Criação e resolução de problemas de relações de proteção

Active IQ Unified Manager 9.16

NetApp
November 19, 2024

Índice

Criação, monitoramento e solução de problemas de relacionamentos de proteção

Com o Unified Manager, você cria relacionamentos de proteção, monitora e soluciona problemas de proteção espelhada e de backup de dados armazenados em clusters gerenciados, além de restaurar os dados quando substituídos ou perdidos.

Tipos de proteção SnapMirror

Dependendo da implantação da topologia de storage de dados, o Unified Manager permite configurar vários tipos de relacionamentos de proteção SnapMirror. Todas as variações da proteção SnapMirror oferecem proteção contra recuperação de desastres com failover, mas oferecem recursos diferentes em performance, flexibilidade de versão e proteção de várias cópias de backup.

Relações de proteção assíncronas tradicionais da SnapMirror

A proteção assíncrona tradicional da SnapMirror fornece proteção espelhada de replicação de bloco entre volumes de origem e destino.

Nas relações SnapMirror tradicionais, as operações de espelhamento são executadas mais rápido do que em relacionamentos SnapMirror alternativos, porque a operação de espelhamento é baseada na replicação de bloco. No entanto, a proteção SnapMirror tradicional requer que o volume de destino seja executado na mesma ou posterior versão menor do software ONTAP como o volume de origem na mesma versão principal (por exemplo, versão 8.x a 8.x ou 9.x a 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 da versão

A proteção assíncrona do SnapMirror com replicação flexível da versão fornece proteção de espelhamento de replicação lógica entre volumes de origem e destino, mesmo que esses volumes estejam sendo executados em versões diferentes do ONTAP 8,3 ou software posterior (por exemplo, versão 8,3 a 8,3.1, ou 8,3 a 9,1 ou 9.2.2 a 9,2).

Nos relacionamentos do SnapMirror com replicação flexível por versão, as operações de espelhamento não são executadas tão rapidamente quanto nas relações SnapMirror tradicionais.

Devido à execução mais lenta, o SnapMirror com proteção de replicação flexível da versão não é adequado para ser implementado em qualquer uma das seguintes circunstâncias:

- O objeto fonte contém mais de 10 milhões de arquivos para proteger.
- 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 são mais de duas horas mais antigos do que os dados na origem.)

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

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

A proteção assíncrona do SnapMirror com a opção de replicação flexível e backup da versão oferece proteção espelhada entre os volumes de origem e destino e a funcionalidade de armazenar várias cópias dos dados espelhados no destino.

O administrador de storage pode especificar quais cópias Snapshot são espelhadas de origem para destino e também especificar por quanto tempo reter essas cópias no destino, mesmo que elas sejam excluídas na origem.

Nos relacionamentos do SnapMirror com a opção de replicação flexível de versão e backup, as operações de espelhamento não são executadas tão rapidamente como nas relações SnapMirror tradicionais.

Replicação unificada da SnapMirror (espelhamento e cofre)

A replicação unificada do SnapMirror permite configurar a recuperação de desastres e o arquivamento no mesmo volume de destino. Assim como no SnapMirror, a proteção de dados unificada realiza 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 Snapshot do volume de origem e, em seguida, transfere essa cópia e os blocos de dados que ela faz referência ao volume de destino. Assim como o SnapVault, a proteção de dados unificada não inclui cópias Snapshot mais antigas na linha de base.

Proteção síncrona SnapMirror com sincronização estrita

A proteção síncrona SnapMirror com sincronização "trict" 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 no volume primário será interrompida.

Proteção síncrona SnapMirror com sincronização regular

A proteção síncrona do SnapMirror com sincronização "veicular" não exige que o volume primário e secundário sejam sempre uma cópia verdadeira 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 ficam fora de sincronia e a e/S do cliente continuará para o volume primário.

O botão Restaurar e os botões de operação de relacionamento não estão disponíveis ao monitorar relações de proteção síncronas na exibição Saúde: Todos os volumes ou na página Detalhes volume / Saúde.

