Criar e solucionar problemas em relacionamentos de proteção

Active IQ Unified Manager

NetApp
November 13, 2026

This PDF was generated from https://docs.netapp.com/pt-br/active-iq-unified-manager-918/data-protection/concept_types_of_snapmirror_protection.html on November 13, 2026. Always check docs.netapp.com for the latest.

Índice

Criar e solucionar problemas em relacionamentos de proteção . . . 1
Tipos de proteção do SnapMirror no Active IQ Unified Manager . . . 1
Relacionamentos tradicionais de proteção assíncrona do SnapMirror . . . 1
SnapMirror Proteção assíncrona com replicação flexível entre versões . . . 1
SnapMirror Proteção assíncrona com replicação flexível em relação à versão e opção de backup . . . 2
SnapMirror Replicação unificada (espelhamento e cofre) . . . 2
SnapMirror Proteção síncrona com sincronização rigorosa . . . 2
SnapMirror proteção síncrona com sincronização regular . . . 2
SnapMirror active sync . . . 2
Configure relações de proteção no Unified Manager . . . 3
Configure relações de proteção no Active IQ Unified Manager . . . 3
Configure uma conexão entre o OnCommand Workflow Automation e o Active IQ Unified Manager . . . 3
Verifique o Active IQ Unified Manager armazenamento em cache na Automação de Fluxo de Trabalho . . . 4
Como a reinstalação ou atualização do OnCommand Workflow Automation afeta o Active IQ Unified Manager . . . 5
Remova a configuração do OnCommand Workflow Automation do Active IQ Unified Manager . . . 5
Execute um failover e failback de uma relação de proteção . . . 5
Execute um failover e failback de uma relação de proteção no Active IQ Unified Manager . . . 5
Interrompa uma relação de proteção do SnapMirror na página Volume/Saúde do Active IQ Unified Manager . . . 7
Reverta as relações de proteção na página de detalhes de Volume/Saúde no Active IQ Unified Manager . . . 7
Remova uma relação de proteção da página Detalhes de Volume/Saúde em Active IQ Unified Manager . . . 8
Ressincronize as relações de proteção na página de detalhes de Volume/Integridade no Active IQ Unified Manager . . . 9
Resolver uma falha em uma tarefa de proteção . . . 10
Resolver uma falha em uma tarefa de proteção no Active IQ Unified Manager . . . 10
Identifique o problema e execute ações corretivas para uma tarefa de proteção com falha no Active IQ Unified Manager . . . 10
Resolva problemas de latência no Active IQ Unified Manager . . . 13

Criar e solucionar problemas em relacionamentos de proteção

Tipos de proteção do SnapMirror no Active IQ Unified Manager

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

Relacionamentos tradicionais de proteção assíncrona do SnapMirror

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

Em relacionamentos tradicionais do SnapMirror, as operações de espelhamento são executadas mais rapidamente do que em relacionamentos alternativos do SnapMirror, porque a operação de espelhamento se baseia na replicação de blocos. No entanto, a proteção tradicional do SnapMirror exige que o volume de destino execute a mesma versão secundária ou uma versão secundária posterior do software ONTAP que o volume de origem, dentro da mesma versão principal (por exemplo, versão 8.x para 8.x ou 9.x para 9.x). Não há suporte para replicação de uma origem 9.1 para um destino 9.0, porque o destino está executando uma versão principal anterior.

SnapMirror Proteção assíncrona com replicação flexível entre versões

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

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

Devido à execução mais lenta, a proteção de replicação com flexibilidade de versão do SnapMirror não é adequada para implementação em nenhuma das seguintes circunstâncias:

- O objeto de origem contém mais de 10 milhões de arquivos a serem protegidos.
- O objetivo de 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 antigos do que duas horas em relação aos dados na origem.)

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

SnapMirror Proteção assíncrona com replicação flexível em relação à versão e opção de backup

O SnapMirror oferece proteção assíncrona com replicação flexível em relação à versão e opção de backup, fornecendo proteção de espelhamento entre os volumes de origem e de destino, além da capacidade de armazenar várias cópias dos dados espelhados no destino.

