



Gerenciar storage com o software Element Element Software

NetApp
November 19, 2025

Índice

| | |
|--|-----|
| Gerenciar storage com o software Element | 1 |
| Encontre mais informações | 1 |
| Acesse a interface do usuário do software Element | 1 |
| Encontre mais informações | 2 |
| Configure as opções do sistema SolidFire após a implantação | 2 |
| Encontre mais informações | 2 |
| Alterar credenciais no NetApp HCI e no NetApp SolidFire | 2 |
| Altere o certificado SSL padrão do software Element | 6 |
| Altere a senha padrão do IPMI para nós | 7 |
| Use opções básicas na IU do software Element | 8 |
| Para mais informações | 9 |
| Ver atividade da API | 9 |
| Ícones na interface do elemento | 10 |
| Fornecer feedback | 11 |
| Gerenciar contas | 11 |
| Para mais informações | 11 |
| Trabalhar com contas usando CHAP | 11 |
| Gerenciar contas de usuários de administrador de cluster | 14 |
| Gerencie seu sistema | 25 |
| Para mais informações | 25 |
| Ativar a autenticação multifator | 26 |
| Configure as definições do cluster | 27 |
| Criar um cluster compatível com unidades FIPS | 43 |
| Ative o FIPS 140-2 para HTTPS no cluster | 46 |
| Comece a usar o gerenciamento de chaves externas | 48 |
| Gerenciar volumes e volumes virtuais | 53 |
| Para mais informações | 53 |
| Trabalhe com volumes | 54 |
| Trabalhe com volumes virtuais | 63 |
| Trabalhar com grupos de acesso de volume e iniciadores | 72 |
| Proteja seus dados | 80 |
| Para mais informações | 80 |
| Use snapshots de volume para proteção de dados | 81 |
| Executar replicação remota entre clusters que executam o software NetApp Element | 94 |
| Use a replicação do SnapMirror entre clusters Element e ONTAP | 108 |
| Faça backup e restaure volumes | 120 |
| Solucionar problemas do sistema | 124 |
| Para mais informações | 125 |
| Ver informações sobre eventos do sistema | 125 |
| Exibir o status das tarefas em execução | 129 |
| Ver alertas do sistema | 129 |
| Visualizar a atividade de performance do nó | 146 |
| Ver o desempenho do volume | 146 |

| | |
|---|-----|
| Ver sessões iSCSI | 148 |
| Ver sessões Fibre Channel | 149 |
| Solucionar problemas de unidades | 150 |
| Solucionar problemas de nós | 154 |
| Trabalhar com utilitários por nó para nós de storage..... | 155 |
| Entenda os níveis de plenitude do cluster | 163 |

Gerenciar storage com o software Element

Use o software Element para configurar o storage SolidFire, monitorar a capacidade e a performance do cluster e gerenciar as atividades de storage em uma infraestrutura de alocação a vários clientes.

Element é o sistema operacional de storage no centro de um cluster SolidFire. O software Element é executado independentemente em todos os nós do cluster e permite que os nós do cluster combinem recursos e apresentem como um único sistema de storage para clientes externos. O software Element é responsável por toda a coordenação, escala e gerenciamento de cluster do sistema como um todo.

A interface do software é construída sobre a API Element.

- ["Acesse a interface do usuário do software Element"](#)
- ["Configure as opções do sistema SolidFire após a implantação"](#)
- ["Atualize os componentes do sistema de storage"](#)
- ["Use opções básicas na IU do software Element"](#)
- ["Gerenciar contas"](#)
- ["Gerencie seu sistema"](#)
- ["Gerenciar volumes e volumes virtuais"](#)
- ["Proteja seus dados"](#)
- ["Solucionar problemas do sistema"](#)

Encontre mais informações

- ["Documentação do software SolidFire e Element"](#)
- ["Plug-in do NetApp Element para vCenter Server"](#)

Acesse a interface do usuário do software Element

Você pode acessar a IU do Element usando o endereço MVIP (IP virtual de gerenciamento) do nó do cluster principal.

