



Criar e solucionar problemas de relacionamentos de proteção

Active IQ Unified Manager

NetApp

October 15, 2025

This PDF was generated from https://docs.netapp.com/pt-br/active-iq-unified-manager-916/data-protection/concept_types_of_snapmirror_protection.html on October 15, 2025. Always check docs.netapp.com for the latest.

Índice

Criar, monitorar e solucionar problemas de relacionamentos de proteção	1
Tipos de proteção SnapMirror	1
Relacionamentos de proteção assíncronos tradicionais do SnapMirror	1
Proteção assíncrona SnapMirror com replicação flexível de versão	1
Proteção assíncrona SnapMirror com replicação flexível de versão e opção de backup	2
SnapMirror Unified Replication (espelho e cofre)	2
Proteção síncrona SnapMirror com sincronização estrita	2
Proteção síncrona SnapMirror com sincronização regular	2
Sincronização ativa do SnapMirror	2
Configurar relacionamentos de proteção no Unified Manager	3
Configurar uma conexão entre o Workflow Automation e o Unified Manager	3
Verificar o cache da fonte de dados do Unified Manager na Automação de Fluxo de Trabalho	4
O que acontece quando o OnCommand Workflow Automation é reinstalado ou atualizado	5
Remover a configuração do OnCommand Workflow Automation do Unified Manager	5
Executar failover e failback de relacionamento de proteção	5
Interromper um relacionamento SnapMirror na página de detalhes Volume/Saúde	6
Relações de proteção reversa da página de detalhes de Volume/Saúde	7
Remover um relacionamento de proteção da página de detalhes de Volume/Saúde	8
Ressincronizar relacionamentos de proteção na página de detalhes de Volume/Saúde	8
Resolver uma falha de trabalho de proteção	9
Identificar o problema e executar ações corretivas para um trabalho de proteção com falha	10
Resolver problemas de atraso	13

Criar, monitorar e solucionar problemas de relacionamentos de proteção

O Unified Manager permite que você crie relacionamentos de proteção, monitore e solucione problemas de proteção de espelho e proteção de cofre de backup de dados armazenados em clusters gerenciados e restaure dados quando eles forem substituídos ou perdidos.

Tipos de proteção SnapMirror

Dependendo da implantação da sua topologia de armazenamento de dados, o Unified Manager permite que você configure vários tipos de relacionamentos de proteção do SnapMirror. Todas as variações da proteção SnapMirror oferecem proteção de recuperação de desastres contra failover, mas oferecem diferentes recursos em desempenho, flexibilidade de versão e proteção de múltiplas cópias de backup.

Relacionamentos de proteção assíncronos tradicionais do SnapMirror

A proteção assíncrona tradicional do SnapMirror fornece proteção de espelhamento de replicação de bloco entre volumes de origem e destino.

Em relacionamentos SnapMirror tradicionais, as operações de espelhamento são executadas mais rapidamente do que em relacionamentos SnapMirror alternativos porque a operação de espelhamento é baseada na replicação de bloco. No entanto, a proteção tradicional do SnapMirror exige que o volume de destino seja executado na mesma versão secundária ou posterior do software ONTAP que o volume de origem na mesma versão principal (por exemplo, versão 8.x para 8.x ou 9.x para 9.x). A replicação de uma origem 9.1 para um destino 9.0 não é suportada porque o destino está executando uma versão principal anterior.

Proteção assíncrona SnapMirror com replicação flexível de versão

A proteção assíncrona do SnapMirror com replicação flexível de versão fornece proteção de espelhamento de replicação lógica entre volumes de origem e destino, mesmo se esses volumes estiverem sendo executados em versões diferentes do software ONTAP 8.3 ou posterior (por exemplo, versão 8.3 para 8.3.1, ou 8.3 para 9.1, ou 9.2.2 para 9.2).

Em relacionamentos SnapMirror com replicação flexível de versão, as operações de espelhamento não são executadas tão rapidamente quanto em relacionamentos SnapMirror tradicionais.

Devido à execução mais lenta, o SnapMirror com proteção de replicação flexível de versão não é adequado para implementação em nenhuma das seguintes circunstâncias:

- O objeto de origem contém mais de 10 milhões de arquivos a serem protegidos.
- O objetivo do ponto de recuperação para os dados protegidos é de duas horas ou menos. (Ou seja, o destino deve sempre conter dados espelhados e recuperáveis que não sejam mais de duas horas mais antigos que os dados na origem.)

Em qualquer uma das circunstâncias listadas, é necessária a execução mais rápida baseada em replicação de bloco da proteção padrão do SnapMirror.