Sincronização ativa do SnapMirror

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

Ele permite descobrir e monitorar as relações síncronas de SnapMirror para grupos de consistência (CGS) disponíveis em clusters e máquinas virtuais de armazenamento do Unified Manager. O SnapMirror active Sync é compatível com clusters AFF ou todos os clusters SAN Array (ASA), onde os clusters primário e secundário podem ser AFF ou ASA. A sincronização ativa do SnapMirror protege aplicações com LUNs iSCSI ou FCP.

Quando você visualiza os volumes e LUNs protegidos pela relação de sincronização ativa do SnapMirror, obtém uma visão unificada para relacionamentos de proteção, grupos de consistência no inventário de

volumes, exibe a topologia de proteção para relacionamentos de grupo de consistência, exibe dados históricos para relacionamentos de grupo de consistência em até um ano. Você também pode baixar o relatório. Você também pode exibir o resumo das relações de Grupo de consistência, pesquisar o suporte para relacionamentos de 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, "Documentação do ONTAP 9 para sincronização ativa do SnapMirror (anteriormente SM-BC)"consulte .

Configuração de relacionamentos de proteção no Unified Manager

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

Antes de começar

- Tem de ter a função Administrador de aplicações ou Administrador de armazenamento.
- Você precisa ter relacionamentos de pares estabelecidos entre dois clusters ou duas máquinas virtuais de storage (SVMs).
- O OnCommand Workflow Automation precisa 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, execute um dos seguintes procedimentos:
   - "Crie uma relação de proteção SnapMirror".
   - "Crie uma relação de proteção SnapVault".
2. Se você quiser criar uma política para o relacionamento, dependendo do tipo de relacionamento que você está criando, siga um destes procedimentos:
   - "Crie uma política do SnapVault".
   - "Crie uma política do SnapMirror".
3. "Crie uma agenda SnapMirror ou SnapVault".

Configurando 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 "WFA pack for Management Clustered Data ONTAP" está incluído no WFA 5,1.1P6, portanto, não há necessidade de baixar este pacote da Loja de Automação NetAppStorage e instalá-lo separadamente em seu SERVIDOR WFA, como era necessário no passado. "Pacote WFA para gerenciar ONTAP"

- Você deve ter o nome do usuário do banco de dados que criou no Unified Manager para oferecer suporte às conexões DO WFA e do Unified Manager.

  Esse usuário do banco de dados deve ter sido atribuído a função de usuário do esquema de integração.

- Você deve ser atribuído a função Administrador ou a função 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.
- Tem de ter a função Administrador de aplicações ou Administrador de armazenamento.

Passos

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

   Você deve usar a porta de 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 (Automação do fluxo de trabalho) é exibida

6. Clique em **Yes** para recarregar a IU da Web e adicionar os recursos do Workflow Automation.

Informações relacionadas

"Documentação do NetApp: OnCommand Workflow Automation (versões atuais)"

Verificando o armazenamento em cache da fonte de dados do Unified Manager no Workflow Automation

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 é bem-sucedida no Workflow Automation. Você pode fazer isso quando integrar o Workflow Automation ao Unified Manager para garantir que a funcionalidade do Workflow Automation esteja disponível após a integração.

Antes de começar

Para executar esta tarefa, é necessário atribuir a função Administrador ou a função arquiteto no Workflow Automation.

Passos

1. Na IU 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 **adquirir agora**.
3. Verifique se a aquisição é bem-sucedida sem erros.

   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, primeiro você deve remover a conexão entre o OnCommand Workflow Automation e o Unified Manager e garantir que todos os OnCommand Workflow Automation em execução ou tarefas agendadas estejam interrompidas.

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.

Remoção da configuração do OnCommand Workflow Automation do Gerenciador Unificado

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

Antes de começar

Tem de ter a função Administrador de aplicações ou Administrador de armazenamento.