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

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

SnapMirror Replicação unificada (espelhamento 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 o SnapMirror, a proteção unificada de dados realiza uma transferência completa na primeira vez que você a invoca. Uma transferência completa sob a política padrão de proteção unificada de dados “MirrorAndVault” cria uma cópia Snapshot 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 unificada de dados não inclui cópias Snapshot mais antigas na transferência completa inicial.

SnapMirror Proteção síncrona com sincronização rigorosa

A proteção síncrona do SnapMirror com sincronização ""“strict”"" garante que os volumes primário e secundário sejam sempre cópias fiéis 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.

SnapMirror proteção síncrona com sincronização regular

SnapMirror A proteção síncrona com sincronização “regular” não exige que os volumes primário e secundário sejam sempre cópias exatas 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 dessincronizados, e a E/S do cliente continuará no volume primário.



O botão Restaurar e os botões de operação de relacionamento não estão disponíveis ao monitorar relacionamentos de proteção síncrona na visualização Saúde: todos os volumes ou na página de detalhes de Volume/Saúde.

SnapMirror active sync

O recurso de sincronização ativa do SnapMirror está disponível com 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 e 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 storage do Unified Manager. SnapMirror active sync é compatível com clusters AFF ou clusters All SAN Array (ASA), em que os clusters primário e secundário podem ser AFF ou ASA. SnapMirror active sync protege aplicações com LUNs iSCSI ou FCP.

Ao visualizar os volumes e LUNs protegidos pela relação de sincronização ativa do SnapMirror, você pode obter uma visão unificada das relações de proteção, dos Grupos de Consistência no inventário de volumes, visualizar a topologia de proteção das relações de Grupo de Consistência e visualizar dados históricos das relações de Grupo de Consistência por até um ano. Você também pode baixar o relatório. Você também pode visualizar o resumo das relações de Grupo de Consistência, pesquisar relações de Grupo de Consistência e obter informações sobre os volumes protegidos pelo Grupo de Consistência.

Na página Relacionamentos, você também pode classificar, filtrar e estender a proteção dos objetos de storage de origem e destino e de seu relacionamento que são protegidos pelo Consistency Group.

Para saber mais sobre o SnapMirror active sync, consulte "Documentação do ONTAP 9 para Snapmirror active sync (anteriormente SM-BC)".

Configure relações de proteção no Unified Manager

Configure relações de proteção no Active IQ Unified Manager

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

Antes de começar

- Você precisa ter a função de Application Administrator ou Storage Administrator.
- Você deve ter estabelecido relacionamentos de peering entre dois clusters ou duas máquinas virtuais de armazenamento (SVMs).
- O OnCommand Workflow Automation deve ser integrado ao Unified Manager:
  - "Configure o OnCommand Workflow Automation".
  - "Verificando o armazenamento em cache da fonte de dados do Unified Manager no Workflow Automation".

Passos

1. Dependendo do tipo de relação de proteção que você deseja criar, faça um dos seguintes procedimentos:
   - "Criar uma relação de proteção do SnapMirror".
   - "Criar uma relação de proteção do SnapVault".
2. Se você deseja criar uma política para o relacionamento, dependendo do tipo de relacionamento que está criando, faça um dos seguintes procedimentos:
   - "Criar uma política do SnapVault".
   - "Criar uma política do SnapMirror".
3. "Crie um agendamento do SnapMirror ou do SnapVault".

Configure uma conexão entre o OnCommand Workflow Automation e o Active IQ 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, além de 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 gerenciamento de Clustered Data ONTAP" está incluído no WFA 5.1.1P6, portanto, não é necessário baixar este pacote da NetAppStorage Automation Store e instalá-lo separadamente em seu servidor WFA, como era necessário anteriormente. "Download WFA"

- Você precisa ter o nome do usuário do banco de dados que você criou no Unified Manager para dar suporte às conexões do WFA e do Unified Manager.

  Este usuário do banco de dados deve ter recebido a função de usuário Integration Schema.

- Você precisa ter a função de Administrador ou a função de Arquiteto atribuída no Workflow Automation.
- Você precisa ter o endereço do host, o número da porta 443, o nome de usuário e a senha para a configuração do Workflow Automation.
- Você precisa ter a função de Application Administrator ou Storage Administrator.