Proteção assíncrona SnapMirror com replicação flexível de versão e opção de backup

A proteção assíncrona SnapMirror com replicação flexível de versão e opção de backup fornece proteção de espelhamento entre volumes de origem e destino e a capacidade de armazenar várias cópias dos dados espelhados no destino.

O administrador de armazenamento pode especificar quais cópias do Snapshot são espelhadas da origem para o destino e também pode especificar por quanto tempo essas cópias serão mantidas no destino, mesmo que sejam excluídas na origem.

Em relacionamentos SnapMirror com replicação flexível de versão e opção de backup, as operações de espelhamento não são executadas tão rapidamente quanto em relacionamentos SnapMirror tradicionais.

SnapMirror Unified Replication (espelho e cofre)

A replicação unificada do SnapMirror permite que você configure a recuperação de desastres e o arquivamento no mesmo volume de destino. Assim como no SnapMirror, a proteção de dados unificada executa uma transferência de linha de base na primeira vez que você a invoca. Uma transferência de linha de base sob a política de proteção de dados unificada padrão "MirrorAndVault" faz uma cópia instantânea do volume de origem e, em seguida, transfere essa cópia e os blocos de dados aos quais ela faz referência para o volume de destino. Assim como o SnapVault, a proteção de dados unificada não inclui cópias mais antigas do Snapshot na linha de base.

Proteção síncrona SnapMirror com sincronização estrita

A proteção síncrona do SnapMirror com sincronização "estrita" garante que os volumes primário e secundário sejam sempre uma cópia verdadeira um do outro. Se ocorrer uma falha de replicação ao tentar gravar dados no volume secundário, a E/S do cliente para o volume primário será interrompida.

Proteção síncrona SnapMirror com sincronização regular

A proteção síncrona do SnapMirror com sincronização "regular" não exige que o volume primário e o secundário sejam sempre uma cópia verdadeira um do outro, garantindo assim a disponibilidade do volume primário. Se ocorrer uma falha de replicação ao tentar gravar dados no volume secundário, os volumes primário e secundário ficarão fora de sincronia e a E/S do cliente continuará no volume primário.



O botão Restaurar e os botões Operação de relacionamento não estão disponíveis ao monitorar relacionamentos de proteção síncronos na exibição Integridade: Todos os volumes ou na página Detalhes do volume/integridade.

Sincronização ativa do SnapMirror

O recurso de sincronização ativa do SnapMirror está disponível com o ONTAP 9.8 e versões posteriores, e você pode usá-lo para proteger aplicativos com LUNs, permitindo que os aplicativos façam failover de forma transparente, garantindo a continuidade dos negócios em caso de desastre.

Ele permite que você descubra e monitore os relacionamentos síncronos do SnapMirror para Grupos de Consistência (CGs) disponíveis em clusters e máquinas virtuais de armazenamento do Unified Manager. A sincronização ativa do SnapMirror é suportada em clusters AFF ou clusters All SAN Array (ASA), onde os clusters primário e secundário podem ser AFF ou ASA. A sincronização ativa do SnapMirror protege aplicativos com LUNs iSCSI ou FCP.

Ao visualizar os volumes e LUNs protegidos pelo relacionamento de sincronização ativa do SnapMirror , você pode obter uma visão unificada dos relacionamentos de proteção, grupos de consistência no inventário de volume, visualizar a topologia de proteção para relacionamentos de grupo de consistência e visualizar dados históricos para relacionamentos de grupo de consistência de até um ano. Você também pode baixar o relatório. Você também pode visualizar o resumo dos relacionamentos do Grupo de Consistência, pesquisar suporte para relacionamentos do Grupo de Consistência e obter informações sobre volumes protegidos pelo Grupo de Consistência.

Na página Relacionamentos, você também pode classificar, filtrar e estender a proteção nos objetos de armazenamento de origem e destino e seus relacionamentos protegidos pelo Grupo de Consistência.

Para saber mais sobre a sincronização ativa do SnapMirror , consulte ["Documentação do ONTAP 9 para sincronização ativa do Snapmirror \(anteriormente SM-BC\)"](#) .

Configurar relacionamentos de proteção no Unified Manager

Há várias etapas que você deve executar para usar o Unified Manager e o OnCommand Workflow Automation para configurar relacionamentos do SnapMirror e do SnapVault para proteger seus dados.