Passos

1. No painel de navegação à esquerda, clique em **Geral** > **Workflow Automation** no menu Configuração à esquerda.
2. Na página **Workflow Automation**, clique em **Remove Setup** (Remover configuração).

Execução de failover e failback de uma relação de proteção

Quando um volume de origem em sua relação de proteção é desativado devido a uma falha de hardware ou a um desastre, você pode usar os recursos de relação de proteção no Unified Manager para tornar o destino de proteção leitura/gravação acessível e fazer failover para esse volume até que a origem esteja on-line novamente. Em seguida, você pode retornar à fonte original quando ela estiver disponível para fornecer dados.

Antes de começar

- Tem de ter a função Administrador de aplicações ou Administrador de armazenamento.
- Tem de ter configurado o OnCommand Workflow Automation para executar esta operação.

Passos

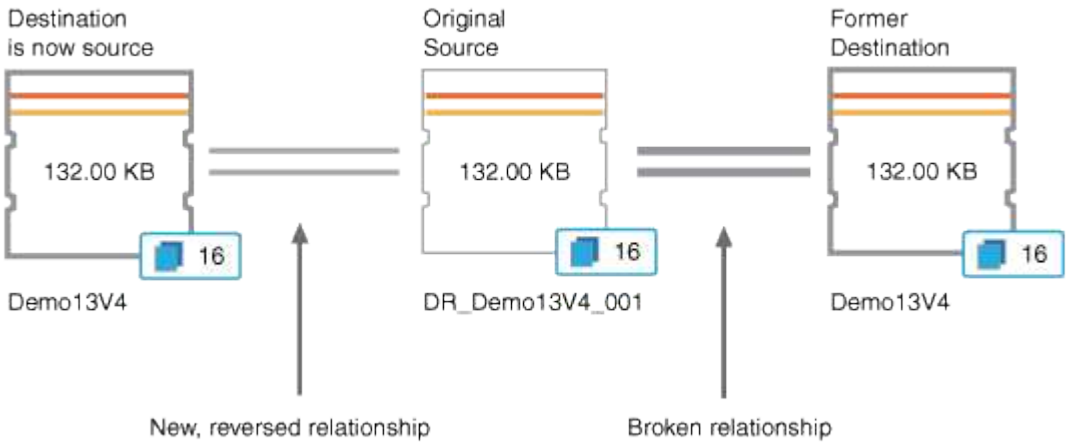
1. "Quebre a relação SnapMirror".

   É necessário interromper o relacionamento antes de converter o destino de um volume de proteção de dados em um volume de leitura/gravação e antes de reverter o relacionamento.

2. "Inverta a relação de proteção".

   Quando o volume de origem original estiver novamente disponível, você poderá decidir restabelecer a relação de proteção original restaurando o volume de origem. Antes de restaurar a origem, é necessário sincronizá-la com os dados gravados no destino anterior. Use 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 destino anterior. Uma nova cópia Snapshot da linha de base é criada para o novo relacionamento.

   A relação invertida é semelhante a uma relação em cascata:



3. "Quebre a relação revertida do SnapMirror".

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

4. "Remova a relação".

   Quando o relacionamento invertido não for mais necessário, você deve remover esse relacionamento antes de restabelecer o relacionamento original.

5. "Ressincronizar o relacionamento".

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

Quebrar uma relação de SnapMirror a partir da página de detalhes de volume / Saúde

Você pode quebrar uma relação de proteção da página de detalhes de volume / Saúde e interromper as transferências de dados entre um volume de origem e destino em uma relação do SnapMirror. Você pode interromper um relacionamento quando quiser migrar dados, para recuperação de desastres ou para teste de aplicações. O volume de destino

é alterado para um volume de leitura e gravação. Você não pode quebrar um relacionamento SnapVault.

Antes de começar

- Tem de ter a função Administrador de aplicações ou Administrador de armazenamento.
- Você deve ter configurado o Workflow Automation.