Passos

1. No painel de navegação esquerdo, clique em **General** > **Workflow Automation**.
2. Na área **Usuário do Banco de Dados** da **página do Workflow Automation**, 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 do Workflow Automation.
3. Na área **Workflow Automation Credentials** da página, insira o nome do host ou o endereço IP (IPv4 ou IPv6), bem como o nome de usuário e a senha para a configuração do Workflow Automation.

   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 Workflow Automation é exibida.

6. Clique em **Sim** para recarregar a IU da web, e adicionar os recursos do Workflow Automation.

Informações relacionadas

"NetApp documentação: o OnCommand Workflow Automation (versões atuais)"

Verifique o Active IQ Unified Manager armazenamento em cache na Automação de Fluxo de Trabalho

Você pode determinar se o armazenamento em 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 com o Unified Manager para garantir que a funcionalidade do Workflow Automation esteja disponível após a integração.

Antes de começar

Para executar esta tarefa, você precisa ter a função Administrator ou a função Architect atribuída no Workflow

Automation.

Passos

1. Na interface de usuário do Workflow Automation, selecione **Execução** > **Fontes de dados**.
2. Clique com o botão direito do mouse no nome da fonte de dados do Unified Manager e selecione **Acquire Now**.
3. Verifique se a aquisição é concluída com sucesso, sem erros.

   Para que a integração do Workflow Automation com o Unified Manager seja bem-sucedida, é necessário resolver os erros de aquisição.

Como a reinstalação ou atualização do OnCommand Workflow Automation afeta o Active IQ Unified Manager

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 atualmente em execução ou agendados sejam interrompidos.

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

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

Remova a configuração do OnCommand Workflow Automation do Active IQ 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 precisa ter a função de Application Administrator ou Storage Administrator.

Passos

1. No painel de navegação esquerdo, clique em **General** > **Workflow Automation** no menu Setup à esquerda.
2. Na página **Workflow Automation**, clique em **Remove Setup**.

Execute um failover e failback de uma relação de proteção

Execute um failover e failback de uma relação de proteção no Active IQ Unified Manager

Quando um volume de origem em seu relacionamento de proteção é desativado devido a uma falha de hardware ou a 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 fique online novamente; em seguida, você pode retornar à origem original quando ela estiver

disponível para fornecer dados.

Antes de começar

- Você precisa ter a função de Application Administrator ou Storage Administrator.
- Você precisa ter configurado o OnCommand Workflow Automation para executar esta operação.

Passos

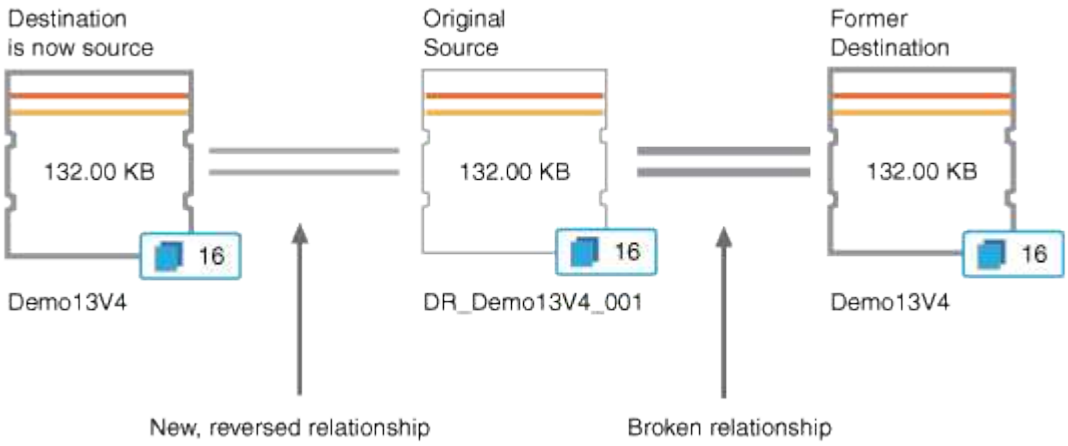
1. "Rompa a relação do SnapMirror".