Antes de começar

- Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.
- Você deve ter estabelecido relacionamentos de pares entre dois clusters ou duas máquinas virtuais de armazenamento (SVMs).
- O OnCommand Workflow Automation deve ser integrado ao Unified Manager:
 - ["Configurar a OnCommand Workflow Automation"](#).
 - ["Verificando o cache da fonte de dados do Unified Manager no Workflow Automation"](#).

Passos

1. Dependendo do tipo de relacionamento de proteção que você deseja criar, faça um dos seguintes:
 - ["Criar um relacionamento de proteção SnapMirror"](#).
 - ["Criar um relacionamento de proteção SnapVault"](#).
2. Se você quiser criar uma política para o relacionamento, dependendo do tipo de relacionamento que estiver criando, faça um dos seguintes procedimentos:
 - ["Criar uma política do SnapVault"](#).
 - ["Criar uma política do SnapMirror"](#).
3. ["Crie uma programação SnapMirror ou SnapVault"](#).

Configurar uma conexão entre o Workflow Automation e o Unified Manager

Você pode configurar uma conexão segura entre o OnCommand Workflow Automation (WFA) e o Unified Manager. A conexão com o Workflow Automation permite que você use recursos de proteção, como fluxos de trabalho de configuração do SnapMirror e do SnapVault , bem como comandos para gerenciar relacionamentos do SnapMirror .

Antes de começar

- A versão instalada do Workflow Automation deve ser 5.1.1P6 ou superior.



O “pacote WFA para gerenciar Clustered Data ONTAP” está incluído no WFA 5.1.1P6, portanto não há necessidade de baixar esse pacote do NetAppStorage Automation Store e instalá-lo separadamente no seu servidor WFA, como era necessário no passado. ["Pacote WFA para gerenciamento do ONTAP"](#)

- Você deve ter o nome do usuário do banco de dados criado no Unified Manager para dar suporte às conexões WFA e Unified Manager.

Este usuário do banco de dados deve ter recebido a função de usuário do Esquema de Integração.

- Você deve receber a função de Administrador ou a função de Arquiteto no Workflow Automation.
- Você deve ter o endereço do host, o número da porta 443, o nome de usuário e a senha para a configuração do Workflow Automation.
- Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.

Passos

1. No painel de navegação esquerdo, clique em **Geral > Automação de fluxo de trabalho**.
2. Na área **Usuário do banco de dados** da página **Automação de fluxo de trabalho**, selecione o nome e insira a senha do usuário do banco de dados que você criou para dar suporte às conexões do Unified Manager e da Automação de fluxo de trabalho.
3. Na área **Credenciais de automação de fluxo de trabalho** da página, insira o nome do host ou endereço IP (IPv4 ou IPv6), e o nome de usuário e a senha para a configuração de automação de fluxo de trabalho.

Você deve usar a porta do servidor do Unified Manager (porta 443).

4. Clique em **Salvar**.
5. Se você usar um certificado autoassinado, clique em **Sim** para autorizar o certificado de segurança.

A página Automação de fluxo de trabalho é exibida.

6. Clique em **Sim** para recarregar a interface da web e adicionar os recursos de automação de fluxo de trabalho.

Informações relacionadas

["Documentação da NetApp : OnCommand Workflow Automation \(versões atuais\)"](#)

Verificar o cache da fonte de dados do Unified Manager na Automação de Fluxo de Trabalho

Você pode determinar se o cache da fonte de dados do Unified Manager está funcionando corretamente verificando se a aquisição da fonte de dados foi bem-sucedida no Workflow Automation. Você pode fazer isso ao integrar o Workflow Automation ao Unified Manager para garantir que a funcionalidade do Workflow Automation esteja disponível após a integração.

Antes de começar

Você deve ter a função de Administrador ou a função de Arquiteto no Workflow Automation para executar esta

tarefa.

Passos

1. Na interface do usuário de automação de fluxo de trabalho, selecione **Execução > Fontes de dados**.
2. Clique com o botão direito do mouse no nome da fonte de dados do Unified Manager e selecione **Adquirir agora**.
3. Verifique se a aquisição foi bem-sucedida e sem erros.

Os erros de aquisição devem ser resolvidos para que a integração do Workflow Automation com o Unified Manager seja bem-sucedida.

O que acontece quando o OnCommand Workflow Automation é reinstalado ou atualizado

Antes de reinstalar ou atualizar o OnCommand Workflow Automation, você deve primeiro remover a conexão entre o OnCommand Workflow Automation e o Unified Manager e garantir que todos os trabalhos do OnCommand Workflow Automation em execução ou agendados sejam interrompidos.

Você também deve excluir manualmente o Unified Manager do OnCommand Workflow Automation.