Passos

1. Na guia **proteção** da página de detalhes **volume / Saúde**, selecione na topologia a relação do SnapMirror que deseja quebrar.
2. Clique com o botão direito do rato no destino e selecione **Break** no menu.

   É apresentada a caixa de diálogo Break Relationship (interromper relação).

3. Clique em **continuar** para quebrar o relacionamento.
4. Na topologia, verifique se o relacionamento está quebrado.

Reverter relações de proteção a partir da página de detalhes de volume / Saúde

Quando um desastre desativa o volume de origem em sua relação de proteção, você pode usar o volume de destino para servir dados convertendo-os para leitura/gravação enquanto você reparar ou substituir a origem. Quando a origem estiver novamente disponível para receber dados, você poderá 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

- Tem de ter a função Administrador de aplicações ou Administrador de armazenamento.
- Você deve ter configurado o Workflow Automation.
- 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 como o destino devem estar online.
- A origem não deve ser o destino de outro volume de proteção de dados.
- Quando você executa essa tarefa, os dados na fonte mais recente do que os dados na cópia Snapshot comum são excluídos.
- As políticas e os horários criados na relação de ressincronização reversa são os mesmos que os da relação de proteção original.

  Se as políticas e agendas não existirem, elas são criadas.

Passos

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

A caixa de diálogo Reverse Resync (Reverse Resync) é exibida.

3. Verifique se a relação exibida na caixa de diálogo **Reverse Resync** é aquela para a qual você deseja executar a operação de ressincronização reversa e clique em **Submit**.

   A caixa de diálogo Reverse Resync (Reverse Resync) é fechada e um link de tarefa é exibido na parte superior da página volume / Health details (Detalhes de volume / Saúde).

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

   É apresentada uma lista filtrada de trabalhos.

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 de trabalho são concluídas com êxito.

Remover uma relação de proteção da página de detalhes de volume / Saúde

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

Antes de começar

- Tem de ter a função Administrador de aplicações ou Administrador de armazenamento.
- Você deve ter configurado o Workflow Automation.

Passos

1. Na guia **proteção** da página de detalhes **volume / Saúde**, selecione na topologia a relação SnapMirror que deseja remover.
2. Clique com o botão direito do rato 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.

   A relação é removida da página de detalhes de volume / Saúde.

Ressincronizar relações de proteção a partir da página de detalhes de volume / Saúde

É possível ressincronizar dados em um relacionamento SnapMirror ou SnapVault que foi quebrado e, em seguida, o destino foi feito 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 for excluída, causando falha nas atualizações do SnapMirror ou do SnapVault.

Antes de começar

- Tem de ter a função Administrador de aplicações ou Administrador de armazenamento.
- Tem de ter configurado o OnCommand Workflow Automation.

Passos

1. Na guia **proteção** da página de detalhes **volume / Saúde**, localize na topologia a relação de proteção que você deseja ressincronizar e clique com o botão direito do Mouse nela.
2. Selecione **Resynchronize** no menu.

   Alternativamente, no menu **ações**, selecione **relacionamento** > **Resyncronizar** para ressincronizar a relação para a qual você está visualizando os detalhes no momento.

   A caixa de diálogo Resyncronizar é exibida.

3. Na guia **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 **predefinição**.

   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 será retornado à caixa de diálogo Resyncronizar.

7. Se você selecionou mais de uma fonte para ressincronizar, clique em **Default** para a próxima fonte para a qual deseja especificar uma cópia Snapshot existente.
8. Clique em **Enviar** para iniciar o trabalho de ressincronização.

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

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

   É apresentada uma lista filtrada de trabalhos.

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 de trabalho forem concluídas com êxito.

Resolução de uma falha de trabalho de proteção

Esse 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 nesse fluxo de trabalho exigem que você faça login usando a função Administrador, você deve estar familiarizado com as funções necessárias para usar várias funcionalidades.

