.

Atualizar um clone do servidor NAS

Atualize o servidor NAS clonado com os dados mais atualizados da origem sem precisar criar um clone.

Pré-requisitos

Quando um servidor NAS de origem passa por alterações significativas de configuração e dados, o servidor NAS clonado deve ser atualizado com as alterações. A partir do PowerStore 4.4, você pode atualizar um clone do servidor NAS com as alterações feitas no servidor de origem.

Um clone do servidor NAS não pode ser atualizado quando:

- O clone não tem uma origem válida (você pode localizar a origem do clone usando o**Origem do servidor NAS**na tabela **NAS Servers** .
- O clone contém um ou mais file systems que não existem no host (file systems órfãos).
- A origem ou o clone contém file systems habilitados para FLR.
- O servidor NAS faz parte do processo de movimentação do NAS ativo.

Se um novo file system foi criado na origem, ele é duplicado para o destino durante a atualização.

Se um file system for excluído do servidor NAS de origem ou um novo file system for criado no servidor NAS clone, a atualização do clone apresentará falha. Para atualizar o clone, é necessário excluir os file systems órfãos e reiniciar a operação de atualização. Você

pode localizar os file systems órfãos selecionando o servidor NAS clone na tabela **NAS Servers** e, em seguida, selecionando**Reutilizar** > **Visualizar sistemas de arquivos órfãos**.

NOTA: Alterações de configuração diferentes de nomes e IPs de SMB e NFS não são sobregravadas como parte da operação de atualização.

NOTA: As políticas de QoS não são atualizadas da origem para o clone.

Sobre esta tarefa

Para atualizar um clone do servidor NAS:

Etapas

1. Abra a janela **NAS Servers** .
2. Selecione um clone do servidor NAS e, em seguida, selecione**Reutilizar** > **Atualizar clone**.

Resultados

O servidor NAS clone é atualizado com dados do servidor NAS de origem e a hora e a data de atualização são atualizadas no**Última atualização**na tabela **NAS Servers** .

Restaurar um recurso de armazenamento de um snapshot

A operação de restauração é usada para reconstruir um ambiente após um evento que pode ter comprometido dados. Você pode usar a operação de restauração para substituir o conteúdo de um recurso de armazenamento principal por dados de um snapshot filho direto. A restauração redefine os dados do recurso de armazenamento pai para o point-in-time no qual o snapshot foi obtido.

Antes de restaurar snapshots, é obrigatório desligar o aplicativo, desmontar o file system que está em execução no host de produção e realizar flush no cache do host para impedir a corrupção dos dados durante a operação de restauração.

Se você restaurar um Grupo de volumes, todos os volumes de membros serão restaurados para o point-in-time associado ao snapshot de origem.

Ao restaurar um recurso a partir de um snapshot que foi replicado de um sistema remoto, verifique o valor de hora dos dados de origem para se certificar de que está usando o snapshot correto.

Restaurar um volume ou grupo de volumes a partir de um snapshot

Sobre esta tarefa

NOTA: Para evitar problemas de integridade dos dados, antes de restaurar um volume, é obrigatório desligar os aplicativos que estão usando o volume e mantê-lo off-line no host.

Etapas

1. Marque a caixa de seleção ao lado do volume ou grupo de volumes que você deseja restaurar.
2. Selecione **Proteger** > **Restaurar de um snapshot**.
3. No painel deslizante **Restaurar volume do snapshot**, selecione o snapshot a ser usado para a operação de restauração.
4. Indique se você deseja criar um snapshot de backup do volume ou grupo de volumes restaurado (a opção é selecionada por padrão).
5. Clique em **Restaurar**.

Restaurar um file system a partir de um snapshot

Sobre esta tarefa

Antes de dar continuidade à operação de restauração, os aplicativos que usam o file system devem ser desligados e o file system colocado off-line nos hosts para evitar problemas de integridade dos dados.

Etapas

1. Marque a caixa de seleção ao lado do file system que você deseja restaurar.
2. Selecione **Proteger** > **Restaurar de um snapshot**.
3. No painel deslizante **Restaurar file system do snapshot**, selecione o snapshot a ser usado na operação de restauração.
4. Indique se deseja criar um snapshot de backup do file system restaurado (a opção é selecionada por padrão).
5. Clique em **Restaurar**.

Snapshots seguros

Não é possível excluir snapshots seguros antes da data de vencimento. Use os snapshots seguros para proteger seus dados contra ataques mal-intencionados.

NOTA: Snapshots seguros são suportados para snapshots de bloco criados para volume ou grupos de volumes e para snapshots de file systems (tanto de protocolo quanto .snapshot).

Com o PowerStore, é possível gerar snapshots seguros. Ao contrário dos snapshots regulares, não é possível excluir manualmente os snapshots seguros. Eles só são excluídos na data de vencimento.

NOTA: Se você quiser usar snapshots seguros, é recomendável analisar as necessidades de negócios com um administrador antes de continuar, para evitar atingir o limite máximo de snapshots.

Os snapshots seguros oferecem proteção contra exclusão acidental ou mal-intencionada de dados de backup e são eficazes contra ataques de ransom. A geração de snapshots seguros garante a restauração de dados para um point-in-time anterior.

Para gerar manualmente um snapshot seguro para um volume, grupo de volumes ou file system, selecione a opção **Secure Snapshot** no painel **Create Snapshot**. Para gerar snapshots seguros como parte de uma política de proteção local, crie uma regra de snapshot e selecione a opção **Snapshot seguro** no painel **Criar regra de snapshot**. Adicione a coluna **Secure Snapshots Enabled** à tabela **Snapshot Rules** para visualizar quais regras geram snapshots seguros.

NOTA: Certifique-se de definir um período de retenção para os snapshots seguros. A opção de snapshot seguro não está disponível quando **Sem exclusão automática** está selecionada.

NOTA: Quando um snapshot de grupo de volumes é configurado como seguro, todos os membros do grupo são definidos como seguros.

Você pode visualizar e monitorar snapshots seguros adicionando a coluna Snapshots seguros à tabela Snapshots. Você também pode filtrar listas de snapshots seguros.

É possível transformar snapshots atuais sem segurança em seguros selecionando a opção **Snapshot seguro** no painel **Detalhes do snapshot**. Da mesma forma, você pode transformar uma regra de snapshot sem segurança em seguro selecionando a opção **Snapshot seguro** no painel **Propriedades** da regra de snapshot.

NOTA: Somente snapshots criados pela regra depois da modificação são seguros. Os snapshots criados antes disso permanecem sem segurança.

Quando uma regra de snapshot seguro é excluída ou removida de uma política, ou quando uma política que inclui uma regra de snapshot seguro não é atribuída a um recurso, os snapshots seguros que foram criados pela regra permanecem seguros e não é possível exclui-los antes do vencimento. Objetos de armazenamento que possuem snapshots seguros não podem ser excluídos até que os snapshots expirem.

Não é possível reduzir o tempo de validade dos snapshots, apenas modificar para uma data e hora posteriores.

Snapshot seguro e replicação:

- Para clusters executando o PowerStoreSO 3.5 e posterior, todos os snapshots seguros gerados no sistema local são replicados como seguros para o cluster remoto.
- Se o cluster de destino estiver executando o PowerStoreSO anterior à versão 3.5, os snapshots seguros serão replicados como snapshots regulares nesse cluster. Nesse caso, a regra de snapshot no cluster de destino não é segura. Se ocorrer failover em um cluster executando o PowerStoreSO anterior à versão 3.5, snapshots seguros não serão criados para o recurso de armazenamento.
- Você pode restaurar um snapshot seguro.
- Não é possível atualizar um snapshot seguro.

Após o upgrade do PowerStore para a versão 3.5, snapshots e regras de snapshot atuais sem segurança podem ser modificados para seguros.

Se você tiver que excluir um snapshot seguro que ainda não atingiu o tempo de validade, entre em contato com o suporte da Dell.

4

Políticas de proteção

Este tópico contém as seguintes informações:

Tópicos:

- Regras de snapshot
- Regras de replicação
- Regras de backup remoto
- Criar uma política de proteção
- Modificar uma política de proteção
- Atribuir uma política de proteção
- Cancelar a atribuição de uma política de proteção

Regras de snapshot

É possível criar regras de snapshot para controlar parâmetros como a frequência de criação de snapshots e o período de retenção de snapshots. Você também pode criar regras de snapshot para gerar snapshots seguros. As regras de replicação, junto com as regras de snapshot e backup remoto, permitem configurar e aplicar políticas consistentes de proteção de dados a recursos de armazenamento com base nos requisitos de proteção de dados.

Se você quiser criar uma regra de snapshot além daquelas já existentes, analise as necessidades de negócios junto com o administrador antes de continuar. Isso pode ajudar a alcançar e manter políticas consistentes no sistema inteiro.

Criar uma regra de snapshot

Etapas

1. Selecione **Proteção** > **Políticas de proteção**.
2. Na janela **Políticas de proteção**, clique em **Regras de snapshot** na barra **Proteção**.
3. Na janela **Regras de snapshot**, clique em **Criar**.
4. No painel deslizante **Criar regra de snapshot**, digite um nome para a nova regra.
5. Defina o seguinte:
   - Selecione os dias em que o snapshot será criado.
   - Defina a frequência/hora de início:
     - Para que um snapshot seja obtido em um intervalo fixo, selecione esta opção e defina o número de horas após o qual um snapshot será criado.
     - Para que um snapshot seja obtido em um momento específico dos dias selecionados, escolha a opção **Horário** e defina a hora e o fuso horário.
   - Defina o período de retenção.
   - Para criar snapshots seguros, selecione a opção **Snapshot seguro**. Para obter detalhes sobre snapshots seguros, consulte Snapshots seguros.

     NOTA: É recomendável analisar as necessidades de negócios com um administrador antes de continuar, para evitar atingir o limite máximo de snapshots.

   - Para snapshots de arquivo, selecione o tipo de acesso de snapshot de arquivo.
6. Clique em **Criar**.

Regras de replicação

Uma regra de replicação é um conjunto de parâmetros que o sistema usa para sincronizar dados em uma sessão de replicação. Os parâmetros incluem selecionar um destino de replicação, tipo de replicação e definir um Recovery Point Objective (RPO).

Depois de configurar uma regra de replicação, você pode optar por usá-la em uma política de proteção nova ou existente, o que altera ou aplica automaticamente os parâmetros da sessão de replicação para qualquer recurso de armazenamento que use a política de proteção.

Não é possível alterar uma política de proteção para usar outra regra de replicação com um sistema de destino diferente. Para alterar uma política de proteção com uma regra de replicação usando um sistema remoto diferente, remova a política antiga antes de atribuir uma nova.

NOTA: A alteração de um sistema remoto exige uma sincronização completa.

Se você quiser criar uma regra de replicação além das já existentes, analise os parâmetros e as necessidades de negócios junto com o administrador antes de continuar. Isso pode ajudar a alcançar e manter políticas consistentes no sistema inteiro.

Criar uma regra de replicação

Etapas

1. Selecione **Proteção** > **Políticas de proteção**.
2. Na janela **Políticas de proteção**, clique em **Regras de replicação** na barra **Proteção**.
3. Na janela **Regras de replicação**, clique em **Criar**.
4. No painel deslizante **Criar regra de replicação**, digite um nome para a nova regra.
5. Defina o seguinte:
   - Crie um nome de regra.
   - Selecione um destino de replicação existente ou configure um novo.
   - Selecione o tipo de replicação (assíncrona ou síncrona).

     NOTA: A seleção do tipo de replicação síncrona define os valores de limite de alerta e RPO como zero. Esses valores não podem ser modificados.

   - Se você selecionou o tipo de replicação assíncrona:
     - Defina o RPO.
     - Defina o limite de alerta.
6. Clique em **Create**.

Recovery Point Objective

O RPO (Recovery Point Objective) indica a quantidade de dados aceitável, medida em unidades de tempo, que pode ser perdida em decorrência de uma falha. Ao configurar uma regra de replicação, você pode configurar a sincronização automática com base no RPO. Os valores de RPO possíveis variam de 5 minutos a 24 horas. O valor padrão de RPO é uma hora.

NOTA: Um intervalo de RPO menor oferece maior proteção e consome menos espaço. No entanto, tem maior impacto no desempenho, o que aumenta o tráfego de rede. Um intervalo de RPO mais alto pode resultar em mais consumo de espaço, o que pode afetar os agendamentos de snapshot e os limites de espaço.

Limite de alerta

Ao configurar uma regra de replicação assíncrona, você pode especificar um limite de alerta, que é o tempo que o sistema aguardará antes de gerar um alerta de conformidade quando uma sessão de replicação não atender ao RPO. A definição do limite de alerta como zero significa que os alertas serão gerados caso o tempo real de sincronização exceda o RPO.

Regras de backup remoto

Crie uma regra de backup remoto e adicione-a a uma política para ativar o backup remoto.

Uma regra de backup remoto é um conjunto de parâmetros que permitem ao sistema PowerStore fazer backup de volumes e grupos de volumes em um equipamento PowerProtect DD. A regra especifica o sistema de destino no qual os backups são criados, a frequência da operação de backup e o tempo de retenção dos backups.

NOTA: As regras de backup remoto não são compatíveis com snapshots seguros.

Depois de gerar a regra de backup remoto, adicione-a a uma política de proteção existente ou gere uma nova política.

NOTA: Uma política de proteção pode incluir apenas uma regra de backup remoto.

Criar uma regra de backup remoto

Etapas

1. Selecione **Protection** > **Protection Policies**.
2. Na janela **Políticas de proteção**, clique em **Regras de backup remoto** na barra **Proteção**.
3. Na janela **Regras de backup remoto**, selecione **Criar**.
4. Defina o seguinte:
   - Rule name
   - Destino — Selecione um PowerProtect DD na lista suspensa ou configure um novo sistema (consulte Adicionar uma conexão remota para backup remoto.
   - Dias da semana em que o backup é criado.
   - Frequência/Hora de início — Selecionar **A cada** define a frequência do backup em horas ou dias. Selecionar **Hora do dia** define a frequência de backup em dias.
   - Período de retenção - Selecione a unidade de tempo (horas, dias, meses ou anos) e defina o período para manter os backups gerados.

     NOTA: A retenção máxima é de 70 anos.

5. Clique em **Create**.

Criar uma política de proteção

Sobre esta tarefa

Crie uma política de proteção para fornecer proteção local ou remota para seus recursos de armazenamento. Cada política de proteção pode incluir uma regra de replicação, uma regra de backup remoto e até quatro regras de snapshot. Uma regra pode fazer parte de várias políticas.

Etapas

1. Selecionar **Protection** > **Protection Policies**.
2. Na janela **Políticas de proteção**, clique em **Criar**.
3. No painel deslizante **Criar política de proteção**, digite um nome para a nova política.
4. Como opção, selecione as regras de snapshot que você deseja incluir na política ou crie uma (consulte Criar uma regra de snapshot).
5. Como opção, selecione uma regra de replicação que você deseja incluir na política ou crie uma (consulte Criar uma regra de replicação).
6. Como opção, selecione uma regra de backup remoto que você deseja incluir na política ou crie uma (consulte Criar uma regra de backup remoto).
7. Clique em **Create**.

Resultados

Quando você cria uma política de proteção que inclui uma regra de replicação, a política é replicada automaticamente para o sistema remoto e atribuída aos recursos de destino criados pela política. Os nomes da política replicada e das regras associadas consistem nos nomes da política e das regras no sistema de origem e acrescentados ao nome do sistema remoto. A fim de manter a sincronização, as alterações feitas na política original ou nas regras incluídas são replicadas para o sistema remoto. Após um failover de replicação, a política replicada se torna ativa no sistema de destino.