   Você deve romper a relação antes de poder converter o destino de um volume de proteção de dados em um volume de leitura/gravação e antes de poder reverter a relação.

2. "Inverta a relação de proteção".

   Quando o volume de origem original estiver disponível novamente, você poderá optar por restabelecer a relação de proteção original restaurando o volume de origem. Antes de restaurar a origem, você deve sincronizá-la com os dados gravados no antigo destino. Você usa a operação de ressincronização reversa para criar uma nova relação de proteção, invertendo as funções da relação original e sincronizando o volume de origem com o antigo destino. Uma nova cópia Snapshot de linha de base é criada para a nova relação.

   A relação inversa é semelhante a uma relação em cascata:



3. "Quebre a relação do SnapMirror invertida".

   Quando o volume de origem original for ressincronizado e puder novamente fornecer dados, use a operação de interrupção para quebrar a relação invertida.

4. "Remova o relacionamento".

   Quando a relação inversa não for mais necessária, você deve removê-la antes de restabelecer a relação original.

5. "Ressincronizar a relação".

   Use a operação de ressincronização para sincronizar os dados da origem para o destino e restabelecer a relação original.

Interrompa uma relação de proteção do SnapMirror na página Volume/Saúde do Active IQ Unified Manager

Você pode romper uma relação de proteção na página Volume / Health details e interromper as transferências de dados entre um volume de origem e um volume de destino em uma relação do SnapMirror. Você pode romper uma relação quando quiser migrar dados, para recuperação de desastres ou para testes de aplicativos. O volume de destino é alterado para um volume de leitura/gravação. Você não pode romper uma relação do SnapVault.

Antes de começar

- Você precisa ter a função de Application Administrator ou Storage Administrator.
- Você precisa ter configurado o Workflow Automation.

Passos

1. Na aba **Proteção** da página de detalhes **Volume / Saúde**, selecione na topologia a relação do SnapMirror que você deseja interromper.
2. Clique com o botão direito do mouse no destino e selecione **Break** no menu.

   A caixa de diálogo "Break Relationship" é exibida.

3. Clique em **Continuar** para interromper a relação.
4. Na topologia, verifique se a relação está rompida.

Reverta as relações de proteção na página de detalhes de Volume/Saúde no Active IQ Unified Manager

Quando um desastre desativa o volume de origem na sua relação de proteção, você pode usar o volume de destino para fornecer dados, convertendo-o em leitura/gravação enquanto repara ou substitui o volume de origem. Quando a origem estiver novamente disponível para receber dados, você pode usar a operação de ressincronização reversa para estabelecer a relação na direção inversa, sincronizando os dados na origem com os dados no destino de leitura/gravação.

Antes de começar

- Você precisa ter a função de Application Administrator ou Storage Administrator.
- Você precisa ter configurado o Workflow Automation.
- A relação não deve ser uma relação do SnapVault.
- Já deve existir uma relação de proteção.
- A relação de proteção deve ser rompida.
- 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 forem mais recentes do que os dados na cópia Snapshot comum serão excluídos.
- As políticas e os cronogramas criados na relação de ressincronização reversa são os mesmos da relação de proteção original.

Se as políticas e os cronogramas não existirem, eles serão criados.

Passos

1. Na guia **Proteção** da página de detalhes **Volume / Saúde**, localize na topologia a relação do SnapMirror na qual você deseja inverter a origem e o destino e clique nela com o botão direito do mouse.
2. Selecione **Reverse Resync** no menu.

   A caixa de diálogo "Reverse Resync" é exibida.

3. Verifique se o relacionamento exibido na caixa de diálogo **Reverse Resync** é aquele para o qual você deseja executar a operação de ressincronização inversa e clique em **Submit**.

   A caixa de diálogo "Reverse Resync" é fechada, e um link do trabalho é exibido na parte superior da página de detalhes Volume / Health.

4. **Opcional:** clique em **View Jobs** na página de detalhes **Volume / Health** para acompanhar o status de cada trabalho de ressincronização reversa.