Depois de reinstalar ou atualizar o OnCommand Workflow Automation, você deve configurar a conexão com o Unified Manager novamente.

Remover a configuração do OnCommand Workflow Automation do Unified Manager

Você pode remover a configuração do OnCommand Workflow Automation do Unified Manager quando não quiser mais usar o Workflow Automation.

Antes de começar

Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.

Passos

1. No painel de navegação esquerdo, clique em **Geral > Automação de fluxo de trabalho** no menu Configuração à esquerda.
2. Na página **Automação de fluxo de trabalho**, clique em **Remover configuração**.

Executar failover e failback de relacionamento de proteção

Quando um volume de origem no seu relacionamento de proteção é desabilitado devido a uma falha de hardware ou um desastre, você pode usar os recursos de relacionamento de proteção no Unified Manager para tornar o destino de proteção acessível para leitura/gravação e fazer failover para esse volume até que a origem esteja online novamente; então, você pode fazer failback para a origem original quando ela estiver disponível para fornecer dados.

Antes de começar

- Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.
- Você deve ter configurado o OnCommand Workflow Automation para executar esta operação.

Passos

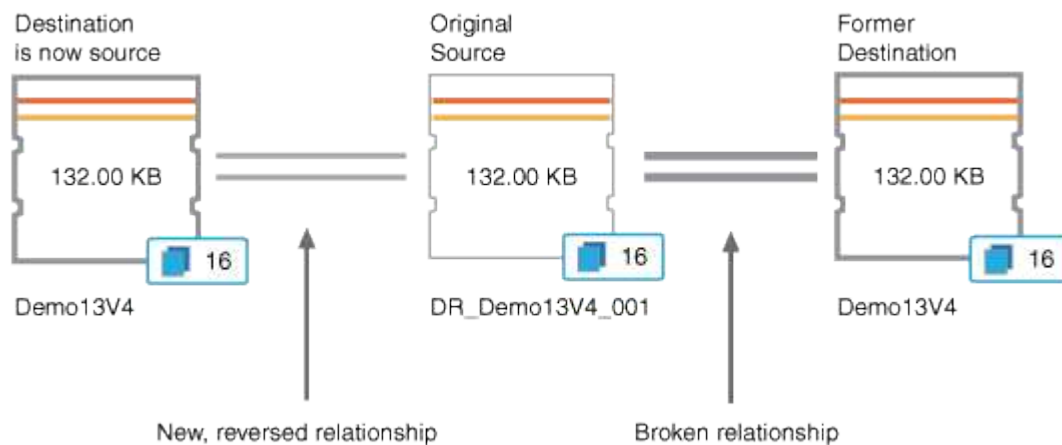
1. "Quebre o relacionamento com o SnapMirror".

Você deve interromper o relacionamento antes de poder converter o destino de um volume de proteção de dados para um volume de leitura/gravação e antes de poder reverter o relacionamento.

2. "Inverter a relação de proteção".

Quando o volume de origem original estiver disponível novamente, você poderá decidir restabelecer o relacionamento de proteção original restaurando o volume de origem. Antes de restaurar a origem, você deve sincronizá-la com os dados gravados no destino anterior. Use a operação de resincronização reversa para criar um novo relacionamento de proteção invertendo as funções do relacionamento original e sincronizando o volume de origem com o destino anterior. Uma nova cópia de Snapshot de base é criada para o novo relacionamento.

O relacionamento inverso é semelhante a um relacionamento em cascata:



3. "Quebre o relacionamento invertido do SnapMirror".

Quando o volume de origem original for resincronizado e puder servir dados novamente, use a operação break para quebrar o relacionamento invertido.

4. "Remover o relacionamento".

Quando o relacionamento invertido não for mais necessário, você deverá removê-lo antes de restabelecer o relacionamento original.

5. "Ressincronize o relacionamento".

Use a operação de resincronização para sincronizar dados da origem para o destino e restabelecer o relacionamento original.

Interromper um relacionamento SnapMirror na página de detalhes Volume/Saúde

Você pode quebrar um relacionamento de proteção na página de detalhes do Volume/Integridade e interromper as transferências de dados entre um volume de origem

e um volume de destino em um relacionamento SnapMirror . Você pode romper um relacionamento quando quiser migrar dados, para recuperação de desastres ou para testes de aplicativos. O volume de destino é alterado para um volume de leitura e gravação. Você não pode quebrar um relacionamento SnapVault .

Antes de começar

- Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.
- Você deve ter configurado a Automação de Fluxo de Trabalho.