As políticas e regras replicadas são gerenciadas pelo sistema e não são exibidas nas tabelas de regras e políticas do sistema de destino. No entanto, passando o mouse sobre o nome da política replicada, é possível ver os detalhes das regras na guia **Proteção** dos volumes ou grupos de volumes de replicação. Para políticas de proteção atribuídas a volumes Metro, uma política idêntica somente leitura é criada no sistema remoto e pode ser visualizada na janela **Políticas de proteção** do sistema remotoPowerStoreGerente.

Modificar uma política de proteção

Você pode modificar uma política de proteção adicionando e removendo regras de snapshot, replicação e backup remoto.

Sobre esta tarefa

NOTA: Alterar as configurações de uma política de proteção aplica as novas configurações a todos os objetos aos quais ela está atribuída. Caso você queira alterar a política de proteção de um recurso, é recomendável criar outra política de proteção e atribuí-la ao recurso.

Não é possível alterar o destino de replicação em uma regra de replicação usada em políticas de proteção atribuídas a um ou mais recursos de armazenamento. Para reconfigurar a replicação para um sistema remoto diferente, cancele a atribuição da política de proteção e atribua uma nova com uma regra de replicação diferente. O cancelamento da atribuição de uma política de proteção com uma regra de replicação excluirá a sessão de replicação associada e a atribuição de outra política de proteção criará uma nova, que precisa de uma sincronização completa para o novo destino.

Você pode alterar uma sessão de replicação assíncrona para síncrona (para recursos de bloco) ou alterar uma sessão de replicação síncrona para assíncrona (recursos de bloco e arquivo) modificando a regra de replicação usada na política de proteção.

Etapas

1. Selecione **Proteção** > **Políticas de proteção**.
2. Marque a caixa de seleção ao lado da política relevante e clique em **Modificar**.
3. No painel deslizante **Propriedades**, é possível modificar os seguintes parâmetros:
   - Nome da política
   - Regras de snapshot selecionadas
   - Regras de replicação selecionadas
   - Regras de backup remoto selecionadas
4. Clique em **Aplicar**.

Atribuir uma política de proteção

Atribua uma política de proteção a um ou mais recursos de armazenamento para aplicar a eles as regras de snapshot, replicação e backup remoto na política. A política de proteção realiza automaticamente as operações de snapshot, replicação e backup remoto com base nos parâmetros especificados.

Caso haja uma política de proteção que atenda aos seus requisitos de proteção de dados, você poderá atribuí-la a um recurso de armazenamento a qualquer momento.

É possível atribuir uma política de proteção a um recurso de armazenamento durante a criação de recursos ou em uma fase posterior.

Para proteção de armazenamento em bloco:

- Atribuir políticas de proteção que contenham regras de snapshot, replicação e backup remoto a volumes egrupos de volumes.
- Quando você atribui ao recurso de armazenamento uma nova política de proteção contendo uma regra de replicação, é necessário fazer uma sincronização inicial completa.
- Com o backup remoto, a atribuição de uma política que inclui uma regra de backup remoto a um volume ou a um grupo de volumes cria automaticamente uma sessão de backup remoto no estado ocioso.
- Se uma política que inclui uma regra de backup remoto for atribuída a um recurso não compatível com backup remoto, a regra será ignorada.

- Com volumes Metro, você pode atribuir somente políticas de proteção que incluem regras de snapshot. Não é possível atribuir uma política que inclui uma regra de replicação a um volume Metro. Depois que a política de proteção é atribuída ao volume Metro ou ao grupo de volumes, as regras de política e snapshot são copiadas para o sistema remoto e exibidas nas tabelas Políticas de proteção e Regras de snapshot com um ícone de cadeado, indicando que são somente leitura.

Para proteção de armazenamento em arquivo:

- PowerStoredá suporte à proteção local (snapshots) no nível do file system e à proteção remota (replicação) no nível do servidor NAS.
- Você só pode atribuir uma política de proteção a um servidor NAS se ela inclui uma regra de replicação. A regra de replicação será aplicada a todos os file systems no servidor NAS, e as regras de snapshot (se existirem) serão ignoradas.
- Você só pode atribuir uma política de proteção a um file system se ela inclui uma regra de snapshot. A regra de snapshot será aplicada ao file system, e uma regra de replicação (se existir) será ignorada.
- Você pode atribuir diferentes políticas de proteção a um servidor NAS e aos file systems que ele contém.

Atribuir uma política de proteção a um objeto de armazenamento

Sobre esta tarefa

Atribua uma política de proteção a um volume, grupo de volumes, file system ou servidor NAS.

Etapas

1. Marque a caixa de seleção do recurso de armazenamento ao qual você deseja atribuir uma política de proteção.
2. Para volumes, grupos de volumes e file systems, selecione **Proteger** > **Atribuir política de proteção**. Para servidores NAS, selecione **Mais ações** > **Atribuir política de proteção**.

   NOTA: Se você selecionou um recurso inválido, a opção de atribuição ficará inativa. Passar o mouse sobre **Atribuir política de proteção** mostra uma dica que explica por que ela é inválida para essa ação.

3. No painel deslizante **Atribuir política de proteção**, selecione a política de proteção.
4. Clique em **Aplicar**.

Atribuir uma política de proteção a vários objetos de armazenamento

Sobre esta tarefa

Atribua uma política de proteção a vários objetos de armazenamento do mesmo tipo (volumes, grupos de volumes, file systems ou servidores NAS).

Etapas

1. Selecione **Proteção** > **Políticas de proteção**.
2. Marque a caixa de seleção de uma política na lista e, em seguida, selecione **Mais ações** > **Atribuir política de proteção**.

   O painel deslizante **Atribuir política de proteção** mostra um resumo de todos os recursos de armazenamento que já têm uma política de proteção atribuída.
3. No painel deslizante **Atribuir política de proteção**, selecione o tipo de recurso e, em seguida, selecione os objetos relevantes na lista de recursos.
4. Repita a etapa 3 se quiser atribuir a política selecionada a outros tipos de recursos.
5. Clique em **Atribuir**.

Alterar a política de proteção atribuída a um objeto de armazenamento

Sobre esta tarefa

Considere as seguintes diretrizes para regras de replicação:

- A substituição de uma política de proteção que inclui uma regra de replicação por uma política sem regras de replicação remove a replicação de todos os recursos atribuídos a essa política.

- A substituição de uma política de proteção que inclui uma regra de replicação por uma política que tem a mesma regra de replicação permite reconfigurar a proteção local sem interromper a replicação.
- A substituição de uma política de proteção que inclui uma regra de replicação por uma política com uma regra de replicação diferente só será possível se ambas as políticas tiverem o mesmo sistema remoto configurado.

  NOTA: Para alterar a atribuição de uma política de proteção com uma regra de replicação usando um sistema remoto diferente, remova a política antiga antes de atribuir uma nova.

- Substituir uma política de proteção que inclui uma regra de replicação assíncrona por uma política que inclui uma regra de replicação síncrona pode afetar o desempenho das sessões de replicação de volume e grupo de volumes.

Considere as seguintes diretrizes para regras de backup remoto:

- A substituição de uma política de proteção que inclui uma regra de backup remoto por uma política sem uma regra de backup remoto remove a proteção remota para o sistema remoto do DD.
- A substituição de uma política de proteção que inclui uma regra de backup remoto por uma política que tem a mesma regra de backup remoto faz com que o próximo backup seja completo (e não incremental).
- A substituição de uma política de proteção que inclui uma regra de backup remoto por uma política com uma regra de backup remoto diferente e o mesmo sistema remoto faz com que o próximo backup seja completo (e não incremental).

Etapas

1. Selecione o recurso de armazenamento relevante para abrir a janela **Visão geral** correspondente.
2. Clique na guia **Proteção**.
3. Ao lado do nome da política de proteção atribuída, clique em **Alterar**.
4. No painel deslizante **Alterar política de proteção**, selecione uma política de proteção diferente.
5. Clique em **Aplicar**.

Cancelar a atribuição de uma política de proteção

Sobre esta tarefa

A remoção da política de proteção de um recurso de armazenamento resulta no seguinte:

- Replicação e snapshots agendados, com base nas regras associadas à interrupção da política.
- Os snapshots existentes permanecem e são mantidos no sistema de acordo com as configurações de regra de snapshot quando foram criados.
- O recurso de armazenamento de destino permanece no modo somente leitura. Você pode clonar o recurso de armazenamento de destino para obter uma cópia de leitura/gravação ou alterar o atributo **destino de replicação** na página **Propriedades** do recurso de armazenamento.

NOTA: Não é possível cancelar a atribuição de uma política de proteção durante a importação.

NOTA: O cancelamento da atribuição de uma política de proteção que inclui uma regra de replicação síncrona só pode ser feito no sistema que tem a política de leitura/gravação (e não a cópia somente leitura da política).

Etapas

1. Marque a caixa de seleção do recurso de armazenamento ao qual você deseja atribuir uma política de proteção.
2. Para volumes, grupos de volumes e file systems, selecione **Proteger** > **Cancelar atribuição de política de proteção**. Para servidores NAS, selecione **Mais ações** > **Cancelar atribuição de política de proteção**.
3. Clique **Cancelar atribuição** para confirmar.

5

Replicação

Este tópico contém as seguintes informações:

Tópicos:

- Replicação assíncrona
- Replicação síncrona
- Pausar uma sessão de replicação
- Retomar uma sessão de replicação
- Failover
- Outras considerações sobre replicação
- Testando a recuperação de desastres para servidores NAS em replicação
- Replicação de Virtual Volumes

Replicação assíncrona

No modo de replicação assíncrona, as atualizações no sistema de destino (como alterações no conteúdo, no tamanho e na associação) ocorrem em um intervalo estabelecido com base no RPO definido. Durante a sincronização, o sistema de destino é atualizado com todas as alterações de dados que ocorreram desde o último ciclo de sincronização.

PowerStore dá suporte à replicação remota assíncrona para volumes, grupos de volumes, servidores NAS e Virtual Volumes.

NOTA: A sincronização de volume virtual é compatível apenas com snapshots somente leitura.

Para aplicar a replicação assíncrona a um recurso de armazenamento, atribua ao recurso uma política de proteção que inclua uma regra de replicação assíncrona. A atribuição de uma política de proteção cria uma sessão de replicação que é adicionada à lista de sessões de replicação (**Protection** > **Replication**), e a coluna Replication Type exibe Asynchronous.

A sincronização pode ocorrer automaticamente (de acordo com um agendamento definido) ou manualmente. Os snapshots são sincronizados do sistema de origem para o sistema de destino e mantêm a eficiência de compartilhamento de block.

NOTA: A sincronização de snapshots não é compatível com replicação de arquivos.

Você pode iniciar manualmente a sincronização de uma sessão de replicação a qualquer momento selecionando a sessão e **Synchronize**. A sessão de replicação precisa estar em um destes estados:

- Funcionando normalmente
- Sistema pausado

Enquanto uma sessão de replicação está sendo sincronizada, você pode realizar as seguintes ações:

- Realizar um failover planejado do sistema de origem.
- Realizar um failover do sistema de destino.
- Pausar sessões de replicação do sistema de origem ou de destino.
- Excluir uma sessão de replicação removendo uma política de proteção.

NOTA: O failover (planejado ou não) só é possível depois que uma cópia de dados de linha de base é gravada no sistema de destino, indicada por um status OK da sessão de replicação.

Para obter um resumo dos atributos de replicação assíncrona e a comparação com replicação síncrona e Metro, consulte Resumo da replicação.

Replicação assíncrona para bloco

Estas informações se aplicam à replicação assíncrona de bloco:

- Quando uma sessão de replicação assíncrona é criada, um recurso somente leitura correspondente é criado no sistema de destino. Uma definição somente leitura da política de proteção também é criada no sistema de destino. Essa política será usada se ocorrer failover na sessão de replicação.
- Se você adicionar volumes a um Grupo de volumes ou alterar o tamanho do Grupo de volumes durante uma sessão de replicação assíncrona, as alterações não serão exibidas imediatamente no destino. Você pode executar uma sincronização manual ou aguardar até que a sincronização ocorra com base no RPO.
- Você pode alternar da replicação assíncrona para a síncrona modificando a regra de replicação na política de proteção atribuída.

NOTA: Alternar da replicação assíncrona para a replicação síncrona pode afetar o desempenho das sessões de replicação de volume e grupo de volumes.

Replicação assíncrona para arquivo

Estas informações se aplicam à replicação assíncrona de arquivo:

- A política de proteção é atribuída ao servidor NAS e, por padrão, todos os file systems em um servidor NAS protegido são sincronizados do sistema de origem para o de destino.
- Você pode optar por adicionar ou excluir file systems do servidor NAS, mesmo quando ele faz parte de uma sessão de replicação.
- Quando os file systems são modificados durante uma sessão de replicação assíncrona, as alterações são refletidas no sistema de destino no próximo ciclo de sincronização.
- Não é permitido alternar da replicação assíncrona para síncrona.
- A replicação de snapshots não é aceita.

Replicação síncrona

No modo de replicação síncrona, as atualizações dos dados no sistema de origem são replicadas para o sistema de destino imediatamente quando ocorre a atualização (replicação de RPO zero). O uso da replicação síncrona garante que ambos os sistemas estejam totalmente sincronizados a qualquer momento. A replicação síncrona garante nenhuma perda de dados , mas pode causar latência, dependendo da distância entre os sistemas de origem e destino.

NOTA: Nenhuma perda de dados é garantida quando a replicação não está funcionando normalmente, como durante pausas na sessão de replicação ou interrupções de rede.

PowerStore é compatível com replicação remota síncrona para volumes, grupos de volumes, clones dinâmicos, snapshots em bloco e servidores NAS.

Para aplicar a replicação síncrona a um recurso de armazenamento, atribua ao recurso uma política de proteção que inclua uma regra de replicação síncrona. A atribuição de uma política de proteção cria uma sessão de replicação que é adicionada à lista de sessões de replicação (**Replicação** > **de proteção**), e a coluna Tipo de replicação exibe Síncrona.

Quando uma sessão de replicação é criada, o recurso de armazenamento é replicado para o destino sistema. Somente as atualizações feitas no recurso são replicadas para o sistema de destino.

Você pode fazer failover de uma sessão de replicação síncrona usando failover planejado ou não planejado. Para obter detalhes, consulte a seção Failover.

Cancelar a atribuição da política de proteção do recurso de armazenamento exclui a sessão de replicação. Quando a sessão de replicação está funcionando normalmente, só é possível cancelar a atribuição da política no sistema de origem.

Quando você atribui uma política de proteção que inclui uma regra de replicação síncrona, o sistema de origem tem uma política de leitura/gravação, enquanto o sistema de destino tem uma cópia somente leitura da política. Somente a política de leitura/gravação pode ser modificada ou removida. Se o sistema que tem a política de leitura/gravação estiver inativo, a execução de um failover alternará as funções dos sistemas e permitirá que você gerencie a política de proteção de leitura/gravação a partir do sistema de destino.

Para habilitar a replicação síncrona, o par de sistemas tem que ser configurado com baixa latência de rede (menos de cinco milissegundos). Não é possível alterar a latência de rede configurada enquanto sessões de replicação síncrona são configuradas para esses sistemas.

Para obter um resumo dos atributos de replicação síncrona e a comparação com replicação assíncrona e Metro, consulte Resumo da replicação.

Replicação síncrona para bloco

- Quando uma sessão de replicação síncrona é criada, um recurso somente leitura correspondente é criado no sistema de destino. Uma definição somente leitura da política de proteção também é criada no sistema de destino. Essa política será usada se ocorrer failover na sessão de replicação.
- Snapshots do usuário:
  - Os snapshots do recurso que foram criados antes da criação da sessão são sincronizados com o sistema de destino.
  - Depois que a sessão de replicação é criada, os snapshots do usuário são executados simultaneamente nos sistemas de origem e destino com conteúdo quase idêntico.
  - Os snapshots do usuário criados quando a sessão de replicação é pausada não são replicados para o sistema de destino após a retomada ou a recuperação.
- Para alterar os parâmetros de um recurso (como nome, tamanho e política de desempenho), pause a sessão de replicação.
- Você pode alternar da replicação síncrona para a assíncrona modificando a regra de replicação na política de proteção atribuída.