Você deve garantir que os bloqueadores de pop-up e as configurações do NoScript estejam desabilitadas no seu navegador.

Você pode acessar a IU usando endereçamento IPv4 ou IPv6, dependendo da configuração durante a criação do cluster.

1. Escolha uma das seguintes opções:

- IPv6: Introduza o endereço MVIP do `https://[IPv6]` por exemplo:

```
https://[fd20:8b1e:b256:45a::1234]/
```

- IPv4: Introduza o endereço MVIP do `https://[IPv4]` por exemplo:

```
https://10.123.456.789/
```

2. Para DNS, introduza o nome do anfitrião.
3. Clique em qualquer mensagem de certificado de autenticação.

Encontre mais informações

- ["Documentação do software SolidFire e Element"](#)
- ["Plug-in do NetApp Element para vCenter Server"](#)

Configure as opções do sistema SolidFire após a implantação

Depois de configurar o sistema SolidFire, talvez você queira executar algumas tarefas opcionais.

Se você alterar credenciais no sistema, talvez queira saber o impactos em outros componentes.

Além disso, você pode configurar configurações para autenticação multifator, gerenciamento de chaves externas e segurança FIPS (Federal Information Processing Standards). Você também deve olhar para a atualização de senhas quando necessário.

Encontre mais informações

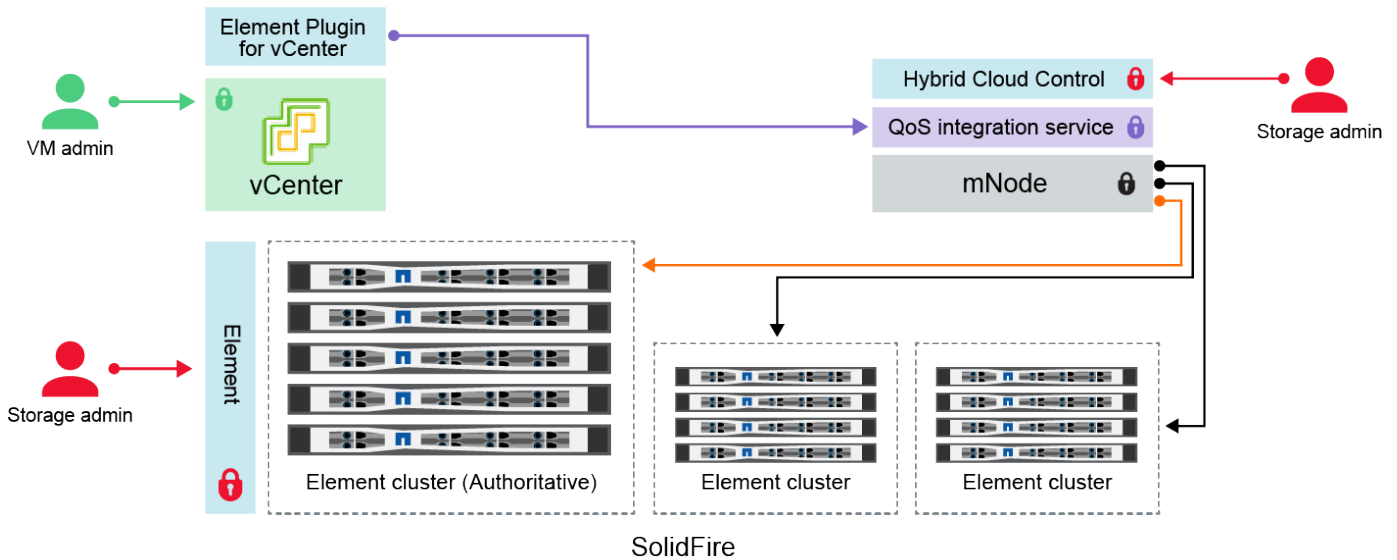
- ["Alterar credenciais no NetApp HCI e no NetApp SolidFire"](#)
- ["Altere o certificado SSL padrão do software Element"](#)
- ["Altere a senha do IPMI para nós"](#)
- ["Ativar a autenticação multifator"](#)
- ["Comece a usar o gerenciamento de chaves externas"](#)
- ["Criar um cluster compatível com unidades FIPS"](#)