Nesse cenário, você acessa a página Painel para ver se há algum problema com seus trabalhos de proteção. Na área Incidente de proteção, você percebe que há um incidente de trabalho terminado, mostrando um erro Falha no trabalho de proteção em um volume. Investigue este 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 no trabalho de proteção**.

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

   A página de detalhes do evento para o trabalho de proteção com falha é exibida.

2. Reveja a mensagem de erro no campo causa da área **Summary** para determinar o problema e avaliar potenciais ações corretivas.

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

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

Você analisa a mensagem de erro de falha do trabalho no campo causa na página de detalhes do evento e determina que o trabalho falhou devido a um erro de cópia Snapshot. Em seguida, avance para a página de detalhes de volume / Saúde para obter mais informações.

Antes de começar

Tem de ter a função Administrador de aplicações.

A mensagem de erro fornecida no campo causa na página de detalhes do evento contém o seguinte texto sobre o trabalho 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 cópia de segurança ou espelho não foi concluído com êxito.

  A tarefa 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`.

- Um trabalho de cópia Snapshot falhou para o `0426cluster2_src_vol2snap` volume de origem `cluster2_src_svm:/cluster2_src_vol2 .`

Nesse cenário, você pode identificar a causa e as possíveis ações corretivas da falha do trabalho. No entanto, a resolução da falha requer que você acesse a IU da Web do Gerenciador do sistema 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 volume de origem.

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

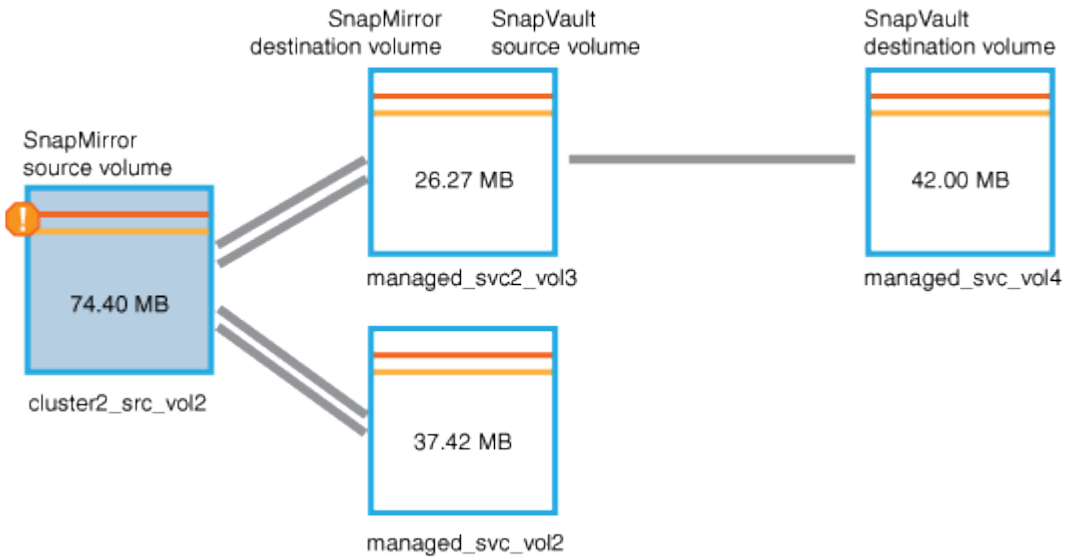
2. Você decide que deseja tentar resolver o evento, para fazer o seguinte:
   a. Clique no botão **Assign to** e selecione **me** no menu.
   b. Clique no botão **confirmar** para que você não continue a receber notificações de alerta repetidas, se os alertas tiverem sido definidos para o evento.
   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 **Source** contém o nome do objeto de origem: Neste caso, o volume no qual o trabalho de cópia Snapshot foi agendado.

   A página de detalhes de volume / Saúde é exibida para `cluster2_src_vol2`, mostrando o conteúdo da guia proteção.

4. Olhando para o gráfico de topologia de proteção, você vê um ícone de erro associado ao primeiro volume na topologia, que é o volume de origem da relação SnapMirror.