Durante a replicação síncrona de bloco, é possível executar:

- Migração intracluster — Durante a transferência, o estado da sessão de replicação muda para Paused for Migration. A sessão de replicação retoma o estado quando a migração é concluída. As sessões que foram pausadas quando a migração começou permanecem pausadas.
- NDU — As sessões de replicação que têm o status Operating Normally quando o NDU é iniciado continuam ativas durante ele. O status das sessões de replicação pausadas muda para Paused for NDU.
- Reconfiguração do cluster — Você pode reconfigurar a rede de replicação do cluster, expandir ou fazer scale-down do cluster ou realocá-lo. A replicação é retomada após a conclusão da reconfiguração.

Quando um volume no sistema de destino é mapeado para um host, o sistema define a afinidade de nó para esse volume e, como resultado, todas as E/Ss são automaticamente direcionadas para o nó selecionado. Não é preciso pausar e retomar a sessão de replicação para que o redirecionamento de E/S entre em vigor. A definição da afinidade de nó para volumes no sistema de destino oferece balanceamento de carga e evita a latência da replicação. Você pode definir a afinidade de nó manualmente usando a API REST.

NOTA: Se não conseguir ver a coluna de afinidade de nó na tabela Volumes, adicione-a usando **Mostrar/ocultar colunas da tabela**.

Estas informações se aplicam à replicação síncrona do grupo de volumes:

- Todos os membros têm que residir no mesmo equipamento.
- Somente grupos de volumes com consistência de ordem de gravação configurada podem ser atribuídos com uma política de proteção que tem uma regra de replicação síncrona.
- Uma política de proteção atribuída a um grupo de volumes se aplica a todos os membros do grupo. Volumes individuais em um grupo de volumes não podem ser protegidos por uma política de proteção.
- Para alterar os parâmetros de um grupo de volumes (como nome, política de desempenho e consistência com a ordem de gravação), pause a sessão de replicação atribuída a ele.

Replicação síncrona para arquivo

Estas informações se aplicam à replicação de arquivos:

- A política de proteção é atribuída ao servidor NAS e, por padrão, todos os file systems em um servidor NAS protegido são sincronizados do sistema de origem para o de destino.
- Você pode optar por adicionar ou excluir file systems do servidor NAS, mesmo quando ele faz parte de uma sessão de replicação.
- Quando uma sessão de replicação síncrona é criada, um servidor NAS e file systems vazios são criados no sistema de destino. A configuração do servidor de arquivos e uma política de proteção somente leitura também são replicadas.
- O servidor NAS no sistema de destino é configurado sem ativação da configuração de IP, e todos os file systems ficam disponíveis sem compartilhamentos habilitados
- Quando uma sessão de replicação é criada, os file systems são replicados para o destino. As alterações subsequentes são replicadas para o destino quando ocorrem.
- 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.
- A partir do PowerStore 4.1, o intervalo de pesquisa dos objetos de replicação aumentou para dois minutos. O aumento foi feito para melhorar o desempenho quando há várias solicitações de consulta. Aguarde mais tempo para que o status do objeto seja atualizado no PowerStore Manager.

- A partir do 4.3, a replicação síncrona de arquivos usa a tecnologia Metro para failover automático, exigindo a configuração de PowerStore um serviço testemunha.

Pausar uma sessão de replicação

Quando você pausa uma sessão de replicação, as alterações feitas no recurso do sistema de origem não são replicadas para o sistema de destino.

É possível pausar uma sessão de replicação a partir do sistema de origem ou de destino. Para pausar um sistema de destino, selecione **Protection** > **Replication** > **[sessão de replicação]** e, em seguida, selecione **Pause**.

Quando você pausa uma sessão de replicação síncrona, um snapshot de recuperação será criado para ser usado como a última base comum quando a sessão for retomada.

A partir do 4.3, a replicação síncrona de PowerStore arquivos usa metro para failover automático. Pausar uma sessão de replicação não envolve a interação da testemunha e desativa o failover automático.

Enquanto uma sessão de replicação está pausada, você pode:

- Retome a sessão de replicação.
- Excluir a sessão de replicação removendo a política de proteção do recurso de armazenamento.
- Redimensionar ou renomear o recurso de armazenamento.
- Alterar a associação de um grupo de volumes.
- Iniciar a migração para outro equipamento do cluster.

Retomar uma sessão de replicação

Quando você retoma uma sessão de replicação, as alterações feitas no recurso do sistema de origem durante a pausa são sincronizadas com o sistema de destino.

É possível retomar uma sessão de replicação a partir do sistema de origem ou de destino. Para retomar um sistema de destino, selecione **Proteção** > **Replicação** > **[sessão de replicação pausada]** e, em seguida, selecione **Retomar**.

Quando você retoma uma sessão de replicação síncrona, as alterações no recurso de armazenamento do sistema de origem são sincronizadas com o recurso do sistema de destino, com base no snapshot de recuperação criado quando a sessão foi pausada. Os dados do host gravados no recurso durante a pausa são sincronizados com o destino. A replicação contínua é retomada para manter a sincronização entre a origem e o destino.

NOTA: Os snapshots que foram criados enquanto a sessão de replicação estava pausada não são sincronizados com o destino.

A partir do 4.3, a replicação síncrona de PowerStore arquivos usa metro para failover automático. Depois de retomar uma sessão de replicação, o estado de serviço da testemunha leva cerca de cinco minutos para mudar para Engajado.

Quando você retoma uma sessão de replicação assíncrona, a sincronização é realizada no próximo RPO. É possível optar por sincronizar os recursos manualmente selecionando a sessão de replicação e, em seguida, selecionando **Sincronizar**.

Failover

O failover de uma sessão de replicação inclui a alternância de funções entre os sistemas de origem e de destino e a inversão da direção da sessão de replicação.

Existem dois tipos de failover:

- Failover planejado — Iniciado pelo usuário. Inclui sincronização entre a origem e o destino para evitar a perda de dados.
- Failover não planejado – Iniciado a partir do sistema de destino em resposta a uma falha do sistema de origem.

Durante o failover da sessão de replicação, o sistema executa as seguintes ações:

- Interromper E/Ss no objeto de origem.
- Sincronizar os objetos de armazenamento de origem e de destino (ocorre somente em um failover planejado).
- Interromper a sessão de replicação.
- Inverter funções entre sistemas de origem e de destino.
- Promover a versão mais recente do objeto na nova origem.
- Retomar E/Ss na nova origem (iniciada pelo usuário).

- Para um failover planejado, se especificado pelo usuário, faça uma nova proteção.

Após um failover, você pode acessar aplicativos no novo sistema de origem para recuperar dados.

Realizar um teste de failover

Depois de configurar uma sessão de replicação, você pode testar a conexão para garantir que seus locais estejam configurados corretamente e preparados para a recuperação de desastres.

NOTA: Um teste de failover só pode ser executado no sistema de destino.

Durante um teste de failover, o sistema realiza um failover e o acesso de produção é fornecido ao local de destino por meio de dados replicados ou de um snapshot point-in-time. O recurso de armazenamento de destino é disponibilizado no modo de leitura/gravação e o acesso à produção é habilitado para hosts e aplicativos. É possível verificar a configuração da recuperação de desastres enquanto a replicação continua em segundo plano.

Para interromper o teste de failover, selecione uma das seguintes ações:

- Fazer failover nos dados de teste atuais — Se você fez alterações nos dados durante o teste de failover, pode usar os dados de teste atualizados. Isso interromperá o teste e preservará os dados de teste. Todos os dados replicados da origem durante o teste são descartados e o sistema de destino se torna a origem.

  NOTA: É preciso confirmar essas alterações antes de fazer failover nos dados de teste.

- Interromper o teste de failover — Quando o teste é interrompido, o acesso de produção ao destino é desativado para hosts e aplicativos e o recurso de armazenamento de destino é atualizado com os dados mais recentes sincronizados do sistema de origem. É possível criar um snapshot de backup dos dados de teste antes de interromper o teste de failover.

Restrições

Um teste de failover só pode ser executado sob as seguintes condições:

- OsPowerStoreA versão no sistema de origem e destino é 2.x ou posterior.
- O estado da sessão de replicação é OK.

  NOTA: Um teste de failover também pode ser executado quando o estado da sessão de replicação é System Paused ou Paused se a sincronização inicial for concluída.

Durante o teste de failover, você não pode executar as seguintes ações no sistema de destino:

- Alterar a associação do grupo de volumes
- Aumentar o tamanho do grupo de volumes
- Alterar o nome do grupo de volumes
- Iniciar a migração
- Remover uma política de proteção

NOTA: Você ainda pode executar essas ações a partir do sistema de origem.

Não é possível realizar um failover planejado enquanto um teste de failover está em andamento. É preciso interromper o teste de failover para executar o failover planejado. No entanto, failovers não planejados ainda podem ocorrer sem interrupções em resposta a um desastre. Se possível, é recomendável interromper o teste de failover antes de um failover não planejado, para evitar a perda de quaisquer dados replicados para o destino após o início do teste de failover.

Também é possível pausar e retomar as sessões de replicação durante um teste de failover. Se você excluir uma sessão de replicação durante um teste de failover, o teste será cancelado.

Iniciar um teste de failover

Você pode iniciar um teste de failover a partir dos dados de destino atuais ou de qualquer snapshot.

Existem duas maneiras de iniciar um teste de failover:

- De **Protection** > **Replication**, selecione a sessão de replicação que você deseja testar e, em seguida, selecione **Start Failover Test**.
- Na guia **Proteção** do recurso, selecione **Replicação** e depois **Iniciar teste de failover**.

Um alerta é gerado na sessão de replicação depois que o teste de failover é iniciado. O alerta é removido quando o teste é interrompido.

Interromper um teste de failover

Antes de interromper o teste de failover, é recomendável desmontar os file systems e interromper qualquer aplicativo em execução no recurso de destino para evitar corrupção dos dados.

Existem duas maneiras de interromper um teste de failover:

- De **Protection** > **Replication**, selecione a sessão de replicação que tem um teste em andamento e, em seguida, selecione **Stop Failover Test**.
- Na guia **Proteção** do recurso com um teste em andamento, selecione **Replicação** e depois **Parar teste de failover**.

Você também pode optar por criar um snapshot para salvar os dados de teste que foram criados durante o teste de failover.

Failover planejado

Quando você executa um failover planejado, a sessão de replicação faz failover manualmente do sistema de origem para o sistema de destino. Antes do failover iniciar, o sistema de destino é sincronizado com o sistema de origem para evitar a perda de dados.

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.

Durante um failover planejado, você pode realizar as seguintes ações:

- Executar um failover não planejado.
- Excluir a sessão de replicação excluindo a política de proteção no recurso de armazenamento.

Não é possível iniciar um failover planejado quando há um teste de failover em andamento.

Você pode iniciar um teste de failover planejado a partir dos dados de origem atuais ou de qualquer snapshot.

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**.

No caso de replicação síncrona, o failover planejado pode ser iniciado do sistema de origem quando a sessão de replicação está no estado Operating Normally. Como os dados são totalmente sincronizados entre os sistemas, o failover não causa nenhuma perda de dados. No entanto, é recomendável interromper as operações de E/S para aplicativos e hosts antes de iniciar o failover.

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: Quando os dados são sincronizados como parte da ação de nova proteção, o gráfico de desempenho do sistema de origem exibe um ponto único. Como o próximo ponto será registrado no gráfico quando ocorrer a próxima sincronização, o gráfico aparece vazio. Para visualizar os valores de desempenho, passe o mouse sobre o gráfico.

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...).

Failover não planejado

O failover não planejado ocorre após eventos no sistema de origem, como falhas, ou eventos que resultam em tempo de inatividade para acesso de produção. O failover não planejado é iniciado no sistema de destino e dá acesso de produção ao recurso de destino inicial com base em um snapshot point-in-time.

NOTA: A partir dePowerStore4.3, A replicação síncrona de arquivos usa Metro para failover automático. Se um serviço de testemunha estiver configurado, o failover automático estará disponível para todas as sessões de replicação síncrona de arquivos. Consulte Testemunha do Metro para obter detalhes sobre a configuração do witness.

Ao iniciar um failover não planejado, você pode indicar se deseja usar a cópia de dados mais recente ou um snapshot dos dados (se disponível) como fonte de dados.

Quando a conexão com o sistema de origem é restabelecida, o recurso de origem inicial é colocado no modo de destino. Use a opção **Reproteger** para sincronizar o recurso de armazenamento de destino e, em seguida, retome a sessão de replicação.

NOTA: Antes de executar um failover não planejado, desligue o servidor NAS no local de produção. Não é recomendável desligar o link de replicação para testar a funcionalidade de failover não planejado, pois isso pode resultar em indisponibilidade de dados. A partir dePowerStore4.3, é necessário desligar o cluster antes do failover não planejado.

NOTA: Na replicação de arquivos, não é recomendável modificar a rede de mobilidade de arquivos depois de executar um failover não planejado. Após a restauração da conexão entre os sistemas de origem e destino, é possível que ambos os servidores NAS estejam no modo de produção.

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.

Failover automático para replicação síncrona de arquivos

A replicação síncrona de arquivos usa a tecnologia Metro para failover automático, exigindo que uma tecnologia de serviço de testemunha faça failover automático para o sistema de destino quando o sistema de origem está inativo.

A partir do 4.3, a replicação síncrona de PowerStore arquivos usa a tecnologia Metro para failover automático. Um serviço de testemunha deve ser configurado para ativar o failover automático.

O sistema identifica quando o sistema de origem está inativo e faz failover automático da sessão de replicação para o sistema de destino.

Na tabela de sessões de replicação (**Replicação** > de proteção), o **estado de failover automático** indica se a sessão de replicação está habilitada para failover automático. Os estados possíveis são:

- Não aplicável — A sessão de replicação não é uma sessão de replicação síncrona de arquivos.
- Upgrade obrigatório — a versão do software do sistema remoto para a sessão de replicação não é compatível com o File Witness Service (FWS). É necessário fazer upgrade do sistema para uma versão compatível com FWS para ativar o failover automático.
- Manual Enable Required — os sistemas local e remoto são compatíveis com failover automático baseado em witness. Para ativar manualmente o failover automático para a sessão de replicação herdada, marque a caixa de seleção ao lado da sessão e, em seguida, selecione **Enable Auto Failover**.
- Enabled for Witness Interaction — a sessão de replicação está habilitada para failover automático baseado em testemunha.

NOTA: O estado de failover automático também é exibido na janela de detalhes da sessão de replicação.

A replicação ocorre no nível do servidor NAS, mas as operações de replicação sincronizada com metro de arquivo são realizadas no nível do grupo do file system, que inclui todos os pares de file systems sincronizados.

Durante uma sessão de replicação síncrona de file metro, se qualquer um dos pares de file system não estiver no estado sincronizado (por exemplo, depois de pausar e retomar a sessão de replicação) e a perda de conexão acionar o failover automático, os file systems não sincronizados não sofrerão failover para o sistema de destino, enquanto todos os file systems que estiverem no estado sincronizado sofrerão failover e a E/S de serviço do novo sistema de origem. Como resultado, o estado da sessão de replicação é alterado para **failover parcial**.

Clicar na seta ao lado do nome do servidor NAS na tabela **Replication** expande sua lista de file systems, mostrando o status de cada file system.

Você pode selecionar uma das opções a seguir:

- Aguarde até que o sistema de origem se recupere e que a sessão de replicação seja totalmente sincronizada e repita o failover.