Alterar credenciais no NetApp HCI e no NetApp SolidFire


Dependendo das políticas de segurança na organização que implantou o NetApp HCI ou o NetApp SolidFire, alterar credenciais ou senhas geralmente faz parte das práticas de segurança. Antes de alterar as senhas, você deve estar ciente do impactos em outros componentes de software na implantação.



Se você alterar credenciais para um componente de uma implantação do NetApp HCI ou do NetApp SolidFire, a tabela a seguir fornece orientações sobre o impactos em outros componentes.



Interações do componente NetApp SolidFire:





- Administrator uses administrative Element storage credentials to log into Element UI and Hybrid Cloud Control
- Element Plugin for VMware vCenter uses password to communicate with QoS service on mNode
- mNode and services use Element certificates to communicate with authoritative storage cluster
- mNode and services use Element administrative credentials for additional storage clusters
- Administrators use VMware vSphere Single Sign-on credentials to log into vCenter

| Tipo e ícone de credencial | Utilização por Admin | Consulte estas instruções |
|--|---|--|
| Credenciais do elemento  | <p>Aplicável a: NetApp HCI e SolidFire</p> <p>Administradores usam essas credenciais para fazer login:</p> <ul style="list-style-type: none"> • Interface de usuário do Element no cluster de storage do Element • Controle de nuvem híbrida no nó de gerenciamento (mnode) <p>Quando o Hybrid Cloud Control gerencia vários clusters de armazenamento, ele aceita apenas as credenciais de administrador para os clusters de armazenamento, conhecido como o cluster <i>autoritativo</i> para o qual o mnode foi configurado inicialmente. Para clusters de storage adicionados mais tarde ao Hybrid Cloud Control, o mnode armazena com segurança as credenciais de administrador. Se as credenciais para clusters de armazenamento adicionados posteriormente forem alteradas, as credenciais também devem ser atualizadas no mnode usando a API mnode.</p> | <ul style="list-style-type: none"> • "Atualize as senhas de administrador do cluster de armazenamento." • Atualize as credenciais de administrador do cluster de armazenamento no mnode usando o "API de modificação exclusiva". |

| Tipo e ícone de credencial | Utilização por Admin | Consulte estas instruções |
|--|---|---|
| <p>Credenciais de logon único do vSphere</p>  | <p>Aplicável a: Apenas NetApp HCI</p> <p>Os administradores usam essas credenciais para fazer login no VMware vSphere Client. Quando o vCenter faz parte da instalação do NetApp HCI, as credenciais são configuradas no mecanismo de implantação do NetApp da seguinte forma:</p> <ul style="list-style-type: none"> • com a senha especificada, e. • com a senha especificada. Quando um vCenter existente é usado para implantar o NetApp HCI, as credenciais de logon único do vSphere são gerenciadas pelos administradores da VMware DE TI. | <p>"Atualize as credenciais do vCenter e do ESXi".</p> |
| <p>Credenciais do controlador de gerenciamento de placa base (BMC)</p>  | <p>Aplicável a: Apenas NetApp HCI</p> <p>Os administradores usam essas credenciais para fazer login no BMC dos nós de computação do NetApp em uma implantação do NetApp HCI. O BMC fornece monitoramento básico de hardware e recursos de console virtual.</p> <p>As credenciais BMC (às vezes chamadas de <i>IPMI</i>) para cada nó de computação NetApp são armazenadas com segurança no nó mnode nas implantações do NetApp HCI. O controle de nuvem híbrida da NetApp usa credenciais BMC na capacidade de uma conta de serviço para se comunicar com o BMC nos nós de computação durante atualizações de firmware de nós de computação.</p> <p>Quando as credenciais do BMC são alteradas, as credenciais dos respectivos nós de computação devem ser atualizadas também no nó mnode para reter toda a funcionalidade de Controle de nuvem híbrida.</p> | <ul style="list-style-type: none"> • "Configure o IPMI para cada nó no NetApp HCI". • Para nós de H410C, H610C e H615C, "Altere a senha padrão do IPMI". • Para nós de H410S e H610S, "Altere a senha padrão do IPMI". • "Altere as credenciais do BMC no nó de gerenciamento". |