Passos

1. Na guia **Proteção** da página de detalhes **Volume / Saúde**, selecione na topologia o relacionamento SnapMirror que você deseja quebrar.
2. Clique com o botão direito do mouse no destino e selecione **Quebrar** no menu.

A caixa de diálogo Romper relacionamento é exibida.

3. Clique em **Continuar** para encerrar o relacionamento.
4. Na topologia, verifique se o relacionamento foi quebrado.

Relações de proteção reversa da página de detalhes de Volume/Saúde

Quando um desastre desabilita o volume de origem no seu relacionamento de proteção, você pode usar o volume de destino para fornecer dados convertendo-os para leitura/gravação enquanto repara ou substitui a origem. Quando a origem estiver novamente disponível para receber dados, você poderá usar a operação de resincronização reversa para estabelecer o relacionamento na direção reversa, sincronizando os dados na origem com os dados no destino de leitura/gravação.

Antes de começar

- Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.
- Você deve ter configurado a Automação de Fluxo de Trabalho.
- O relacionamento não deve ser um relacionamento SnapVault .
- Uma relação de proteção já deve existir.
- A relação de proteção deve ser quebrada.
- Tanto a origem quanto o destino devem estar online.
- A origem não deve ser o destino de outro volume de proteção de dados.
- Ao executar esta tarefa, os dados na origem que são mais recentes que os dados na cópia comum do Snapshot são excluídos.
- As políticas e programações criadas no relacionamento de resincronização reversa são as mesmas que aquelas no relacionamento de proteção original.

Se políticas e cronogramas não existirem, eles serão criados.

Passos

1. Na guia **Proteção** da página de detalhes **Volume / Saúde**, localize na topologia o relacionamento SnapMirror no qual você deseja reverter a origem e o destino e clique com o botão direito do mouse.

2. Selecione **Ressincronização reversa** no menu.

A caixa de diálogo Ressincronização reversa é exibida.

3. Verifique se o relacionamento exibido na caixa de diálogo **Ressincronização reversa** é aquele para o qual você deseja executar a operação de ressincronização reversa e clique em **Enviar**.

A caixa de diálogo Ressincronização reversa é fechada e um link de tarefa é exibido na parte superior da página de detalhes Volume/Saúde.

4. **Opcional:** Clique em **Exibir trabalhos** na página de detalhes **Volume / Saúde** para rastrear o status de cada trabalho de ressincronização reversa.

Uma lista filtrada de trabalhos é exibida.

5. **Opcional:** Clique na seta **Voltar** no seu navegador para retornar à página de detalhes **Volume / Saúde**.

A operação de ressincronização reversa é concluída quando todas as tarefas do trabalho são concluídas com sucesso.

Remover um relacionamento de proteção da página de detalhes de Volume/Saúde

Você pode remover um relacionamento de proteção para excluir permanentemente um relacionamento existente entre a origem e o destino selecionados: por exemplo, quando você deseja criar um relacionamento usando um destino diferente. Esta operação remove todos os metadados e não pode ser desfeita.

Antes de começar

- Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.
- Você deve ter configurado a Automação de Fluxo de Trabalho.

Passos

1. Na guia **Proteção** da página de detalhes **Volume / Saúde**, selecione na topologia o relacionamento SnapMirror que você deseja remover.
2. Clique com o botão direito do mouse no nome do destino e selecione **Remover** no menu.

A caixa de diálogo Remover relacionamento é exibida.

3. Clique em **Continuar** para remover o relacionamento.

O relacionamento é removido da página de detalhes Volume/Saúde.

Ressincronizar relacionamentos de proteção na página de detalhes de Volume/Saúde

Você pode ressincronizar dados em um relacionamento SnapMirror ou SnapVault que foi quebrado e então o destino foi transformado em leitura/gravação para que os dados na origem correspondam aos dados no destino. Você também pode ressincronizar quando uma cópia comum necessária do Snapshot no volume de origem for excluída, causando falha nas atualizações do SnapMirror ou SnapVault .

Antes de começar

- Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.
- Você deve ter configurado o OnCommand Workflow Automation.

Passos

1. Na guia **Proteção** da página de detalhes **Volume / Saúde**, localize na topologia o relacionamento de proteção que você deseja ressincronizar e clique com o botão direito do mouse.

2. Selecione **Ressincronizar** no menu.

Como alternativa, no menu **Ações**, selecione **Relacionamento > Ressincronizar** para ressincronizar o relacionamento cujos detalhes você está visualizando no momento.

A caixa de diálogo Ressincronizar é exibida.