NOTA: Para garantir que todos os file systems estejam sincronizados, verifique se o status da sessão de replicação (coluna **Replication** > **Session Status**) foi alterado para **Failed Over**. A partir do PowerStore 4.3, você também pode usar a API REST para verificar o estado de sincronização de uma sessão de replicação. Para sessões de replicação síncrona de metro de arquivo, verifique o status no sistema de destino. Para sessões de replicação legadas, verifique o status no sistema de origem.

- Repita o failover usando a opção Force - selecione a sessão de replicação e, em seguida, selecione **Failover**. No aviso de **replicação de failover** exibido, selecione a opção **Force failover from destination resource** .

  NOTA: O failover forçado pode ser iniciado usando a ou a PowerStore Manager API REST.

  NOTA: O uso de failover forçado pode resultar em perda de alguns dados.

Recuperar um servidor NAS

Você pode resolver cenários de várias falhas em sistemas por meio de ações de failover ou recuperação para manter a acessibilidade e a funcionalidade do servidor NAS.

Podem ocorrer cenários de várias falhas em que os sistemas de origem e destino não podem se comunicar entre si e um dos sistemas ou ambos não podem se comunicar com o serviço witness. Quando esses cenários acontecem, os servidores NAS nos sistemas local e remoto ficam off-line e o serviço witness não pode determinar qual sistema deve permanecer acessível ao host.

Para resolver os seguintes cenários de falha, inicie um failover para o sistema de destino:

- A conexão entre o sistema de destino e o serviço witness fica inativa e, em seguida, o sistema de origem fica inativo.
- O serviço de testemunha fica inativo e, em seguida, o sistema de origem fica inativo.

Para resolver os seguintes cenários de falha, use a opção **Recover** (**Storage** > **NAS Servers** > **[servidor NAS]** > **More Actions** > **Recover**):

- A conexão entre o sistema de origem e o serviço witness fica inativa e, em seguida, o sistema de destino fica inativo.
- O serviço de testemunha fica inativo e, em seguida, o sistema de destino fica inativo.
- A conexão entre o sistema de destino e o serviço testemunha, seguida pela conexão entre o sistema de origem e o sistema testemunha, cai e, em seguida, a conexão entre os sistemas de origem e de destino fica inativa.
- O serviço de testemunha fica inativo e, em seguida, a conexão entre os sistemas de origem e de destino fica inativa.

Depois de selecionar **Recover**, o servidor NAS recuperado entra no modo de produção.

NOTA: Não use a opção **Recover** para cenários diferentes dos especificados acima.

NOTA: A recuperação do servidor NAS também pode ser iniciada usando a API REST.

Outras considerações sobre replicação

Durante a replicação de bloco, quando o sistema de origem está pausado para NDU e o sistema de destino está ativo, o status do sistema de destino é alterado para *System_Paused*. Se o sistema de destino fica inativo durante o NDU do sistema de origem, quando ele se torna ativo novamente, o status permanece como *OK*.

Durante a replicação de arquivo, quando o sistema de origem está pausado para NDU, o sistema de destino permanece no estado *OK*, independentemente do status de conectividade.

A partir do 4.3, a replicação síncrona de PowerStore arquivos usa metro para failover automático. É recomendável fazer failover da sessão de replicação para o local remoto antes de iniciar o NDU, a fim de evitar o failover automático durante as reinicializações do cluster do local de origem.

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.
- Failover planejado (consulte a seção acima).

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 Replication.
   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.

Replicação de Virtual Volumes

PowerStore integra-se ao VMware Live Site Recovery para dar suporte à replicação assíncrona de volume virtual.

A proteção remota da máquina virtual é configurada usando gerenciamento baseado em política de armazenamento (SPBM) do vSphere. Para recuperação de falha, o failover de máquinas virtuais é configurado usando o VMware Live Site Recovery.

O VMware Live Site Recovery é uma solução de recuperação de desastres que automatiza a recuperação ou a migração de máquinas virtuais entre um local protegido e um local de recuperação.

Regras de snapshot e replicação criadas em PowerStore são expostos ao vSphere e podem ser adicionados às políticas de proteção. O vSphere fornece uma política de armazenamento para PowerStore durante a criação do vVol.

Um grupo de replicação que inclui volumes virtuais que devem ser replicados juntos é a unidade de replicação e failover configurada no vSphere.

Snapshots somente leitura e leitura/gravação podem ser gerados para vVols. A sincronização, manual ou de acordo com o agendamento definido, é apenas aplicada a snapshots somente leitura.

Para visualizar os detalhes de uma sessão de replicação de Virtual Volume:

1. Selecione **Proteção** > **Replicação**.
2. Clique no status da sessão de replicação para visualizar os detalhes.

O gráfico na janela de detalhes da sessão de replicação indica que o vSphere gerencia a sessão.

Na janela de detalhes da sessão de replicação, você pode fazer o seguinte:

- Visualizar os detalhes da sessão de replicação.
- Renomear o grupo de replicação.
- Pausar e retomar a sessão de replicação.
- Sincronizar a sessão de replicação.

Pré-requisitos

Antes de configurar a replicação de Virtual Volume, certifique-se de que os seguintes pré-requisitos sejam atendidos:

- Os sistemas local e remoto devem estar conectados e ter o recurso de vVol (consulte Sistemas remotos).
- Os contêineres de armazenamento devem ser definidos nos dois sistemas (**Armazenamento** > **Contêineres de armazenamento** > **Criar**) para serem emparelhados. Se houver um único contêiner de armazenamento em cada sistema, os contêineres de armazenamento serão emparelhados automaticamente. Do contrário, será necessário especificar o destino do contêiner de armazenamento manualmente (**Armazenamento** > **Contêineres de armazenamento** > **[contêiner de armazenamento]** > **Proteção** > **Criar**).

Criar uma sessão de replicação de Virtual Volume

Sobre esta tarefa

Para obter informações sobre a configuração necessária no vSphere, consulte a documentação do usuário do VMware SRM.

Etapas

1. No PowerStore, crie uma regra de replicação.

   A regra de replicação é exposta para o vCenter como um recurso de replicação.
2. No vSphere, crie uma política usando a regra exposta.

   Uma cópia somente leitura da política de proteção, com um nome idêntico, é adicionada ao PowerStore (visível na tabela **Políticas de proteção** e marcada com um ícone de cadeado).

   NOTA: Também é possível adicionar regras de snapshot para ativar a proteção local.

   NOTA: Não é possível criar, modificar ou excluir uma política de proteção somente leitura e atribuir ou cancelar a atribuição da política a máquinas virtuais usando o PowerStore. Para realizar essa ação, use a atualização da Política de armazenamento no vSphere.
3. No vSphere, crie uma máquina virtual, atribua a ela uma política de armazenamento com uma regra de replicação e a associe a um grupo de replicação.

Resultados

O grupo de replicação e a sessão de replicação são criados automaticamente no PowerStore (visível em **Proteção** > **Replicação** > **[sessão do grupo de replicação]**.

Monitorando o desempenho do grupo de replicação

Quando uma política de armazenamento que inclui uma regra de replicação do PowerStore é criada na VMware e atribuída a uma VM baseada em vVol, uma sessão de replicação é criada no PowerStore para os recursos do vVol no mesmo grupo de recursos. O VMware Live Site Recovery usa esses grupos de recursos da VMware para gerenciar as VMs protegidas em grupos de replicação.

Você pode monitorar o desempenho de um grupo de replicação no PowerStore. Selecione **Proteção** > **Replicação** e clique no status de uma sessão de replicação do vVol para exibir os detalhes da sessão (o **Tipo de recurso** deve ser *Grupo de replicação*. Clique na guia **Desempenho do grupo de replicação** para exibir os dados de desempenho do grupo de replicação. Você pode selecionar para exibir gráficos dos seguintes dados:

- Dados restantes para replicação

- Largura de banda da replicação (normalizada)
- Tempo de transferência da replicação

Também é possível definir a linha do tempo para os dados exibidos.

Recuperação de máquinas virtuais

O Site Recovery Manager (SRM) é uma solução para recuperação de desastres da VMware que automatiza a recuperação de máquinas virtuais durante estados de falha.

Para ativar a recuperação de máquinas virtuais, é necessário configurar um plano de recuperação usando o SRM. Um plano de recuperação executa etapas de recuperação predefinidas em grupos de replicação selecionados. As etapas de recuperação incluem failover, reproteção e teste de failover.

Um grupo de proteção é criado no vSphere e inclui um ou mais grupos de replicação e um plano de recuperação. Se ocorrer falha, o SRM executará o plano de recuperação nos Virtual Volumes dos grupos de replicação.

Em PowerStore, você pode monitorar o status da sessão de replicação durante a recuperação.

Para obter mais detalhes, consulte o *Guia do VMware Site Recovery Manager*.

6

Proteção Metro

Este tópico contém as seguintes informações:

Tópicos:

- Pré-requisitos e limitações
- Configurar a conectividade do host
- Testemunha do Metro
- Configurar um volume Metro
- Configurar um grupo de volumes Metro
- Definir a função Metro
- Monitorar recursos Metro
- Pausar um recurso Metro
- Retomar um recurso Metro
- Promover um recurso Metro
- Rebaixar um recurso Metro
- Encerrar um recurso Metro
- Resumo das ações permitidas em um recurso metro
- Usando políticas de proteção com Metro
- Usando QoS com metro

Pré-requisitos e limitações

Antes de configurar a proteção Metro, considere as seguintes limitações:

- O suporte metro está disponível apenas comModelo PowerStore TePowerStoreEquipamentos modelo Q.
- A proteção Metro é habilitada para volumes e grupos de volumes.
- A proteção Metro é compatível com hosts do Windows, Linux e VMware ESXi conectados por FC/SCSI ou iSCSI.

NOTA: Os hosts Windows e Linux são compatíveis a partir de:PowerStoreSO 4.x.

Quando uma conexão com um sistema remoto é estabelecida, o sistema detecta a configuração automaticamente e ativa os recursos compatíveis para o sistema remoto. Para habilitar o recurso Metro de bloco, certifique-se de que as seguintes condições sejam atendidas em ambosPowerStoreSistemas:

- Os dois sistemas estão em execuçãoPowerStoreOS 3.x ou posterior.
- A latência no sistema remoto é baixa.
- Tipo de conexão de dados:
  - TCP - Quando local e remotoPowerStoresistemas que executam a versão 3.x (ou posterior) são instalados, a conexão TCP é suportada automaticamente. No entanto, quando um ou ambos osPowerStoreOs sistemas estão executando a versão 2.x. Você deve fazer upgrade dos sistemas para a versão 3.x para ativar o Metro. Após o upgrade, é exibido um alerta para você atualizar o tipo de conexão do sistema remoto. Clique no link no alerta para abrir a janela **Atualizar transporte do sistema remoto**. Depois, clique em **Atualizar transporte**.

    NOTA: O alerta é removido somente depois que o transporte é atualizado.

  - FC - A partir dePowerStoreversão 4.4, tipo de conexão FC é compatível com o Metro.

Para implementar um serviço de testemunha, certifique-se de que os seguintes pré-requisitos sejam atendidos:

- O serviço de testemunha deve ser instalado em um host Linux independente (virtual ou físico).
- O serviço de testemunha deve ser implementado em um terceiro domínio de falha, que é separado dos doisPowerStoreSistemas que fazem parte da sessão metro. A instalação do serviço testemunha em um sistema separado garante sua disponibilidade se ocorrer falta de energia nos sistemas metro.

- Sistemas operacionais compatíveis: Consulte a *Matriz de suporte simples do Dell Technologies PowerStore* na página de documentação do PowerStore.
- Dependências (obrigatórias no host Linux):
  - Java 11 ou Java 17 (paraPowerStoreversão 4.2 e posterior)
  - SQLite

  NOTA: As dependências listadas são instaladas automaticamente ao usar um gerenciador de pacotes (como yum ou zypper).
- Hardware:
  - O sistema operacional precisa estar em execução em uma arquitetura de CPU x64.
  - Mínimo de 4 GB de RAM.
  - Um mínimo de 5 GB de espaço em disco disponível.
- Portas:
  - A porta 443/tcp precisa estar aberta no host testemunha antes de instalar a testemunha.
  - Os firewalls do data center devem permitir que o tráfego na porta 443 seja ativadoPowerStorePara enviar solicitações ao serviço de testemunha.
- Latência de rede - Latência máxima de 100 milissegundos na rede de gerenciamento entrePowerStoree o serviço de testemunhas.
- Acesso à conta de usuário - o acesso root ou sudo é necessário para instalar o serviço de testemunha no host.
- Garanta a conectividade com oPowerStoreRede de gerenciamento.
- Para uma testemunha virtual, é recomendável usar um Endereço IP estático para a VM testemunha. No entanto, se você estiver usando DHCP, adicione a testemunha aPowerStoreusando o nome do domínio totalmente qualificado (FQDN).

NOTA: Para obter mais informações sobre limites Metro, consulte a *Matriz de suporte simples do Dell Technologies PowerStore* na página de documentação do PowerStore.

Configurar a conectividade do host

NOTA: O suporte a host é fornecido para o VMware vSphere Metro Storage Cluster. Há suporte à conectividade Fibre Channel e iSCSI.

NOTA: A partir do sistema PowerStore versão 4.x, o suporte a host é oferecido para hosts Windows e Linux.

A conectividade Metro do host é configurada em sistemas PowerStore locais e remotos e permite que hosts e aplicativos percebam volumes físicos dos dois sistemas como sendo um único volume. Ao configurar a conectividade Metro para o host, selecione a array preferencial para determinar qual sistema manterá o acesso ao armazenamento se ocorrer uma falha.

É necessário definir um host (ESXi, Windows ou Linux) nos sistemas locais e remotos para permitir a conectividade metro do host.

Quando você cria um host, o assistente **Adicionar host** permite definir a conectividade do host:

NOTA: As opções de conectividade do host são demonstradas graficamente no assistente **Adicionar host**.

- **Conectividade local** — Fornece acesso do host somente para o sistema local.

  NOTA: A conectividade local também pode ser usada com volumes Metro.
- **Conectividade Metro** — Fornece acesso do host aos sistemas local e remoto. Se você selecionar essa opção, defina o acesso ao sistema:
  - **O host está colocalizado com este sistema** — A latência do caminho do host é mais baixa para o sistema local e mais alta para o sistema remoto. O host sempre tenta enviar E/S para o sistema local (exceto quando o sistema local está inativo).
  - **O host está colocalizado com o sistema remoto** — A latência do caminho do host é mais baixa para o sistema remoto. O host sempre tenta enviar E/S para o sistema remoto (exceto quando o sistema remoto está inativo).
  - **Colocalizado com os dois sistemas** — A latência e o desempenho do caminho do host são iguais para os sistemas local e remoto. O host envia E/S para os sistemas local ou remoto de acordo com as considerações sobre múltiplos caminhos.

NOTA: Independentemente da conectividade configurada, é necessário configurar todos os hosts do ESXi no mesmo vCenter Cluster.

NOTA: Em um host do ESXi mapeado para um volume Metro, é recomendável usar PSP (Path Selection Plugin) de rodízio com o modo de latência ativado.

NOTA: Se um dos sistemas ficar off-line, o host do ESXi entrará em uma condição APD (All Paths Down). Para resolver essa condição, é recomendável configurar o vSphere HA. Essa configuração permite que as máquinas virtuais nos hosts do ESXi disponíveis reiniciem e resolvam a condição APD.

Testemunha do Metro

No PowerStoreOS 3.6 e posterior, você pode adicionar um serviço testemunha à proteção metro para oferecer proteção contra cenários de falha única.

O serviço de testemunha é um terceiro passivo instalado em um host independente.

NOTA: O serviço de testemunha deve ser implementado em um terceiro domínio de falha, que é separado dos dois PowerStore sistemas que fazem parte da sessão metro. A instalação do serviço testemunha em um sistema separado garante sua disponibilidade se ocorrer falta de energia nos sistemas metro.