   Uma lista filtrada de tarefas é exibida.

5. **Opcional:** clique na seta **Voltar** do seu navegador para retornar à página de detalhes de **Volume / Saúde**.

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

Remova uma relação de proteção da página Detalhes de Volume/Saúde em Active IQ Unified Manager

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

Antes de começar

- Você precisa ter a função de Application Administrator ou Storage Administrator.
- Você precisa ter configurado o Workflow Automation.

Passos

1. Na aba **Proteção** da página de detalhes **Volume / Saúde**, selecione na topologia a relação do 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 a relação.

   A relação foi removida da página de detalhes de Volume / Health.

Ressincronize as relações de proteção na página de detalhes de Volume/Integridade no Active IQ Unified Manager

Você pode ressincronizar dados em uma relação do SnapMirror ou do SnapVault que foi interrompida e, em seguida, o destino foi configurado como leitura/gravação, para que os dados na origem correspondam aos dados no destino. Você também pode ressincronizar quando uma cópia Snapshot comum necessária no volume de origem é excluída, fazendo com que as atualizações do SnapMirror ou do SnapVault falhem.

Antes de começar

- Você precisa ter a função de Application Administrator ou Storage Administrator.
- Você precisa ter configurado o OnCommand Workflow Automation.

Passos

1. Na guia **Protection** da página de detalhes **Volume / Health**, localize na topologia a relação de proteção que você deseja ressincronizar e clique com o botão direito do mouse sobre ela.
2. Selecione **Resynchronize** no menu.

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

   A caixa de diálogo Ressincronizar é exibida.

3. Na aba **Opções de Ressincronização**, selecione uma prioridade de transferência e a taxa de transferência máxima.
4. Clique em **Cópias Snapshot de origem**; em seguida, na coluna **Cópia Snapshot**, clique em **Padrão**.

   A caixa de diálogo Selecionar cópia Snapshot de origem é exibida.

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

   Você retorna à caixa de diálogo Ressincronizar.

7. Se você selecionou mais de uma origem para ressincronizar, clique em **Default** para a próxima origem para a qual deseja especificar uma cópia Snapshot existente.
8. Clique em **Submit** para iniciar a tarefa de ressincronização.

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

9. **Opcional:** clique em **Ver trabalhos** na página **Detalhes de volume/integridade** para acompanhar o status de cada trabalho de ressincronização.

   Uma lista filtrada de tarefas é exibida.

10. **Opcional:** clique na seta **Voltar** do seu navegador para retornar à página de detalhes de **Volume / Saúde**.

    O processo de ressincronização termina quando todas as tarefas do trabalho são concluídas com sucesso.

Resolver uma falha em uma tarefa de proteção

Resolver uma falha em uma tarefa de proteção no Active IQ Unified Manager

Este fluxo de trabalho fornece um exemplo de como você pode identificar e resolver uma falha em uma tarefa de proteção a partir do painel do Unified Manager.

Antes de começar

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

Nesse cenário, você acessa a página Dashboard para ver se há algum problema com suas tarefas de proteção. Na área Protection Incident, você percebe que há um incidente Job Terminated, mostrando um erro Protection Job Failed em um volume. Você investiga esse erro para determinar a possível causa e a possível solução.

Passos

1. No painel "Incidentes de proteção" da área "Incidentes e riscos não resolvidos" do Dashboard, 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 de detalhes do evento para a tarefa de proteção com falha é exibida.

2. Analise a mensagem de erro no campo Cause da área **Summary** para determinar o problema e avaliar possíveis ações corretivas.

   Consulte "Identificar o problema e executar ações corretivas para uma falha na tarefa de proteção".

Identifique o problema e execute ações corretivas para uma tarefa de proteção com falha no Active IQ Unified Manager

Você analisa a mensagem de erro de falha da tarefa no campo Causa da página Detalhes do evento e determina que a tarefa falhou devido a um erro de cópia Snapshot. Em seguida, você acessa a página Detalhes do volume/integridade para obter mais informações.

Antes de começar

Você precisa ter a função de Application Administrator.

A mensagem de erro exibida no campo Causa da 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:

- Uma tarefa de backup ou espelhamento não foi concluída com êxito.