3. Na aba **Opções de ressincronização**, selecione uma prioridade de transferência e a taxa máxima de transferência.

4. Clique em **Cópias de instantâneo de origem**; em seguida, na coluna **Cópia de instantâneo**, clique em **Padrão**.

A caixa de diálogo Selecionar cópia do instantâneo de origem é exibida.

5. Se você quiser especificar uma cópia de Snapshot existente em vez de transferir a cópia de Snapshot padrão, clique em **Cópia de Snapshot existente** e selecione uma cópia de Snapshot na lista.

6. Clique em **Enviar**.

Você retornará à caixa de diálogo Ressincronizar.

7. Se você selecionou mais de uma fonte para ressincronizar, clique em **Padrão** para a próxima fonte para a qual deseja especificar uma cópia de Snapshot existente.

8. Clique em **Enviar** para iniciar o trabalho de ressincronização.

O trabalho de ressincronização é iniciado, você retorna à página de detalhes de Volume/Saúde e um link de trabalhos é exibido na parte superior da página.

9. **Opcional:** Clique em **Exibir trabalhos** na página **Detalhes do volume/saúde** para rastrear o status de cada trabalho de ressincronização.

Uma lista filtrada de trabalhos é exibida.

10. **Opcional:** Clique na seta **Voltar** no seu navegador para retornar à página de detalhes **Volume / Saúde**.

O trabalho de ressincronização é concluído quando todas as tarefas são concluídas com sucesso.

Resolver uma falha de trabalho de proteção

Este fluxo de trabalho fornece um exemplo de como você pode identificar e resolver uma falha de tarefa de proteção no painel do Unified Manager.

Antes de começar

Como algumas tarefas neste fluxo de trabalho exigem que você efetue login usando a função de Administrador, você deve estar familiarizado com as funções necessárias para usar várias funcionalidades.

Neste cenário, você acessa a página Painel para verificar se há algum problema com seus trabalhos de proteção. Na área Incidente de Proteção, você percebe que há um incidente de Trabalho Encerrado, mostrando um erro de Falha de Trabalho de Proteção em um volume. Você investiga esse erro para determinar a possível causa e a possível resolução.

Passos

1. No painel Incidentes de proteção da área Incidentes e riscos não resolvidos do painel, clique no evento **Falha na tarefa de proteção**.



O texto vinculado ao evento é escrito no formato `object_name:/object_name - Error Name`, como `cluster2_src_svm:/cluster2_src_vol2 - Protection Job Failed`.

A página Detalhes do evento para a tarefa de proteção com falha é exibida.

2. Revise a mensagem de erro no campo Causa da área **Resumo** para determinar o problema e avaliar possíveis ações corretivas.

Ver ["Identificar o problema e executar ações corretivas para um trabalho de proteção com falha"](#).

Identificar o problema e executar ações corretivas para um trabalho de proteção com falha

Você analisa a mensagem de erro de falha da tarefa no campo Causa na página Detalhes do evento e determina que a tarefa falhou devido a um erro de cópia do instantâneo. Em seguida, prossiga para a página de detalhes Volume/Saúde para coletar mais informações.

Antes de começar

Você deve ter a função de Administrador do Aplicativo.

A mensagem de erro fornecida no campo Causa na página Detalhes do evento contém o seguinte texto sobre a tarefa com falha:

```
Protection Job Failed. Reason: (Transfer operation for
relationship 'cluster2_src_svm:cluster2_src_vol2->cluster3_dst_svm:
managed_svc2_vol3' ended unsuccessfully. Last error reported by
Data ONTAP: Failed to create Snapshot copy 0426cluster2_src_vol2snap
on volume cluster2_src_svm:cluster2_src_vol2. (CSM: An operation
failed due to an ONC RPC failure.)
Job Details
```

Esta mensagem fornece as seguintes informações:

- Um trabalho de backup ou espelhamento não foi concluído com sucesso.

O trabalho envolveu uma relação de proteção entre o volume de origem `cluster2_src_vol2` no servidor virtual `cluster2_src_svm` e o volume de destino `managed_svc2_vol3` no servidor virtual chamado `cluster3_dst_svm`.

- Falha no trabalho de cópia do Snapshot para 0426cluster2_src_vol2snap no volume de origem cluster2_src_svm:/cluster2_src_vol2 .

Neste cenário, você pode identificar a causa e possíveis ações corretivas da falha do trabalho. No entanto, para resolver a falha, é necessário acessar a interface da Web do System Manager ou os comandos da CLI do ONTAP .