Quando ocorre uma falha, os sistemas local e remoto PowerStore entram em contato com o serviço de testemunha e solicitam a interrupção da sessão metro. A testemunha então determina qual sistema permanece acessível aos hosts e continua a atender às E/Ss. Se possível, a testemunha dá preferência ao sistema PowerStore que foi atribuído com a função preferencial. A adição do serviço de testemunha a uma sessão metro oferece proteção contra cenários de falha única, inclusive falhas preferenciais do sistema que não são tratadas sem uma testemunha.

O serviço de testemunha é simples e não mantém dados essenciais que não podem ser criados novamente. Sendo assim, não há necessidade de fazer backup, salvar nem recuperar a testemunha. Ela poderá ser removida e reinstalada sempre que a recuperação for necessária.

Implementar a Metro witness

Se os pré-requisitos forem atendidos, você poderá usar o RPM para instalar diretamente o serviço testemunha. Caso contrário, você pode usar um gerenciador de pacotes (yum, zypper) para instalar automaticamente as dependências. Você pode fazer download do pacote de instalação na página do Suporte Dell.

Para instalar o serviço de testemunha em um host Linux, execute o seguinte comando:

```
sudo rpm -i <rpm_file>
```

NOTA: Você pode usar um gerenciador de pacotes ou RPM para desinstalar o serviço testemunha.

NOTA: O serviço de testemunha está disponível somente comModelo PowerStore TePowerStoreEquipamentos modelo Q.

Configurar a testemunha do Metro

Sobre esta tarefa

- Somente o administrador, o administrador de segurança e o administrador de armazenamento estão autorizados a configurar o serviço testemunha.
- Você pode configurar o serviço de testemunha antes ou depois de configurar o metro.
- Somente um serviço de testemunha pode ser configurado por cluster.
- O serviço de testemunha configurado é usado para todas as sessões metro e não pode ser desativado para sessões específicas.
- O status do serviço de testemunha muda para Engajado somente depois de configurado para os sistemas local e remoto PowerStore .
- Para acessar as ferramentas de instalação do serviço de testemunha (gerador de token seguro e impressão digital), use o caminho:

```
sles15:~ # ls /opt/dell-witness-service/scripts
```

NOTA: Siga as etapas a seguir para sistemas PowerStore local e remoto.

Etapas

1. PowerStore No Manager, selecione **Protection** > **Metro Witness**.
2. Na janela **Testemunha do Metro**, selecione **Adicionar**.
3. Na janela **Adicionar testemunha**, configure os seguintes campos:

- Nome
- Endereço IP/FQDN
- Token de segurança — Para gerar um token de segurança, execute o script generate_token.sh. Para obter detalhes, consulte o *Guia de configuração de segurança do PowerStore* na página da documentação do PowerStore.

  NOTA: O token expira em dez minutos.

- Descrição (opcional)

4. Verifique os requisitos de instalação exibidos e marque a caixa de seleção para confirmar.
5. Selecione **Add**.
6. Na janela **Autorização do usuário**, analise a impressão digital do certificado da testemunha e selecione **Confirmar** para aceitar.

   NOTA: Para obter detalhes, consulte o *Guia de configuração de segurança do PowerStore* na página da documentação do PowerStore.

   O certificado é salvo no sistema PowerStore.

Resultados

A testemunha é criada e todos os volumes e grupos de volumes do Metro existentes são automaticamente atribuídos a ela. Os volumes e grupos de volumes Metro recém-criados são atribuídos automaticamente à testemunha. A coluna **Recursos do Metro** na janela **Testemunha do Metro** mostra o número de recursos atribuídos à testemunha.

Modificação e recuperação de testemunha

O serviço de testemunha é simples e não mantém dados essenciais que não podem ser criados novamente. Sendo assim, não há necessidade de fazer backup, salvar nem recuperar a testemunha. Ela poderá ser removida e reinstalada sempre que a recuperação for necessária.

Modificar os parâmetros da testemunha

Sobre esta tarefa

Na janela **Propriedades da testemunha**, é possível modificar o nome e a descrição da testemunha.

NOTA: Se quiser alterar o Endereço IP ou FQDN dela, remova e reinstale a testemunha.

Etapas

1. Selecione **Proteção** > **Testemunha do Metro**.
2. Marque a caixa de seleção ao lado da testemunha e selecione **Modificar**.
3. Modifique os campos necessários e selecione **Aplicar**.

Substituir a testemunha

Sobre esta tarefa

Para substituir o serviço witness, remova-o PowerStore dos sistemas e, em seguida, adicione-o. A remoção e adição da testemunha é necessária mesmo que o nome do host ou endereço IP não seja alterado, já que a nova testemunha tem um certificado diferente que deve ser adicionado aos PowerStore sistemas.

Etapas

1. Remova o serviço de testemunha de cada um dos PowerStore sistemas. Para obter informações, consulte Remover a testemunha.
2. Adicione o serviço de testemunha a cada um dos PowerStore sistemas. Para obter informações, consulte Configurar o metro witness.

Modificar a configuração do host testemunha

Se o host no qual o serviço de testemunha está instalado precisar ser modificado, você poderá executar um dos seguintes procedimentos:

- Crie um host com a configuração necessária e instale a testemunha. Em seguida, remova a testemunha existente dos PowerStore sistemas e substitua-a pela nova testemunha.
- Modifique o host existente:
  - Remova a testemunha existente dos PowerStore sistemas. Para obter informações, consulte Remover a testemunha.
  - Desinstale a testemunha do host existente.
  - Faça as alterações de configuração necessárias no host.
  - Reinstale a testemunha no host. Para obter detalhes, consulte Implementar o metro witness.
  - Adicione a testemunha aos PowerStore sistemas. Para obter informações, consulte Configurar o metro witness.

Monitorar a testemunha

Selecione **Proteção** > **Testemunha do Metro** > **[testemunha]** para exibir as propriedades da testemunha.

O serviço de testemunha mantém a comunicação com todos os nós em todos os equipamentos.

A janela **Propriedades** da testemunha exibe o estado de conexão de cada nó e o estado geral de conexão do serviço testemunha.

Possíveis estados de conexão:

- Inicializando — Todos os nós estão inicializando a conexão com a testemunha.
- OK — Todos os nós podem se comunicar com a testemunha.
- Excluindo — A testemunha está sendo excluída do cluster.
- Parcialmente conectado — Alguns nós em alguns equipamentos podem se comunicar com a testemunha ou a mesma testemunha não está registrada no sistema par.
- Desconectado — Nenhum nó consegue se comunicar com a testemunha.

Depois que a testemunha é configurada, cada sessão Metro tenta interagir com ela de modo independente. Cada sessão Metro tem um estado que indica se ela pode usar a testemunha quando ocorre uma falha. Possíveis estados da testemunha para uma sessão Metro:

- Inicializando — A testemunha está sendo inicializado, mas não está engajada.
- Desengajada — A sessão Metro está pausada ou interrompida.
- Engajada — Todos os nós de todos os equipamentos estão conectados à testemunha e podem usá-la em caso de falha.
- Desengajado Configuração inválida ou indisponível — A configuração da testemunha é inválida (por exemplo, a testemunha está configurada apenas em um sistema PowerStore ou duas testemunhas diferentes estão configuradas nos sistemas local e remoto) ou a testemunha está indisponível.
- Desengajada: Falha ao iniciar — Houve falha na inicialização da testemunha com a sessão Metro.
- Unconfigure in Progress — A testemunha está sendo removida do PowerStore sistema.

Quando o cluster tem vários equipamentos, alguns deles podem estar conectados à testemunha enquanto outros não estão. Como resultado, talvez a testemunha não esteja engajada em todas as sessões Metro existentes.

Remover a testemunha

Você pode remover o serviço de testemunha do PowerStore a qualquer momento, independentemente de ele estar atribuído a sessões metro.

Para remover a testemunha, selecione **Proteção** > **Testemunha do Metro**, marque a caixa ao lado da testemunha e selecione **Excluir**.

A exclusão da testemunha remove-a de todas as sessões Metro, e as sessões voltam a usar regras de preferência como um meio de determinar o comportamento do sistema em caso de falha.

Se ocorrer um erro durante a exclusão da testemunha, ela permanecerá no estado Desconfiguração em andamento até que o erro seja resolvido. Depois, a exclusão será retomada.

Testemunha — Cenários de falha

Quando ocorre uma falha em um ambiente metro com um serviço witness, o sistema se comporta da seguinte maneira:

Quando a conexão entre os sistemas local e remoto é perdida, a sessão metro é interrompida. Ambos os sistemas solicitam que a sessão testemunha seja dividida. A testemunha responde com sucesso à primeira solicitação e com erro à segunda solicitação. O sistema que teve sucesso como resposta mantém o acesso de E/S ao volume metro enquanto o sistema que recebeu o erro se rebaixa.

O sistema não preferencial envia a solicitação à testemunha alguns segundos após o sistema preferencial. Como resultado, se o sistema preferencial estiver ativo, ele receberá a resposta de sucesso e será selecionado para manter o acesso de E/S do host.

Se o sistema preferencial estiver inativo, ele não enviará uma solicitação para a testemunha, e o não preferencial receberá a resposta de sucesso.

Quando um dos sistemas perde a conexão com o host, não há impacto, já que ambos os sistemas ainda estão a caminho. e o host pode acessá-los. Se ocorrer perda de conexão entre o sistema, o sistema que ainda tem conexão com o witness receberá uma resposta de sucesso e manterá o acesso à E/S do host.

Configurar um volume Metro

Sobre esta tarefa

Habilitar a configuração metro para um volume torna-o visível para hosts a partir de doisPowerStoreSistemas com uma conexão de sistema remoto.

O metro pode ser configurado para volumes e para clones de volumes que não são membros de um grupo de volumes.

Os seguintes volumes não podem ser configurados como metro:

- Um volume atribuído com uma política de proteção que inclui uma regra de replicação
- Um volume ou um clone de volume que é membro de um grupo de volumes
- Um volume com uma política de proteção somente leitura
- Um volume que está sendo migrado ou importado
- Um volume que é um destino de replicação somente leitura, deixado depois que a replicação é removida

NOTA: Se uma witness foi configurada para issoPowerStoresystem, o volume metro é atribuído automaticamente à testemunha.

Etapas

1. Selecionar **Armazenamento** > **Volume** e marque a caixa de seleção de um volume.
2. Selecionar **Proteger** > **Configurar um Volume Metro**.
   É exibido o painel deslizante **Configurar volume Metro**.
3. Selecione um sistema remoto ou configure um novo.
4. Se o sistema remoto tiver vários equipamentos, você poderá selecionar o posicionamento do volume no sistema remoto.
5. Clique em **Configure**.
6. No sistema remoto, mapeie o volume metro configurado para um host.

Configurar um grupo de volumes Metro

Sobre esta tarefa

Habilitar a configuração metro para um grupo de volumes torna-o visível para hosts a partir de doisPowerStoreSistemas com uma conexão de sistema remoto.

NOTA: Todos os volumes em um grupo são tratados como uma única instância e todas as ações no grupo de volumes se aplicam a todos os membros.

Não é possível configurar os seguintes grupos de volumes como Metro:

- Um grupo de volumes vazio
- Um clone de grupo de volumes
- Um grupo de volumes com um membro clone
- Um grupo de volumes sem consistência com a ordem de gravação
- Um grupo de volumes que inclui volumes que não são locais.
- Um grupo de volumes atribuído com uma política de proteção que inclui uma regra de replicação.
- Um grupo de volumes com uma política de proteção somente leitura
- Um grupo de volumes que está sendo migrado ou importado
- Um grupo de volumes que é um destino de replicação somente leitura

NOTA: Se uma witness foi configurada para issoPowerStoreSystem, o grupo de volumes Metro é atribuído automaticamente à testemunha.

Etapas

1. Selecionar **Armazenamento** > **Grupo de volumes** E marque a caixa de seleção de um grupo de volumes.
2. Selecionar **Proteger** > **Configurar o grupo de volumes metro**.
   O painel deslizante **Configure Metro Volume Group** será exibido.
3. Selecione um sistema remoto ou configure um novo.
4. Clique em **Configure**.
5. No sistema remoto, mapeie o grupo de volumes Metro configurado para um host.

Definir a função Metro

NOTA: A função metro pode ser definida para volumes individuais, clones de volumes individuais ou grupos de volumes. Não é possível definir uma função metro para volumes ou clones que são membros de um grupo de volumes.

Na configuração do recurso metro, o sistema do qual o recurso metro (volume, clone de volume ou grupo de volumes) foi configurado é automaticamente definido como preferencial. Quando o recurso Metro é interrompido ou pausado e a testemunha do Metro não foi configurada, o sistema preferencial mantém o acesso de host e produção e uma associação ativa com uma política de proteção.

Quando o estado do recurso metro é Operating Normally (active/active), você pode alterar a função do recurso metro de preferencial para não preferencial ou de não preferencial para preferencial usando as seguintes opções:

- **Modify Preferred Role** — Use esta opção para alterar a função atual do recurso Metro selecionado. Essa opção pode ser usada no sistema preferencial ou não preferencial.

  NOTA: Você pode acessar essa opção selecionando **Protection** > **Metro** e, em seguida, clique no status Metro do recurso relevante para abrir a janela Metro Resource Details.

- **Set Local Role To Preferred** - Use essa opção para definir a função de vários recursos metro não preferenciais selecionados como preferenciais. Essa opção deve ser usada antes de desligar o sistema preferencial para manutenção planejada. Configurar os recursos Metro não preferenciais como preferenciais permite manter o acesso de host e produção durante o desligamento.

Monitorar recursos Metro

Sobre esta tarefa

Você pode visualizar todos os recursos metro no sistema, monitorar seus status e executar ações em um volume, clone ou grupo de volumes Metro selecionado.

Etapas

1. Selecionar**Protection** > **Metro**Para abrir a lista de recursos e detalhes do Metro.
2. Marque a caixa de seleção de um recurso Metro para visualizar as ações que podem ser realizadas nele.
3. Para visualizar informações detalhadas sobre um recurso Metro específico, clique no status do recurso na**Status do Metro**coluna.

   Você também pode visualizar informações detalhadas sobre um recurso Metro no**Armazenamento** > **Volumes**ou o argumento**Armazenamento** > **Grupos de volumes**Página:

   a. Clique no nome de um recurso Metro na**Armazenamento** > **Volumes**ou o argumento**Armazenamento** > **Grupos de volumes**para exibir a página Resource Information.
   b. Selecione o**Protection**e, em seguida, selecione o**Volume Metro**ou o argumento**Grupo de volumes Metro**para exibir as informações do Metro para o recurso selecionado.

Pausar um recurso Metro

Sobre esta tarefa

NOTA: Você pode pausar volumes metro individuais, clones ou grupos de volumes. Não é possível pausar um volume metro ou um clone metro que são membros de um grupo de volumes.

É necessário pausar um recurso Metro temporariamente nos seguintes cenários:

- Quando há necessidade de alterações de configuração que não podem ser realizadas quando o recurso está funcionando normalmente, como alterações nas propriedades do recurso.
- Quando os sistemas preferencial ou não preferencial exigem manutenção, como a substituição de componentes de hardware com defeito ou alterações na infraestrutura de rede.
- Quando há uma falha no sistema preferencial que requer a promoção do sistema não preferencial para permitir a recuperação controlada.

A pausa pode ser iniciada no sistema preferencial ou no sistema não preferencial. Quando um recurso Metro é pausado, a sincronização entre os sistemas é interrompida temporariamente. As políticas de proteção e o acesso de produção permanecem ativos no sistema preferencial.

Quando um recurso Metro é interrompido e não há conexão entre o sistema local e o remoto, a pausa é implementada somente no sistema local (onde ele foi implementado):

- Quando uma pausa é iniciada no sistema preferencial:
  - O acesso de host e produção permanece ativado em um recurso Metro preferencial pausado.
  - O acesso de host e produção permanece inalterado no recurso Metro não preferencial.
- Quando uma pausa é iniciada no sistema não preferencial:
  - O acesso de host e produção permanece desativado, a menos que o recurso Metro tenha sido promovido.
  - Como não há conectividade de rede, a pausa não modifica o estado do recurso metro preferencial.
- Quando a conectividade for resolvida, a pausa também deverá ser iniciada no sistema remoto.