  A tarefa envolvia 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`.

- Um trabalho de cópia Snapshot falhou para `0426cluster2_src_vol2snap` no volume de origem `cluster2_src_svm:/cluster2_src_vol2`.

Nesse cenário, você pode identificar a causa e as possíveis ações corretivas da falha da tarefa. No entanto, para resolver a falha, você precisa acessar a interface 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 Snapshot falhou no volume de origem, indicando que provavelmente há um problema com o seu volume de origem.

   Opcionalmente, você poderia clicar no link **Job Details** no final da mensagem de erro, mas para os fins deste cenário, você opta por não fazer isso.

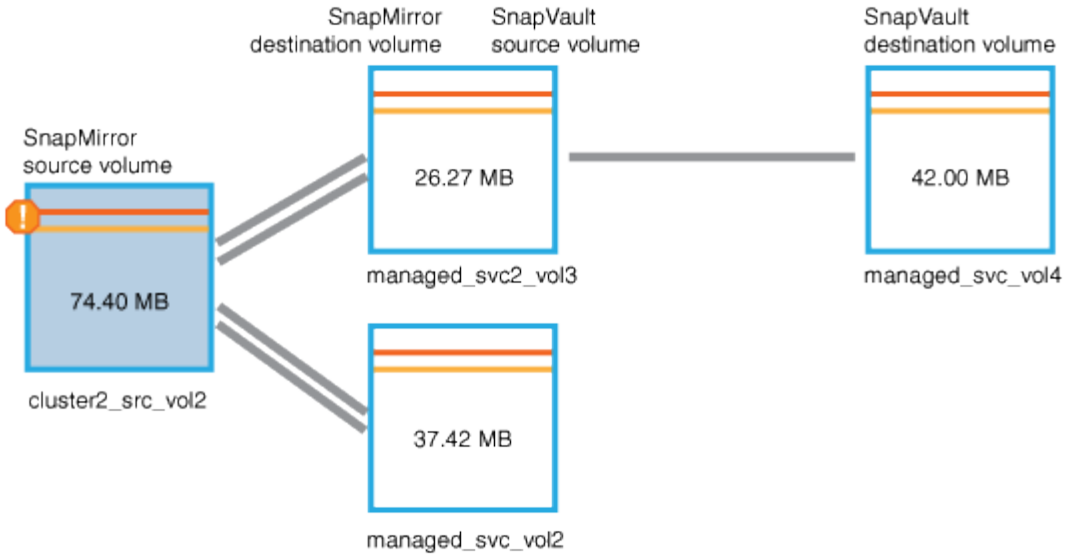
2. Você decide que quer tentar resolver o evento, então faz o seguinte:
   a. Clique no botão **Atribuir a** e selecione **Eu** do menu.
   b. Clique no botão **Acknowledge** para que você não continue recebendo notificações de alerta repetidas, caso alertas tenham sido configurados para o evento.
   c. Opcionalmente, você também pode adicionar notas sobre o evento.
3. Clique no campo **Origem** 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 Snapshot foi agendado.

   A página de detalhes Volume / Health é exibida para `cluster2_src_vol2`, mostrando o conteúdo da guia Protection.

4. Ao observar o gráfico da topologia de proteção, você verá um ícone de erro associado ao primeiro volume na topologia, que é o volume de origem para a relação do SnapMirror.

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



5. Ao posicionar o cursor sobre o ícone de erro, você vê a caixa de diálogo pop-up que exibe as configurações de limite e vê que o volume excedeu o limite de erro, o que indica um problema de capacidade.
6. Clique na guia **Capacidade**.

   Informações sobre a capacidade das exibições de volume `cluster2_src_vol2`.

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

   Você poderia optar por ativar o crescimento automático, mas para os fins deste cenário, você decide investigar mais a fundo antes de tomar uma decisão sobre como resolver o problema de capacidade.

9. Ao rolar a página para baixo até a lista de **Eventos**, você vê que os eventos Protection Job Failed, Volume Days Until Full e Volume Space Full foram gerados.
10. Na lista **Events**, clique no evento **Volume Space Full** para obter mais informações, após decidir que esse evento parece ser o mais relevante para o seu problema de capacidade.