Passos

1. Você analisa a mensagem de erro e determina que uma tarefa de cópia do Snapshot falhou no volume de origem, indicando que provavelmente há um problema com seu volume de origem.

Opcionalmente, você pode clicar no link **Detalhes do trabalho** no final da mensagem de erro, mas para os propósitos deste cenário, você escolhe não fazer isso.

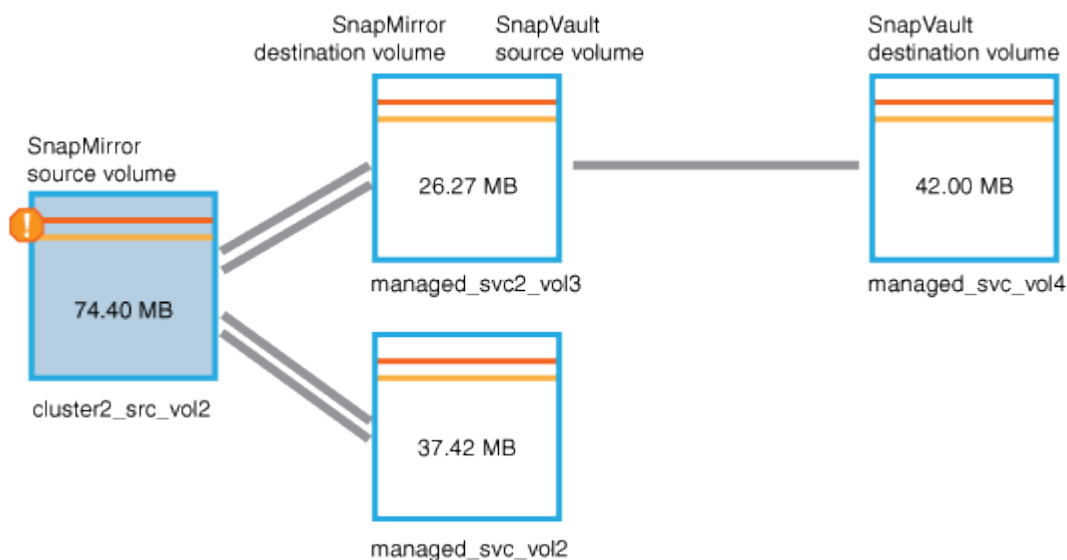
2. Você decide que quer tentar resolver o evento, então faz o seguinte:
 - a. Clique no botão **Atribuir a** e selecione **Eu** no menu.
 - b. Clique no botão **Reconhecer** para que você não continue recebendo notificações de alerta repetidas, caso alertas tenham sido definidos para o evento.
 - c. Opcionalmente, você também pode adicionar notas sobre o evento.
3. Clique no campo **Fonte** no painel **Resumo** para ver detalhes sobre o volume de origem.

O campo **Origem** contém o nome do objeto de origem: neste caso, o volume no qual o trabalho de cópia do Snapshot foi agendado.

A página de detalhes do Volume/Saúde é exibida para cluster2_src_vol2 , mostrando o conteúdo da aba Proteção.

4. Observando o gráfico de topologia de proteção, você vê um ícone de erro associado ao primeiro volume na topologia, que é o volume de origem do relacionamento SnapMirror .

Você também vê as barras horizontais no ícone do volume de origem, indicando os limites de aviso e erro definidos para esse volume.



5. Coloque o cursor sobre o ícone de erro para ver a caixa de diálogo pop-up que exibe as configurações de limite e veja que o volume excedeu o limite de erro, indicando um problema de capacidade.

6. Clique na aba **Capacidade**.

Informações de capacidade sobre volume `cluster2_src_vol2` exibe.

7. No painel **Capacidade**, você vê que há um ícone de erro no gráfico de barras, indicando novamente que a capacidade do volume ultrapassou o nível limite definido para o volume.
8. Abaixo do gráfico de capacidade, você vê que o crescimento automático de volume foi desabilitado e que uma garantia de espaço de volume foi definida.

Você pode decidir habilitar o crescimento automático, mas para os propósitos deste cenário, você decide investigar mais antes de tomar uma decisão sobre como resolver o problema de capacidade.

9. Você rola para baixo até a lista **Eventos** e vê que os eventos Falha na tarefa de proteção, Dias de volume até o limite máximo e Espaço de volume cheio foram gerados.
10. Na lista **Eventos**, clique no evento **Espaço de volume cheio** para obter mais informações, tendo decidido que esse evento parece mais relevante para seu problema de capacidade.

A página Detalhes do evento exibe o evento Espaço de volume cheio para o volume de origem.