Etapas

1. Selecionar **Protection** > **Metro**.
2. Marque a caixa de seleção do recurso metro a ser pausado e clique em **Pausar**.
   É exibido o painel deslizante **Pause Metro Volume/Volume Group**.
3. Clique em **Pausar** para confirmar.

Retomar um recurso Metro

Sobre esta tarefa

NOTA: Você pode retomar volumes metro individuais, clones ou grupos de volumes. Não é possível retomar um volume Metro ou um clone Metro que são membros de um grupo de volumes.

A retomada pode ser iniciada no sistema preferencial ou no sistema não preferencial.

Quando você retoma um recurso Metro preferencial que está pausado, o sistema preferencial começa a sincronizar dados com o sistema não preferencial. Depois que a sincronização é concluída, o status do recurso Metro retorna a um estado ativo/ativo.

Quando você retoma um recurso Metro promovido (anteriormente não preferencial) que estava pausado, o sistema não preferencial começa a sincronizar com o preferencial (estado Reprotecting) para voltar ao estado ativo/ativo.

NOTA: Se um recurso Metro ficou pausado por muito tempo, a sincronização poderá demorar um pouco devido ao acúmulo de dados no sistema preferencial.

Se o sistema não preferencial foi promovido, a retomada do recurso Metro do sistema não preferencial promovido sincroniza dados desse sistema com o sistema preferencial.

Etapas

1. Selecionar**Protection** > **Metro**.
2. Marque a caixa de seleção do recurso metro a ser retomado e clique em**Resume**.
   A caixa de diálogo **Resume Metro Volume/Volume Group** é exibida.
3. Clique em**Resume**para confirmar.

Promover um recurso Metro

Pré-requisitos

- Você pode promover volumes metro individuais, clones ou grupos de volumes. Não é possível promover um volume Metro ou um clone Metro que sejam membros de um grupo de volumes.
- A promoção de um recurso Metro é permitida no estado `Fractured` ou `Paused`.

Sobre esta tarefa

Quando o link entre os dois sistemas de armazenamento falha ou quando o sistema não preferencial está inativo, a sincronização entre os sistemas é interrompida, assim como o recurso Metro. O sistema preferencial permanece ativo e continua a atender à E/S. Se o usuário estiver no sistema preferencial, nenhuma ação será necessária e os sistemas serão sincronizados quando o problema for resolvido.

Quando ocorre uma falha no sistema preferencial, a sincronização entre os sistemas é interrompida, assim como o recurso Metro. Os dois sistemas param de atender à E/S. Para poder acessar o recurso Metro, o usuário precisa promovê-lo no sistema não preferencial para permitir o acesso de host e de produção a ele até o sistema preferencial se recuperar.

Se o usuário verificar que o sistema preferencial está disponível, o recurso Metro no sistema não preferencial poderá ser promovido sem implicações. Quando o usuário está no sistema não preferencial, não é possível saber o status do sistema preferencial (se ele está inativo ou se o link entre o sistema está inativo). Nesse caso, promover o volume Metro no sistema não preferencial poderá fazer com que ambos os sistemas continuem atendendo à E/S, mas sem sincronizar.

Etapas

1. Selecionar**Protection** > **Metro**.

   A página Metro lista todos os recursos Metro e possibilita a avaliação de todos os recursos afetados e a priorização da promoção de acordo com suas considerações.

   NOTA: O status do recurso Metro deve ser `Fractured`.

2. Selecione o status do recurso metro para exibir a página de detalhes do recurso metro e, em seguida, selecione**Promover**.
   É exibido o painel deslizante **Promote Metro Volume/Volume Group**.

   NOTA: Antes que a promoção ocorra, é obtido um snapshot do recurso Metro.

3. Você tem que entender a implicação de promover o recurso Metro caso o sistema remoto esteja atendendo à E/S. Se possível, verifique se o sistema remoto está inativo.
4. Marque a caixa de seleção de confirmação na parte inferior do painel deslizante **Promover volume/grupo de volumes Metro** e selecione**Promover**.
   O estado promovido do recurso Metro é indicado na página de detalhes dele.

Rebaixar um recurso Metro

Sobre esta tarefa

NOTA: Você pode rebaixar volumes metro individuais, clones ou grupos de volumes. Não é possível rebaixar um volume Metro nem um clone Metro que sejam membros de um grupo de volumes.

Quando o sistema preferencial fica sem espaço de armazenamento, a sincronização entre os sistemas é interrompida, assim como o recurso Metro. Os dois sistemas param de atender à E/S. Nesse caso, o recurso Metro no sistema não preferencial precisa ser promovido para permitir o acesso de host e produção a ele até o sistema preferencial resolver o problema. Para ativar esse estado, primeiro o recurso Metro no sistema preferencial precisa ser rebaixado.

Etapas

1. Selecionar**Protection** > **Metro**.

   NOTA: A página Metro lista todos os recursos Metro e possibilita a avaliação de todos os volumes afetados e a priorização do rebaixamento de recursos de acordo com suas considerações.

2. Selecione o status de um recurso metro para exibir a página de detalhes do recurso metro e, em seguida, selecione**Rebaixar**.
   É exibido o painel deslizante **Demote Metro Volume/Volume Group**.

3. Você tem que entender a implicação de rebaixar o recurso Metro caso o sistema remoto esteja atendendo à E/S. Se possível, verifique se o sistema remoto está inativo.
4. Selecionar**Rebaixar**.
   O estado rebaixado do recurso é indicado na página de detalhes do recurso Metro.

Encerrar um recurso Metro

Sobre esta tarefa

NOTA: Você pode encerrar volumes metro individuais, clones ou grupos de volumes. Não é possível encerrar um volume Metro nem um clone Metro que são membros de um grupo de volumes.

Quando você encerra um recurso Metro, a configuração do Metro é removida, o que resulta em dois volumes ou grupos de volumes independentes. Se o recurso remoto não for excluído, o sistema removerá a política de proteção atribuída a ele, desassociará os hosts e fará a atribuição usando um WWN de SCSI novo e diferente. Você pode encerrar um recurso Metro no sistema preferencial ou no sistema não preferencial.

Etapas

1. Selecionar**Protection** > **Metro**.
2. Selecione o status de um recurso metro para exibir a página de detalhes do recurso metro e, em seguida, selecione**Encerrar Metro**.
   É exibido o painel deslizante **End Metro Volume/Volume Group**.
3. Selecione uma das seguintes opções no painel deslizante:
   - Encerrar o Metro e manter os recursos nos sistemas local e remoto.

     NOTA: O sistema remoto desassocia os hosts e atribui outro WWN de SCSI ao recurso. Se você encerrar um grupo de volumes Metro, um WWN de SCSI diferente será atribuído a cada membro do grupo de volumes.

   - Encerrar o Metro e excluir o recurso e os snapshots associados no sistema remoto.

     NOTA: Não é possível excluir os volumes remotos e os grupos de volumes associados a snapshots seguros não expirados.

4. Clique em**Fim**.

Resumo das ações permitidas em um recurso metro

A tabela abaixo resume as ações permitidas que você pode realizar em um recurso metro, dependendo do status atual do metro e do sistema em que a ação é iniciada.

NOTA: A tabela aborda casos de uso comuns e não inclui cenários de falhas raras.

Tabela 2. Ações do Metro permitidas

Local	Status do Metro	Modificar função	Promover	Rebaixar	Pause	Resume	Encerrar Metro
No sistema preferencial	Funcionando normalmente	Sim	Não	Não	Sim	Não	Sim
	Paused	Não	Não	Sim	Não	Sim	Sim
	Interrompido	Não	Não	Sim	Sim	Não	Sim
	Alternar para sincronização do Metro	Não	Não	Não	Sim	Não	Sim
Em um sistema não preferencial	Funcionando normalmente	Sim	Não	Não	Sim	Não	Sim
	Paused	Não	Sim (se outro sistema	Não	Não	Sim	Sim

Tabela 2. Ações do Metro permitidas (continuação)

Local	Status do Metro	Modificar função	Promover	Rebaixar	Pause	Resume	Encerrar Metro
			estiver inacessível)				
	Interrompido	Não	Sim (se outro sistema estiver inacessível)	Não	Sim	Não	Sim
	Alternar para sincronização do Metro	Não	Não	Não	Sim	Não	Sim

Usando políticas de proteção com Metro

Quando um recurso Metro existente é atribuído com uma política de proteção ou quando um recurso com uma política de proteção é configurado para Metro, a mesma proteção é aplicada ao recurso Metro nos dois sistemas. A política de proteção criada no sistema remoto é somente leitura. Alterações na política de proteção e nas regras de snapshot só podem ser feitas na política criada pelo usuário (independentemente do sistema de armazenamento em que ela foi criada). A política somente leitura é sincronizada com as alterações a cada 15 minutos.

Os snapshots iniciados pelo usuário criados em um sistema de armazenamento também são gerados no outro sistema.

NOTA: A replicação síncrona e assíncrona não é compatível com recursos Metro. Não é possível atribuir uma política de proteção que contém uma regra de replicação a um recurso Metro.

A atribuição de uma política de proteção pode ser feita no sistema local ou remoto (preferencial ou não preferencial).

O cancelamento da atribuição da política de proteção deve ser feito no sistema de armazenamento em que ela foi atribuída. Depois que o cancelamento da atribuição da política de proteção for feito no recurso do sistema local, a atribuição da política também será cancelada no recurso do outro sistema. Quando não houver recursos Metro usando a política de proteção somente leitura, ela será excluída automaticamente do sistema.

NOTA: Quando, devido a uma falha do recurso Metro, não for possível cancelar a atribuição da política no sistema de armazenamento em que ela foi atribuída, estas opções são permitidas:

- Uma política somente leitura pode ter sua atribuição cancelada ou pode ser trocada por uma política de leitura e gravação de um recurso Metro preferencial quando ele é interrompido.
- Uma política somente leitura pode ter sua atribuição cancelada ou pode ser trocada por uma política de leitura e gravação de um recurso Metro promovido não preferencial.

NOTA: Quando o recurso Metro é interrompido ou uma sessão Metro é pausada, os snapshots são gerados somente no sistema ativo. Quando o recurso Metro é autorrecuperado ou a sessão é retomada, os snapshots não são copiados para o sistema remoto e permanecem no sistema local até que expirem ou sejam excluídos.

Usando QoS com metro

Quando um volume ou um grupo de volumes metro é configurado com uma política de QoS, a política não é replicada para o sistema remoto. Se você estiver usando uma configuração metro em que a QoS é usada, é recomendável configurar a mesma política de QoS em ambos os lados do recurso metro.

Se uma política de QoS estiver configurada apenas em um lado do recurso metro, um host pode preferir determinados caminhos para enviar E/S. O mesmo pode ocorrer quando uma política de QoS é configurada em ambos os lados do recurso metro, mas os limites de QoS não correspondem.

7

Backup remoto

Este tópico contém as seguintes informações:

Tópicos:

- Terminologia
- Pré-requisitos e limites
- Recursos de documentação
- Fluxo de trabalho básico de backup remoto
- Estados da sessão
- Gerenciando sessões de backup remoto
- Recursos
- Sessões de recuperação
- Sessões de acesso instantâneo
- Alta disponibilidade
- Alertas de backup remoto

Terminologia

Tabela 3. Terminologia de backup remoto

TERMO	DESCRIPTION
PowerProtect DD	Um equipamento Data Domain de nova geração projetado principalmente para backup de dados.
PowerProtect Data Manager	Um aplicativo de gerenciamento centralizado para gerenciar um ou mais PowerProtect DD físicos ou na nuvem.
Unidade de armazenamento DD	Uma unidade lógica no PowerProtect DD que é exposta a aplicativos de backup usando o protocolo DD Boost.
Sistema remoto PowerProtect DD	Uma unidade de armazenamento no sistema PowerProtect DD.
Sessão remota	Uma sessão de snapshot remoto que reflete o estado e o andamento de uma operação em um sistema remoto PowerProtect DD. O tipo de sessão pode ser Backup, Recuperação ou Acesso instantâneo.
Snapshot remoto	Uma representação dos dados que passaram por backup no PowerProtect DD e podem ser recuperados ou navegados usando acesso instantâneo.

Pré-requisitos e limites

Ao usar o backup remoto, considere as seguintes limitações:

- Só é possível criar uma sessão de backup remoto por recurso (volume ou grupo de volumes).
- Só é possível criar uma sessão de recuperação ou de acesso instantâneo por snapshot remoto.
- Até duas sessões de acesso instantâneo podem ser criadas por nó.
- As sessões de backup e recuperação remotas e as sessões de acesso instantâneo são mutuamente exclusivas — quando uma sessão de acesso instantâneo está ativa, as sessões de backup e recuperação remotas não podem ser executadas e, quando as sessões de backup e recuperação remotas estão ativas, as sessões de acesso instantâneo não podem ser executadas.
- Quando a reconfiguração de rede ou um NDU está em andamento, não é possível executar sessões de backup remoto, recuperação e acesso instantâneo.

- Uma sessão de acesso instantâneo pode ser criada para um grupo de volumes que consistem em quatro volumes.
- Se o tamanho do volume de backup exceder o limite fixo da cota da Unidade de armazenamento (SU) do Data Domain, o backup poderá falhar. Recomenda-se não definir cotas de SU ao usar o backup remoto. Consulte a documentação do PowerProtect DD para obter detalhes.
- Para obter o desempenho ideal do sistema, é recomendável fazer backup de até 125 volumes para o PowerProtect DD por equipamento.
- Para obter o desempenho ideal do sistema, é recomendável fazer backup de até 125 sessões de backup remoto por equipamento.
- O backup remoto não é compatível com volumes Metro.
- O suporte para DDVE na nuvem só está disponível com o provedor de serviços em nuvem AWS.
- A desduplicação está desativada no lado do client, mas ativada no equipamento PowerProtect.
- A alta disponibilidade não é compatível com acesso instantâneo. Se um cluster for reinicializado ou sofrer fail over, ocorrerá falha no acesso instantâneo. Para obter mais informações, consulte o artigo da base de conhecimento 000208509 da Dell (As sessões de acesso instantâneo exibirão um estado de falha após a reinicialização do nó).

Recursos de documentação

Para obter mais informações, consulte os seguintes recursos:

Tabela 4. Recursos de documentação

Documento	Descrição	Local
Guia do usuário e administração do PowerProtect Data Manager	Fornece informações de configuração para o PowerProtect Data Manager.	Dell Support
Dell PowerProtect Data Manager: proteção de dados para Dell PowerStore Guia de storage arrays	Este documento tem como foco o backup e a recuperação de dados de volume de bloco no PowerStore storage arrays usando o PowerProtect Data Manager.	Dell Infohub
PowerStore Ajuda on-line	A Ajuda on-line contém informações contextuais da página aberta no PowerStore Manager.	Incorporado em PowerStore Manager

Fluxo de trabalho básico de backup remoto

Fazer backup de recursos em um PowerProtect DD é a ação básica que você pode executar. Quando os backups são criados em um PowerProtect DD, é possível procurá-los e recuperá-los. Todas as ações de backup remoto estão vinculadas a uma sessão de backup remoto que permite o acompanhamento do progresso.

Sobre esta tarefa

Execute as seguintes etapas para criar uma sessão de backup remoto:

Etapas

1. Adicionar uma conexão de sistema remoto para backup remoto.
2. Criar uma regra de backup remoto.
3. Criar uma política de proteção— Apenas uma regra de backup remoto pode ser adicionada a uma política de proteção.
4. Atribuir uma política de proteção— Atribua uma política que inclua uma regra de backup remoto a um volume ou grupo de volumes. Uma sessão de backup remoto é criada e exibida na guia **Sessões de backup** da página **Backup remoto**.