    A página de detalhes do evento exibe o evento "Volume Space Full" 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 de Resumo, você verá as ações corretivas sugeridas.

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

    Você percorre a lista de ações sugeridas que pode executar para resolver o evento Volume Space Full:

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

- Ative e execute a compressão neste volume.

13. Você decide habilitar o crescimento automático no volume, mas, para isso, precisa determinar o espaço livre disponível no agregado pai e a taxa de crescimento atual do volume:
    a. Observe o agregado pai, `cluster2_src_aggr1`, no painel **Related Devices**.

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

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

    b. Na parte superior da página, observe o ícone que indica um incidente crítico e leia o texto abaixo do ícone.

       Você determina que "Dias para atingir a capacidade máxima: menos de um dia | Taxa de crescimento diário: 5,4%".

14. Acesse o System Manager ou a ONTAP CLI para habilitar a `volume autogrow` opção.

    Anote os nomes do volume e do agregado para tê-los disponíveis ao ativar o crescimento automático.

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

Resolva problemas de latência no Active IQ Unified Manager

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 ManagerDashboard para verificar se há algum problema com seus relacionamentos de proteção e, caso existam, encontrar soluções.

Antes de começar

Você precisa ter a função de Application Administrator ou Storage Administrator.

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

Passos

1. No painel **Proteção** da página **Painel de Controle**, localize o erro de atraso da relação do SnapMirror e clique nele.

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

2. Na página de detalhes de **Event**, você pode realizar uma ou mais das seguintes tarefas:
   - Analise 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 Source da área Summary para obter detalhes sobre o volume.

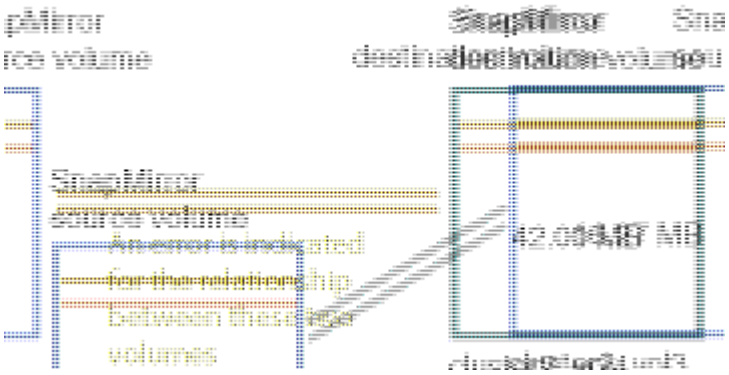
- Procure anotações que possam ter sido adicionadas sobre este evento.
- Adicione uma nota ao evento.
- Atribua o evento a um usuário específico.
- Reconheça ou resolva o evento.

3. Nesse cenário, você clica no nome do objeto (nesse caso, um volume) no campo Origem da área **Resumo** para obter detalhes sobre o volume.

   A página Detalhes de Volume/Saúde exibe a aba Proteção.

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

   Você observa que o volume com o erro de atraso é o último volume em uma cascata de SnapMirror de três volumes. O volume que você selecionou está contornado em cinza-escuro, e uma linha dupla laranja partindo do volume de origem indica um erro de relação do SnapMirror.



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

   Ao selecionar cada volume, as informações de proteção nas áreas Resumo, Topologia, Histórico, Eventos, Dispositivos Relacionados e Alertas Relacionados mudam para exibir detalhes relevantes para o volume selecionado.

6. Você visualiza a área **Resumo** e posiciona o cursor sobre o ícone de informações no campo **Atualização Programada** para cada volume.

   Nesse cenário, você observa que a política SnapMirror é DPDefault e que o agendamento SnapMirror é atualizado de hora em hora, cinco minutos após a hora. Você percebe que todos os volumes na relação estão tentando concluir uma transferência SnapMirror ao mesmo tempo.

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

Informações sobre direitos autorais

Copyright © 2026 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 DESTE DOCUMENTO. 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 SOBRESSALENTES; 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 DESTE SOFTWARE, 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.