11. Na área **Resumo**, você lê o campo Causa do evento: The full threshold set at 90% is breached. 45.38 MB (95.54%) of 47.50 MB is used.
12. Abaixo da área Resumo, você vê Ações corretivas sugeridas.



As Ações Corretivas Sugeridas são exibidas apenas para alguns eventos, portanto você não vê essa área para todos os tipos de eventos.

Clique na lista de ações sugeridas que você pode executar para resolver o evento Espaço de Volume Cheio:

- Habilite o crescimento automático neste volume.
- Redimensione o volume.
- Habilite e execute a deduplicação neste volume.
- Habilite e execute a compactação neste volume.

13. Você decide habilitar o crescimento automático no volume, mas para isso, você deve determinar o espaço livre disponível no agregado pai e a taxa de crescimento do volume atual:

- a. Observe o agregado pai, `cluster2_src_aggr1`, no painel **Dispositivos relacionados**.



Você pode clicar no nome do agregado para obter mais detalhes sobre ele.

Você determina que o agregado tem espaço suficiente para habilitar o crescimento automático de volume.

- b. No topo da página, observe o ícone que indica um incidente crítico e revise o texto abaixo do ícone.

Você determina que "Dias para atingir a plenitude: Menos de um dia | Taxa de crescimento diária: 5,4%".

14. Vá para o Gerenciador de Sistema ou acesse o ONTAP CLI para habilitar o volume `autogrow` opção.



Anote os nomes do volume e do agregado para que eles estejam disponíveis ao habilitar o crescimento automático.

15. Após resolver o problema de capacidade, retorne à página de detalhes do **Evento** do Unified Manager e marque o evento como resolvido.

Resolver problemas de atraso

Este fluxo de trabalho fornece um exemplo de como você pode resolver um problema de atraso. Neste cenário, você é um administrador ou operador acessando a página Unified Manager Dashboard para verificar se há algum problema com seus relacionamentos de proteção e, se houver, encontrar soluções.

Antes de começar

Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.

Na página Painel, você olha a área Incidentes e riscos não resolvidos e vê um erro de atraso do SnapMirror no painel Proteção em Riscos de proteção.

Passos

1. No painel **Proteção** na página **Painel**, localize o erro de atraso no relacionamento do SnapMirror e clique nele.

A página Detalhes do evento para o evento de erro de atraso é exibida.

2. Na página de detalhes do **Evento**, você pode executar uma ou mais das seguintes tarefas:
 - Revise a mensagem de erro no campo Causa da área Resumo para determinar se há alguma ação corretiva sugerida.
 - Clique no nome do objeto, neste caso um volume, no campo Origem da área Resumo para obter detalhes sobre o volume.
 - Procure por notas que possam ter sido adicionadas sobre este evento.
 - Adicione uma nota ao evento.
 - Atribua o evento a um usuário específico.
 - Reconheça ou resolva o evento.
3. Neste cenário, você clica no nome do objeto (neste caso, um volume) no campo Origem da área **Resumo** para obter detalhes sobre o volume.

A guia Proteção da página de detalhes Volume/Saúde é exibida.

4. Na aba **Proteção**, você vê o diagrama de topologia.

Observe que o volume com o erro de atraso é o último volume em uma cascata SnapMirror de três volumes. O volume selecionado é contornado em cinza escuro, e uma linha laranja dupla do volume de origem indica um erro de relacionamento do SnapMirror .



5. Clique em cada um dos volumes na cascata do SnapMirror .

Conforme você seleciona cada volume, as informações de proteção nas áreas Resumo, Topologia, Histórico, Eventos, Dispositivos relacionados e Alertas relacionados mudam para exibir detalhes relevantes ao volume selecionado.

6. Você olha para a área **Resumo** e posiciona o cursor sobre o ícone de informações no campo **Atualizar cronograma** para cada volume.

Neste cenário, você observa que a política do SnapMirror é DPDefault, e a programação do SnapMirror é atualizada a cada hora, cinco minutos após a hora. Você percebe que todos os volumes no relacionamento estão tentando concluir uma transferência do SnapMirror ao mesmo tempo.

7. Para resolver o problema de atraso, modifique os agendamentos de dois dos volumes em cascata para que cada destino inicie uma transferência do SnapMirror depois que sua origem tiver concluído uma transferência.

Informações sobre direitos autorais

Copyright © 2025 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTES DOCUMENTOS. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALIENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTES DOCUMENTOS, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

Informações sobre marcas comerciais

NETAPP, o logotipo NETAPP e as marcas listadas em <http://www.netapp.com/TM> são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.