| Tipo e ícone de credencial | Utilização por Admin | Consulte estas instruções |
|--|---|--|
| <p>Credenciais ESXi</p>  | <p>Aplicável a: Apenas NetApp HCI</p> <p>Os administradores podem fazer login em hosts ESXi usando SSH ou DCUI local com uma conta raiz local. Nas implantações do NetApp HCI, o nome de usuário é 'root' e a senha foi especificada durante a instalação inicial desse nó de computação no mecanismo de implantação do NetApp.</p> <p>As credenciais raiz do ESXi para cada nó de computação do NetApp são armazenadas com segurança no nó mnode nas implantações do NetApp HCI. O Controle de nuvem híbrida da NetApp usa as credenciais em uma capacidade de conta de serviço para se comunicar diretamente com os hosts ESXi durante as atualizações de firmware do nó de computação e verificações de integridade.</p> <p>Quando as credenciais raiz ESXi são alteradas por um administrador da VMware, as credenciais dos respectivos nós de computação devem ser atualizadas no nó mnode para manter a funcionalidade de Controle de nuvem híbrida.</p> | <p>"Atualizar credenciais para hosts do vCenter e do ESXi".</p> |
| <p>Palavra-passe de integração o QoS</p>  | <p>Aplicável a: NetApp HCI e opcional no SolidFire</p> <p>Não é usado para logins interativos por administradores.</p> <p>A integração de QoS entre o VMware vSphere e o Element Software é habilitada por:</p> <ul style="list-style-type: none"> • Plug-in Element para vCenter Server, e. • Serviço de QoS no mnode. <p>Para autenticação, o serviço QoS usa uma senha que é exclusivamente usada neste contexto. A senha de QoS é especificada durante a instalação inicial do plug-in Element para vCenter Server ou gerada automaticamente durante a implantação do NetApp HCI.</p> <p>Sem impactos em outros componentes.</p> | <p>"Atualize as credenciais do QoSSIOC no plug-in do NetApp Element para o vCenter Server".</p> <p>A senha do plug-in do NetApp Element para o vCenter Server SIOC também é conhecida como <i>QoSSIOC password</i>.</p> <p>Consulte o artigo de base de dados do vCenter Server.</p> |

| Tipo e ícone de credencial | Utilização por Admin | Consulte estas instruções |
|--|---|---------------------------------|
| Credenciais do vCenter Service Appliance  | <p>Aplica-se a: NetApp HCI somente se configurado pelo mecanismo de implantação do NetApp</p> <p>Os administradores podem fazer login nas máquinas virtuais do vCenter Server Appliance. Nas implantações do NetApp HCI, o nome de usuário é 'root' e a senha foi especificada durante a instalação inicial desse nó de computação no mecanismo de implantação do NetApp. Dependendo da versão do VMware vSphere implantada, certos administradores no domínio de logon único do vSphere também podem fazer login no dispositivo.</p> <p>Sem impactos em outros componentes.</p> | Não são necessárias alterações. |
| Credenciais de administrador do nó de gerenciamento do NetApp  | <p>Aplicável a: NetApp HCI e opcional no SolidFire</p> <p>Os administradores podem fazer login nas máquinas virtuais do nó de gerenciamento do NetApp para configuração avançada e solução de problemas. Dependendo da versão do nó de gerenciamento implantada, o login via SSH não é habilitado por padrão.</p> <p>Nas implantações do NetApp HCI, o nome de usuário e a senha foram especificados pelo usuário durante a instalação inicial desse nó de computação no mecanismo de implantação do NetApp.</p> <p>Sem impactos em outros componentes.</p> | Não são necessárias alterações. |