   Você também vê as barras horizontais no ícone de 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 ver que o volume excedeu o limite de erro, indicando um problema de capacidade.

6. Clique na guia **capacidade**.

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

7. No painel **Capacity**, você vê que há 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 crescimento automático de volume foi desativado e que uma garantia de espaço de volume foi definida.

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

9. Role para baixo até a lista **Eventos** e veja que os eventos Falha no trabalho de proteção, dias de volume até cheio e espaço de volume cheio foram gerados.
10. Na lista **Eventos**, você clica no evento **espaço em volume completo** para obter mais informações, tendo decidido que esse evento parece mais relevante para o seu problema de capacidade.

    A página Detalhes do evento exibe o evento espaço de volume completo 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 verá ações corretivas sugeridas.

    As ações corretivas sugeridas são exibidas apenas para alguns eventos, para que você não veja essa área para todos os tipos de eventos.

    Você clica na lista de ações sugeridas que você pode executar para resolver o evento espaço de volume cheio:

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

13. Você decide ativar 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 **Related Devices** (dispositivos relacionados).

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

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

    b. Na parte superior da página, olhe para o ícone que indica um incidente crítico e reveja o texto abaixo do ícone.

       Você determina que "dias completos: Menos de um dia | taxa de crescimento diária: 5,4%".

14. Vá para o Gerenciador do sistema ou acesse a CLI do ONTAP para ativar a `volume autogrow` opção.

Anote os nomes do volume e do agregado para que você os tenha disponíveis ao ativar o crescimento automático.

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

Resolvendo problemas de atraso

Este fluxo de trabalho fornece um exemplo de como você pode resolver um problema de atraso. Nesse cenário, você é um administrador ou operador acessando a página do Unified ManagerDashboard para ver se há algum problema com seus relacionamentos de proteção e, se existirem, para encontrar soluções.

Antes de começar

Tem de ter a função Administrador de aplicações ou Administrador de armazenamento.

Na página Painel, você analisa 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 de relacionamento do SnapMirror e clique nele.

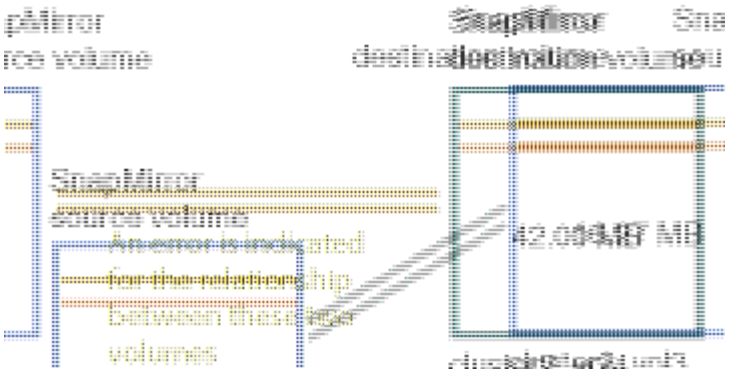
   A página de detalhes do evento para o evento de erro de atraso é exibida.

2. Na página de detalhes 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.
   - Confirmar ou resolver o evento.
3. Nesse cenário, você clica no nome do objeto (neste caso, um volume) no campo fonte da área **Resumo** para obter detalhes sobre o volume.

   É apresentado o separador proteção da página volume / Health details (Detalhes do volume / Saúde).

4. Na guia **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 delineado em cinza escuro e uma linha laranja dupla do volume de origem indica um erro de relacionamento SnapMirror.



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

   À medida que seleciona 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 olha para a área **Summary** e posiciona o cursor sobre o ícone de informações no campo **Update Schedule** para cada volume.

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

7. Para resolver o problema de atraso, você modifica as programações de dois volumes em cascata para que cada destino inicie uma transferência de SnapMirror depois que sua origem concluir uma transferência.

Informações sobre direitos autorais

Informações sobre marcas comerciais