Estados da sessão

As sessões de backup remoto, recuperação e acesso instantâneo passam por vários estados que indicam o progresso delas e possíveis problemas.

Os estados de sessão possíveis são:

- **Inicializando** — A sessão está sendo criada. Depois que a criação for concluída, o status muda para Ocioso.

- **Ociosa** — Nenhum dado é transferido para o equipamento remoto. A sessão permanece no estado Ocioso até que a regra de backup remoto agendada seja acionada ou você iniciar um backup manual.
- **Preparação** — O sistema PowerStore está se preparando para executar um backup. Se houver várias sessões ativas, a sessão poderá permanecer no estado Preparação até chegar na parte superior da fila.
- **Encaminhamento de E/S** (aplica-se somente a sessões de acesso instantâneo) — A sessão está encaminhando a E/S do host.
- **Em andamento** — O sistema cria o backup no sistema remoto. Durante esse estado, você pode clicar no link de status para monitorar o andamento do backup e visualizar mais detalhes.
- **Concluída** (aplica-se somente a sessões de recuperação) — A sessão foi concluída com sucesso.
- **Pausada pelo sistema** — o upgrade não disruptivo ou a migração pausaram a sessão.
- **Pausada** — A sessão está pausada.
- **Cancelando** — A sessão está sendo cancelada.
- **Cancelada** — A sessão foi explicitamente cancelada. As sessões nos estados Preparação, Em andamento e Pausada podem ser canceladas.
- **Excluindo** — A sessão está sendo excluída.
- **Falha** — A sessão apresentou falha ao criar o backup.
- **Reversão em andamento** — Ocorreu um erro enquanto a sessão estava ativa e as alterações foram revertidas.
- **Limpeza de falha obrigatória** — Ocorreu um erro enquanto as alterações eram revertidas (como resultado de um erro anterior). O serviço de limpeza, que é executado periodicamente, resolve automaticamente o problema e o estado da sessão é alterado para Falha. Para sessões de backup remoto, os backups agendados não podem ser executados enquanto a sessão estiver nesse estado.
- **Limpeza de cancelamento obrigatória** — Ocorreu um erro durante a operação de cancelamento da sessão. O serviço de limpeza, que é executado periodicamente, resolve o problema automaticamente, e o estado da sessão é alterado para "Cancelada". Para sessões de backup remoto, os backups agendados não podem ser executados enquanto a sessão estiver nesse estado.
- **Limpeza obrigatória** — A sessão foi concluída com sucesso, mas ocorreu um erro durante a fase de limpeza local. O serviço de limpeza, que é executado periodicamente, resolve automaticamente o problema e o estado da sessão é alterado para Concluída. Para sessões de backup remoto, os backups agendados não podem ser executados enquanto a sessão estiver nesse estado.
- **Limpeza em andamento** — Uma limpeza está em andamento.

Gerenciando sessões de backup remoto

Quando você atribui uma política de proteção que inclui uma regra de backup remoto a um volume ou a um grupo de volumes, uma sessão de backup remoto é criada e exibida na guia **Sessões de backup** da página **Backup remoto**.

Na guia **Sessões de backup**, você pode executar as seguintes ações em uma sessão de backup remoto:

- **Fazer backup** — Faça backup manual sob demanda quando a sessão estiver ociosa. Por exemplo, se o recurso não tiver sido submetido a backup por um longo período.

  NOTA: Um backup criado manualmente está sujeito à política de retenção definida na regra de backup remoto.

- **Pausar** — Pausar uma sessão em um estado ocioso faz com que ela seja pausada imediatamente. Se você pausar uma sessão em andamento, ela só será pausada depois que o backup atual em execução for concluído. Os backups subsequentes não serão realizados enquanto a sessão estiver pausada.
- **Retomar** — Use esta opção para retomar uma sessão de backup pausada. O próximo backup ocorrerá de acordo com o agendamento definido.
- **Excluir** — Use esta opção somente para excluir uma sessão de um recurso protegido por uma política externa. Em recursos protegidos por política do PowerStore, é possível excluir a sessão de backup remoto associada cancelando a atribuição da política do recurso ou removendo a regra de backup remoto da política atribuída.
- **Cancelar** — Use esta opção para cancelar uma sessão de backup somente quando ela estiver em andamento. O cancelamento de uma sessão faz com que o backup atual seja cancelado e os dados copiados sejam descartados.

  NOTA: Quando a sessão está no estado Preparação, outras sessões podem ser colocadas na fila antes dela. Quando você clica em **Cancelar**, o estado da sessão é alterado para **Cancelando**, mas a sessão só é cancelada quando atinge o topo da fila e se torna ativa (estado em andamento).

Recursos

A guia Recursos exibe todos os volumes e grupos de volumes que têm snapshots remotos associados.

Um recurso é adicionado à tabela **Recursos** depois que uma sessão de backup remoto que foi criada para o recurso aciona a criação de um snapshot remoto.

Se um volume ou um grupo de volumes que tem snapshots remotos associados for excluído do PowerStore, os snapshots remotos não serão afetados. O recurso excluído permanecerá listado na tabela Recursos até que todos os snapshots remotos associados expirem. Para ver se um recurso está excluído, adicione a coluna **Origem excluída** à tabela Recursos usando a opção **Mostrar/ocultar colunas da tabela**.

Na guia **Recursos**, é possível executar as seguintes ações:

- Gerenciar snapshots — Selecionar um recurso na lista e clicar em **Gerenciar snapshots** exibe todos os snapshots remotos criados para esse recurso:
  - A validade dos snapshots criados de maneira automática e manual baseia-se no tempo de retenção que foi configurado na regra de backup remoto.
  - Não é possível alterar a validade de um snapshot remoto. Alterar o período de retenção em uma regra de backup remoto não afeta os snapshots existentes.
  - Para snapshots gerados automaticamente, o nome de um snapshot remoto inclui o nome da regra de backup remoto que o criou.
  - Para criar uma sessão de recuperação de um snapshot, selecione-o na lista e clique em **Recuperar**. Consulte Recuperar um snapshot remoto para o mesmo cluster do PowerStore para obter informações detalhadas.
  - Para excluir um ou mais snapshots, selecione-os e clique em **Excluir**.

  NOTA: Caso queira ver os snapshots remotos de um recurso e executar ações relacionadas, clique no recurso e selecione a guia **Snapshots remotos**.

- Acesso instantâneo — Selecionar um recurso na lista e clicar em **Acesso instantâneo** inicia o processo de ativação do acesso instantâneo para o snapshot remoto selecionado. Para obter detalhes, consulte Criar uma sessão de acesso instantâneo.
- Detectar snapshots remotos — Use essa opção quando quiser recuperar um snapshot remoto de um recurso em um cluster diferente do PowerStore. Para obter detalhes, consulte Recuperar um snapshot remoto para um outro cluster.

Sessões de recuperação

Snapshots de volumes e grupos de volumes que são submetidos a backup em um PowerProtect DD podem ser recuperados para o mesmo cluster ou para outros clusters do PowerStore.

Talvez você queira recuperar um snapshot remoto para restaurar o recurso de origem ou criar um clone dinâmico.

Recupere um snapshot remoto para o mesmo cluster do PowerStore:

- Se o volume de origem ou o grupo de volumes do backup recuperado ainda existir no sistema, um snapshot local será criado no cluster do PowerStore. Se possível, a recuperação será incremental.
- Se o volume de origem ou o grupo de volumes do backup recuperado não existir mais no sistema, um novo volume e um snapshot local serão criados, e o novo volume será restaurado com os dados do snapshot.

Recupere um snapshot remoto para um outro cluster do PowerStore:

- Como o volume de origem nunca existiu nesse cluster, um novo volume e um snapshot local serão criados. O novo volume é restaurado com os dados do snapshot.

Uma sessão de recuperação será criada para cada operação de recuperação. O status inicial da sessão é Preparação. Depois que a sessão começa a copiar o snapshot, o status muda para Em andamento e, depois que o snapshot é copiado, o estado muda para Concluído.

Você pode visualizar e monitorar o andamento das sessões de recuperação na guia **Sessões de recuperação** (**Proteção** > **Backup remoto**). Também é possível executar estas ações:

- Excluir — Use essa opção para excluir uma sessão de recuperação em um status **Concluído**.
- Cancelar — Use essa opção para cancelar uma sessão de recuperação em um status **Em andamento**.

  NOTA: Quando o status da sessão é **Em andamento**, outras sessões podem ser colocadas na fila antes dela. Quando você clica em **Cancelar**, o estado da sessão é alterado para **Cancelando**, mas a sessão só é cancelada quando atinge o topo da fila e se torna ativa.

Depois que um backup é recuperado, ele funciona como qualquer snapshot local. Você pode usar um backup recuperado para restaurar um volume primário ou criar um clone. O snapshot recuperado é definido como Sem exclusão automática. Você pode alterar essa configuração definindo um período de retenção. Você também pode modificá-lo para ser um snapshot seguro.

Recuperar um snapshot remoto para o mesmo cluster do PowerStore

Sobre esta tarefa

Quando você precisa restaurar um recurso pai ou criar um clone dinâmico, talvez queira recuperar um snapshot remoto para o mesmo cluster do PowerStore no qual reside o recurso de origem. É possível recuperar um snapshot remoto tanto de um recurso existente quanto de um excluído.

Etapas

1. Clique em **Proteção** > **Backup remoto** e selecione a guia **Recursos**.

   A guia **Recursos** exibe todos os recursos (volumes e grupos de volumes) que têm snapshots remotos associados.
2. Na lista Recursos, clique na caixa de seleção ao lado do recurso e selecione **Gerenciar snapshots** para visualizar todos os backups criados para esse recurso.
3. No painel **Gerenciar snapshots**, selecione o snapshot que você deseja recuperar e clique em **Recuperar**.
4. Na mensagem de confirmação, clique em **Recuperar**.
   Uma sessão de recuperação é criada para o snapshot e adicionada à tabela Sessões de recuperação. Se o recurso de origem existir no cluster, um snapshot local será criado no recurso de origem e o backup recuperado será copiado para ele. A recuperação pode ser de uma cópia completa ou incluir apenas as diferenças entre o backup e o recurso (cópia incremental), dependendo do último backup. Se o recurso de origem não existir mais no cluster, um novo volume ou grupo de volumes será criado no cluster do PowerStore, bem como um snapshot local para o qual o snapshot remoto será copiado.

   Você pode monitorar o andamento da sessão de recuperação em **Proteção** > **Backup remoto** > **Sessões de recuperação**.

Recuperar um snapshot remoto para um outro cluster

Sobre esta tarefa

Quando você recupera um snapshot remoto para um cluster do PowerStore que não é aquele que tem o recurso de origem, um novo volume ou grupo de volumes é criado no cluster do PowerStore, bem como um snapshot local para o qual o snapshot remoto é copiado.

Etapas

1. Clique em **Proteção** > **Backup remoto** e selecione a guia **Recursos**.
2. Clique em **Detectar snapshots remotos**.
3. No painel **Detectar snapshots remotos**, defina o seguinte:
   - Sistema remoto PowerProtect DD — Selecione o PowerProtect DD do qual você deseja recuperar o backup.
   - ID global do PowerStore — Especifique o identificador global exclusivo para o cluster do PowerStore a partir do qual o backup foi iniciado. Você pode ver o ID global do cluster em **Settings** > **Cluster** > **Properties**. Para obter informações adicionais sobre como recuperar o ID global do cluster, consulte o artigo 000226798 da base de conhecimento da Dell (Como obter o ID global do cluster principal...).
   - De — Especifique a data e a hora de início para pesquisar snapshots remotos.
   - Até — Especifique a data e a hora de término para pesquisar snapshots remotos.
4. Clique em **Avançar**.
5. Na lista de snapshots detectados, selecione o snapshot que deseja recuperar e clique em **Próxima**.

   NOTA: Você só pode selecionar snapshots que foram criados por um cluster do PowerStore.
6. Analise o resumo de informações e clique em **Recuperar**.

Resultados

O PowerStore cria uma sessão de recuperação que pode ser visualizada na guia **Sessões de recuperação**. Quando a sessão é concluída, o snapshot recuperado e um novo volume são criados no cluster local.

Recuperação — Considerações adicionais

- Quando a origem original de um snapshot de backup recuperado do DD não existe mais (snapshot órfão), os blocos no volume recém-criado que não foram gravados durante o backup do volume original são alocados e gravados com zeros. Como resultado,

as capacidades física e lógica são iguais (ao analisar os dados de capacidade de backup recuperados). Quando o novo volume for mapeado para um host, o espaço usado e livre será exibido corretamente. Para obter mais informações, consulte o artigo da base de conhecimento Dell 000208504 (após recuperar PowerStore do Data Domain...).

- Quando um volume ou grupo de volumes de origem não existe mais no cluster do PowerStore, recuperar o respectivo backup sempre resulta na criação de uma nova origem junto com o snapshot recuperado.
- Se o tamanho do snapshot recuperado não corresponder ao tamanho do volume de origem, a recuperação será completa (o snapshot inteiro será copiado do PowerProtect para o PowerStore.
- Será feita a recuperação incremental (recuperando apenas as alterações que ocorreram desde o backup) se as seguintes condições forem atendidas:
  - O tamanho do volume de origem não foi alterado desde o backup.
  - O volume de origem e o backup remoto mais recente existem no cluster do PowerStore.
- A taxa média de transferência para uma recuperação incremental nem sempre é precisa, embora a porcentagem do andamento da recuperação reflita com precisão o volume de dados recuperados.

Sessões de acesso instantâneo

Com o acesso instantâneo, você pode acessar snapshots remotos em um PowerProtect DD sem precisar recuperá-los para o cluster do PowerStore.

- Use a opção de acesso instantâneo para procurar um snapshot remoto antes de decidir se deseja recuperá-lo ou para acessar um snapshot de um recurso excluído, corrompido ou modificado e copie-o para o host.
- Apenas uma sessão de acesso instantâneo é permitida por snapshot remoto.
- Uma sessão de acesso instantâneo pode ser criada para grupos de volumes que incluem até quatro membros.
- Quando uma sessão de acesso instantâneo para um recurso de armazenamento está em execução, o cluster do PowerStore não pode executar operações de backup e recuperação para recursos protegidos que estão no mesmo equipamento que esse recurso. É recomendável encerrar a sessão de acesso instantâneo quando possível para fornecer proteção contínua aos recursos de armazenamento.
- Ocorre falha no acesso instantâneo quando um cluster é reinicializado ou sofre fail over. Para reinicializar o acesso instantâneo nesse caso, desassocie o volume de acesso instantâneo do host, exclua a sessão e crie-a novamente.
- O sistema define a afinidade do nó com sessões de acesso instantâneo na criação. Se o host não puder acessar o nó com o qual a sessão de acesso instantâneo tem afinidade, a sessão de acesso instantâneo não fará failover para o outro nó, e o host poderá encontrar problemas para acessar os dados no recurso de acesso instantâneo.

As seguintes informações são fornecidas na guia **Sessões de acesso instantâneo**:

- Status — O status da sessão é Encaminhamento de E/S.
- Recurso local — Exibe o novo volume ou grupo de volumes que é criado como parte da sessão. Clicar no hiperlink de recurso local abre a página Detalhes desse recurso. Nela, você pode visualizar os detalhes do volume ou os membros do grupo de volumes. Você também pode visualizar dados de desempenho, verificar alertas emitidos e associar ou desassociar hosts para o recurso.

Na guia Sessões de acesso instantâneo, é possível encerrar uma sessão de acesso instantâneo. Para encerrar a sessão, primeiro você precisa remover todas as associações de host para o recurso local.