Encontre mais informações

- ["Altere o certificado SSL padrão do software Element"](#)
- ["Altere a senha do IPMI para nós"](#)
- ["Ativar a autenticação multifator"](#)
- ["Comece a usar o gerenciamento de chaves externas"](#)
- ["Criar um cluster compatível com unidades FIPS"](#)

Altere o certificado SSL padrão do software Element

Você pode alterar o certificado SSL padrão e a chave privada do nó de armazenamento no cluster usando a API NetApp Element.

Quando um cluster de software NetApp Element é criado, o cluster cria um certificado SSL (Secure Sockets Layer) exclusivo autoassinado e uma chave privada que é usada para todas as comunicações HTTPS por meio da IU do Element, IU por nó ou APIs. O software Element suporta certificados autoassinados, bem como certificados emitidos e verificados por uma autoridade de certificação (CA) confiável.

Você pode usar os seguintes métodos de API para obter mais informações sobre o certificado SSL padrão e fazer alterações.

- **GetSSLCertificate**

Você pode usar o "[Método GetSSLCertificate](#)" para recuperar informações sobre o certificado SSL instalado atualmente, incluindo todos os detalhes do certificado.

- **SetSSLCertificate**

Você pode usar o "[Método SetSSLCertificate](#)" para definir os certificados SSL de cluster e por nó para o certificado e a chave privada que você fornece. O sistema valida o certificado e a chave privada para impedir que um certificado inválido seja aplicado.

- **RemoveSSLCertificate**

O "[Método RemoveSSLCertificate](#)" remove o certificado SSL e a chave privada atualmente instalados. Em seguida, o cluster gera um novo certificado autoassinado e uma chave privada.



O certificado SSL do cluster é aplicado automaticamente a todos os novos nós adicionados ao cluster. Qualquer nó removido do cluster reverte para um certificado autoassinado e todas as informações de chave e certificados definidos pelo usuário são removidas do nó.

Encontre mais informações

- "[Altere o certificado SSL padrão do nó de gerenciamento](#)"
- "[Quais são os requisitos para definir certificados SSL personalizados no Element Software?](#)"
- "[Documentação do software SolidFire e Element](#)"
- "[Plug-in do NetApp Element para vCenter Server](#)"

Altere a senha padrão do IPMI para nós

Você pode alterar a senha de administrador IPMI (Intelligent Platform Management Interface) padrão assim que tiver acesso IPMI remoto ao nó. Você pode querer fazer isso se houver atualizações de instalação.

Para obter detalhes sobre como configurar o acesso IPM para nós, "[Configure o IPMI para cada nó](#)" consulte .

Você pode alterar a senha do IPM para esses nós:

- H410S nós
- H610S nós

Altere a senha padrão do IPMI para H410S nós

Você deve alterar a senha padrão para a conta de administrador IPMI em cada nó de armazenamento assim que configurar a porta de rede IPMI.

O que você vai precisar

Você deve ter configurado o endereço IP IPMI para cada nó de armazenamento.

Passos

1. Abra um navegador da Web em um computador que possa acessar a rede IPMI e navegue até o endereço IP IPMI do nó.
2. Introduza o nome de utilizador `ADMIN` e a palavra-passe `ADMIN` no aviso de início de sessão.
3. Ao iniciar sessão, clique no separador **Configuration** (Configuração).
4. Clique em **usuários**.
5. Selecione o `ADMIN` usuário e clique em **Modificar usuário**.
6. Marque a caixa de seleção **alterar senha**.
7. Introduza uma nova palavra-passe nos campos **Password** (Palavra-passe) e **Confirm Password** (confirmar palavra-passe).
8. Clique em **Modificar** e, em seguida, clique em **OK**.
9. Repita este procedimento para quaisquer outros nós H410S com senhas IPMI padrão.