Os volumes e grupos de volumes criados como parte das sessões de acesso instantâneo também são exibidos em **Armazenamento** > **Volumes** > **Acesso instantâneo** e **Armazenamento** > **Grupos de volumes** > **Acesso instantâneo**.

Criar uma sessão de acesso instantâneo

O acesso instantâneo permite que você tenha acesso a snapshots remotos no PowerProtect DD sem precisar recuperá-los para o cluster do PowerStore.

Etapas

1. Selecione **Proteção** > **Backup remoto** > **Recursos**.
2. Na lista de recursos, marque a caixa de seleção ao lado do recurso e clique em **Acesso instantâneo**.
   O painel **Ativar o acesso instantâneo** exibe todos os snapshots remotos disponíveis para o recurso selecionado.
3. Selecione o snapshot que você deseja acessar.

   NOTA: Você também pode selecionar o recurso e, em seguida, selecionar **Snapshots remotos** > **snapshot remoto** > **Ativar acesso instantâneo**.

4. Também é possível associar hosts ao volume criado quando a sessão de acesso instantâneo é iniciada. Clique em **Associar hosts**, selecione os hosts que você deseja associar e clique em **Aplicar**.
   Os hosts mapeados são listados na seção Conectividade do host.
   NOTA: Essa opção só existe para volumes, não para grupos de volumes. A associação de hosts a membros de um grupo de volumes só será possível depois que você criar a sessão de acesso instantâneo (veja os detalhes abaixo).
5. Clique em **Habilitar**.
   Uma sessão de acesso instantâneo é criada e adicionada à guia **Sessões de acesso instantâneo**. Um volume ou grupo de volumes associado local é criado para a sessão e pode ser visualizado na guia **Instant Access** na janela **Volumes** ou **Volume Groups**.
   NOTA: A guia **Acesso instantâneo** é exibida somente quando o PowerProtect DD é adicionado como um sistema remoto.

   O recurso criado é leitura/gravação. Os dados são gravados temporariamente no equipamento PowerProtect DD enquanto o snapshot remoto permanece inalterado. Quando a sessão é excluída, todas as gravações são perdidas.

Resultados

Depois de criar um acesso instantâneo para um grupo de volumes, você pode associar hosts a membros do grupo de volumes que foi criado para a sessão:

1. Selecione **Proteção** > **Backup remoto** > **Sessões de acesso instantâneo**.
2. Clique no link do grupo de volumes na coluna **Recurso local** para visualizar os membros.
3. Selecione os membros que você deseja associar e clique em **Associar** para abrir o painel **Associar hosts**.

Acesso instantâneo — Considerações adicionais

- O PowerStore oferece suporte ao acesso instantâneo a todos os recursos de bloco, exceto aos datastores VMFS do VMware vStorage. Se você precisar acessar dados em um snapshot remoto, recupere-o e depois crie e monte um clone dinâmico.
- A alta disponibilidade não é suportada para acesso instantâneo. Consulte Alta disponibilidade e o artigo da base de conhecimento da Dell 000208509 (Sessões de acesso instantâneo exibem um estado de falha após a reinicialização do nó).
- O acesso instantâneo não é aceito para DDVE na nuvem.

Alta disponibilidade

A alta disponibilidade é compatível (mas não garantida) para sessões de backup remoto e de recuperação, mas não para sessões de acesso instantâneo:

- Quando um nó está inativo ou um nó é reinicializado —
  - Faça backup e recupere o failover de sessões para o nó par e continue nele.
  - As sessões de acesso instantâneo são específicas do nó. Quando o nó em que a sessão está em execução fica inacessível ou inativo, a sessão muda para um estado com falha. Desassocie o volume do host, exclua a sessão e, em seguida, crie a sessão novamente.
- Quando um equipamento é desligado ou reinicializado —
  - Todas as sessões de backup e recuperação são retomadas quando o equipamento está ativo novamente.
  - As sessões de acesso instantâneo mudam para um estado com falha. Desassocie o volume do host, exclua a sessão e, em seguida, crie a sessão novamente.

Alertas de backup remoto

A guia **Alertas** (em **Monitoramento**) exibe alertas gerais que são gerados para sessões de backup remoto, como criação e conclusão de sessões, adição ou remoção de um sistema remoto e assim por diante. Você pode filtrar alertas de backup remoto selecionando **Sessão remota** e **Sistema remoto** como Tipo de recurso.

Os alertas também são emitidos quando ocorrem falhas. O número de alertas é exibido nas guias **Sessões de backup** e **Recuperar sessões**. Clique no número para abrir a guia **Alertas**.

8

Backup NDMP para servidores NAS

Este tópico contém as seguintes informações:

Tópicos:

- Ativar o backup de NDMP

Ativar o backup de NDMP

Você pode configurar o backup padrão para os servidores NAS usando NDMP. O NDMP (Network Data Management Protocol, protocolo de gerenciamento de dados da rede) 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, pode detectar oPowerStoreNDMP usando o endereço IP do servidor NAS.

Sobre esta tarefa

O NDMP é realizado após a criação do servidor NAS.

PowerStoreé 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. Selecionar **Armazenamento** > **NAS Servers** > **[Servidor NAS]** > **Protection**.
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 **Apply**.

Próximas etapas

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

A

Resumo da replicação

Este apêndice contém as seguintes informações:

Tópicos:

- Resumo da replicação

Resumo da replicação

A tabela abaixo resume os vários atributos de replicação (síncrona e assíncrona) e do metro.

Tabela 5. Replicação e metro — resumo

Atributo	Replicação assíncrona	Replicação síncrona	Metro
Tipo compatível	Bloco e arquivo	Bloco e arquivo	Block
Recursos de armazenamento	Volumes, grupos de volumes, clones dinâmicos, servidores NAS, vVols	Volumes, grupos de volumes, clones dinâmicos, servidores NAS	Volumes, grupos de volumes
Tipo de replicação	Assíncrono	Síncrono	Síncrono
RPO de destino	Valor fixo 5 min - 24 h	0	0
Acesso do host	Ativo/passivo. Requer failover	Ativo/passivo. Requer um failover ou RTO>0. Para arquivo, exige failover automático.	Alteração do caminho ALUA ativo/ativo
Protocolos de host	SCSI, NVMe	SCSI, NVMe	SCSI
WWN/NQN em bloco	Diferente	Diferente	O mesmo WWN nas duas extremidades
Witness	Não	Arquivo — Sim Bloco - Não	Sim
RTT/distância	Não aplicável	5 milissegundos	5 milésimos de segundo*
Impacto do acesso ao host sobre o desempenho	Impacto mínimo, dependendo do dimensionamento e da carga de trabalho	Adiciona latência adicional (espelha o tempo de ida e volta)	Adiciona latência adicional (espelha o tempo de ida e volta)
Replicação de snapshots	Replicação de snapshots em bloco na origem. A replicação de snapshot para arquivo não é compatível.	Snapshots em bloco quase idênticos. A replicação de snapshot para arquivo não é compatível.	Snapshots quase idênticos
Teste de failover	Sim (por exemplo, arquivo, utilizando um clone)	Sim (por exemplo, arquivo, utilizando um clone)	Não aplicável
Conversão assíncrona <-> síncrona	Permitida para recursos de bloco. Não compatível com arquivo.	Permitida para recursos de bloco. Não compatível com arquivo.	Não compatível
Snapshot de recuperação	Base comum em cada ciclo de replicação	Compatível quando pausado	Não compatível
Upgrade não disruptivo	A replicação é pausada durante o NDU	Sessões ativas continuam	Sessões ativas continuam

1

1 Alguns aplicativos protegidos podem requerer RTT/distância inferior para configuração metro.

B

Casos de uso

Este tópico contém as seguintes informações:

Tópicos:

- Casos de uso de snapshots e clones thin
- Casos de uso de replicação
- Casos de uso de proteção Metro

Casos de uso de snapshots e clones thin

Você pode usar snapshots e clones thin para restaurar volumes corrompidos e criar ambientes de teste.

Os snapshots são cópias somente leitura que podem ser usadas para salvar o estado atual de um objeto. Você pode usá-los para recuperar rapidamente os dados se houver um erro de corrupção ou do usuário. Os snapshots não podem ser acessados diretamente por um host.

Os clones thin são cópias graváveis de um snapshot, volume ou Grupo de volumes que podem ser acessadas por um host. Os clones thin podem ser criados diretamente como uma cópia do objeto pai ou usando um de seus snapshots. Tanto os snapshots quanto os clones thin são cópias que fazem uso eficiente de espaço e compartilham blocos de dados com o objeto pai.

Usando snapshots e clones thin para recuperação parcial de um volume

Você pode usar snapshots e clones thin para recuperar parte de um volume, como arquivos individuais ou registros de base de dados, de um point-in-time anterior. Primeiro, crie um clone thin usando o snapshot que contém os dados que você precisa recuperar. Em seguida, dê acesso de host ao clone e recupere os dados do host.

Usando snapshots para restaurar um volume ou Grupo de volumes

Você pode usar os snapshots para reverter um volume a um point-in-time anterior se houver corrupção. Para reverter um volume ou Grupo de volumes para um point-in-time anterior, use a operação de restauração de volume e forneça um snapshot de antes da corrupção. A operação de restauração é instantânea. Você também pode criar um snapshot de backup para salvar o estado do volume ou Grupo de volumes antes de usar a operação de restauração.

Usando clones thin para testar um patch antes de aplicá-lo ao volume de produção

Antes de instalar um patch ou uma atualização de software de um aplicativo principal em um volume, você pode obter um clone thin do volume e aplicar a atualização ao clone thin. Depois de instalar a atualização e verificar se ela é segura para seu ambiente, você pode instalar a atualização nos outros volumes.

Criar clones thin para uso em desenvolvimento

Em vez de provisionar volumes ou grupos de volumes para cada desenvolvedor individual, você pode criar clones thin. A criação de clones thin do volume ou Grupo de volumes permite distribuir os mesmos dados e configurações para cada desenvolvedor. Os clones thin também ocupam menos espaço do que se você criar um clone completo do volume ou provisionar volumes individuais ou grupos de volumes. Você também pode obter snapshots de clones thin e replicá-los.

Casos de uso de replicação

Você pode usar a replicação para tempo de inatividade planejado, como durante a migração entre clusters, a instalação de uma atualização de software importante e uma recuperação de desastres.

Migração entre clusters

Se for necessário migrar um objeto de armazenamento para outro cluster do PowerStore, você poderá configurar uma replicação única entre os dois clusters, seguida de um failover planejado para o novo cluster para concluir a migração. Após a migração, desmonte o objeto de origem para recuperar o espaço no cluster original.

Usando réplicas para tempo de inatividade planejado

O tempo de inatividade planejado é uma situação em que você coloca off-line o sistema de origem para fins de manutenção ou teste, enquanto opera no sistema de destino. Antes do tempo de inatividade planejado, a origem e o destino são executados com uma sessão de replicação ativa. Não há perda de dados no tempo de inatividade planejado.

Nesse cenário, o sistema de origem (Boston) é colocado off-line para manutenção, e o sistema de destino (New York) é usado como sistema de produção durante o período de manutenção. Uma vez concluída a manutenção, a produção volta para o sistema Boston.

Para iniciar o tempo de inatividade planejado, selecione **Planned Failover** no sistema de origem Boston. O sistema de destino New York é completamente sincronizado com o de origem para garantir que não haja perda de dados. A sessão permanece pausada, enquanto o sistema de origem Boston se torna somente leitura e o de destino se torna leitura/gravação. O recurso de armazenamento de destino New York pode fornecer acesso ao host. No recurso de armazenamento de destino New York, selecione **Reprotect** para retomar a replicação na direção inversa.

Para retomar as operações no sistema Boston após a manutenção, selecione **Planned Failover** no sistema New York. Depois que o failover for concluído, use **Reprotect** no sistema Boston.

NOTA: Para replicar dados do destino para a origem com a operação Reprotect, confira se há uma política de replicação no sistema de destino com uma regra de replicação apontando para o sistema de origem. Por exemplo, se a sessão de replicação normal for de um local no sistema Boston para um local no sistema New York, a política de replicação no recurso de armazenamento de destino no New York deverá apontar para o Boston.

Usando réplicas para recuperação de desastres

Em um cenário de recuperação de desastres, o sistema de origem (Boston) fica indisponível devido a desastre natural ou falha humana. Foi criado um sistema de destino (New York) que contém uma réplica, ou seja, uma cópia completa dos dados de produção. O acesso aos dados pode ser restaurado mediante failover para New York porque uma sessão de replicação foi configurada entre os sistemas Boston e New York.

A utilização de réplicas para recuperação de desastres minimiza perdas de dados potenciais. A réplica é atualizada com a última sincronização do destino com a origem, conforme especificado na regra de replicação associada. A quantidade no caso de uma possível perda de dados baseia-se na configuração de RPO (Recovery Point Objective) da regra de replicação associada. A sessão de replicação pode sofrer failover para o sistema de destino New York, usando os dados mais recentes que foram replicados do sistema Boston.

Depois que a sessão sofrer failover para o sistema New York, ele se tornará leitura/gravação. Ao estabelecer originalmente uma sessão de replicação entre os sistemas de origem e destino, o recurso de armazenamento recebeu as permissões de acesso corretas para o host e o compartilhamento. A criação correta do acesso do host no sistema de destino diminui o tempo de inatividade em caso de desastre.

Para retomar as operações no sistema Boston, quando ele estiver disponível:

1. No sistema New York, selecione a opção **Reprotect**, que retoma a sessão de replicação na direção inversa.
2. Depois que os sistemas estiverem sincronizados, selecione a opção **Planned Failover** no sistema New York.
3. Marque a caixa de seleção para proteger o sistema automaticamente após o failover. Ou, após a conclusão do failover, no sistema Boston, selecione **Reprotect**.

NOTA: Para replicar dados do destino para a origem com a operação Reprotect, confira se há uma política de replicação no sistema de destino com uma regra de replicação apontando para o sistema de origem. Por exemplo, se a sessão de replicação for de um local no sistema Boston para um local no sistema New York, a política de replicação no recurso de armazenamento de destino no New York deverá apontar para o Boston.

Casos de uso de proteção Metro

Use a proteção metro para garantir alta disponibilidade, balanceamento de carga e migração de dados.

Usando Metro para alta disponibilidade

Um volume Metro é exposto usando dois storage arrays distintos que cooperam para expor um único volume Metro para os hosts de aplicativo fornecendo os mesmos dados e imagem SCSI. Os hosts e aplicativos em execução neles percebem dois volumes físicos como sendo um único volume com vários caminhos. Consequentemente, os hosts podem acessar os dois lados do volume Metro. Se houver uma perda de link ou uma falha em um dos sistemas, o acesso do host ainda poderá ser mantido para o sistema ativo.

A proteção Metro oferece replicação síncrona bidirecional, pela qual os dois lados do volume Metro podem ser usados para produção. Em vez de recuperação de desastres (fazendo failover de uma sessão de replicação para um sistema remoto), o Metro permite a prevenção de desastres fornecendo sincronização automática entre os sistemas sem tempo de inatividade.

Usando Metro para balanceamento de carga

Com o volume Metro do PowerStore, os data centers podem ser otimizados para usar totalmente os sistemas PowerStore por meio de um ambiente ativo/ativo que permite o balanceamento de carga de trabalho entre sistemas PowerStore. Mover aplicativos sem disrupção entre sistemas PowerStore é um processo simples e pode ser feito quando o balanceamento de desempenho ou de capacidade é necessário.

Usando Metro para migração

É possível usar volumes metro quando for necessário migrar cargas de trabalho entre sistemas PowerStore. O uso de volumes metro para migração é simples, além de diminuir o risco de perda de dados. Com a opção de volumes metro, a migração não causa interrupções. Após a conclusão da migração, é possível remover ou manter o volume metro para permitir uma recuperação rápida quando ocorre uma falha do sistema ou, até mesmo, uma falha em todo o local.