Altere a senha padrão do IPMI para H610S nós

Você deve alterar a senha padrão para a conta de administrador IPMI em cada nó de armazenamento assim que configurar a porta de rede IPMI.

O que você vai precisar

Você deve ter configurado o endereço IP IPMI para cada nó de armazenamento.

Passos

1. Abra um navegador da Web em um computador que possa acessar a rede IPMI e navegue até o endereço IP IPMI do nó.
2. Introduza o nome de utilizador `root` e a palavra-passe `calvin` no aviso de início de sessão.
3. Ao iniciar sessão, clique no ícone de navegação do menu no canto superior esquerdo da página para abrir a gaveta da barra lateral.
4. Clique em **Configurações**.
5. Clique em **User Management**.
6. Selecione o usuário **Administrator** na lista.
7. Ative a caixa de verificação **alterar palavra-passe**.
8. Insira uma nova senha forte nos campos **Senha** e **confirmar senha**.
9. Clique em **Salvar** na parte inferior da página.
10. Repita este procedimento para quaisquer outros nós H610S com senhas IPMI padrão.

Encontre mais informações

- ["Documentação do software SolidFire e Element"](#)
- ["Plug-in do NetApp Element para vCenter Server"](#)

Use opções básicas na IU do software Element

A interface do usuário da Web do software NetApp Element (Element UI) permite monitorar e executar tarefas comuns no sistema SolidFire.

As opções básicas incluem a visualização de comandos API ativados pela atividade da IU e o fornecimento de feedback.

- ["Ver atividade da API"](#)
- ["Ícones na interface do elemento"](#)
- ["Fornecer feedback"](#)

Para mais informações

- ["Documentação do software SolidFire e Element"](#)
- ["Plug-in do NetApp Element para vCenter Server"](#)

Ver atividade da API

O sistema Element usa a API NetApp Element como base para seus recursos e funcionalidades. A IU do Element permite visualizar vários tipos de atividade da API em tempo real no sistema conforme você usa a interface. Com o log da API, você pode visualizar a atividade da API do sistema iniciada pelo usuário e em segundo plano, bem como chamadas de API feitas na página que você está visualizando no momento.

Você pode usar o log da API para identificar quais métodos de API são usados para certas tarefas e ver como usar os métodos e objetos da API para criar aplicativos personalizados.

Para obter informações sobre cada método, ["Referência da API do Element Software"](#) consulte .

1. Na barra de navegação da IU do Element, clique em **API Log**.
2. Para modificar o tipo de atividade da API exibida na janela Registro da API, execute as seguintes etapas:
 - a. Selecione **Requests** para exibir o tráfego de solicitação de API.
 - b. Selecione **respostas** para exibir o tráfego de resposta da API.
 - c. Filtre os tipos de tráfego de API selecionando um dos seguintes:
 - **Usuário iniciado:** Tráfego de API por suas atividades durante esta sessão de IU da Web.
 - *** Inquérito de fundo*:** Tráfego de API gerado pela atividade do sistema em segundo plano.
 - **Página atual:** Tráfego de API gerado por tarefas na página que você está visualizando atualmente.

Encontre mais informações

- ["Gerenciamento de storage com a API Element"](#)
- ["Documentação do software SolidFire e Element"](#)
- ["Plug-in do NetApp Element para vCenter Server"](#)

Taxa de atualização da interface afetada pela carga do cluster

Dependendo dos tempos de resposta da API, o cluster pode ajustar automaticamente o intervalo de atualização de dados para determinadas partes da página do software NetApp Element que você está visualizando.










O intervalo de atualização é redefinido para o padrão quando você recarrega a página no navegador. Você pode ver o intervalo de atualização atual clicando no nome do cluster no canto superior direito da página. Observe que o intervalo controla a frequência com que solicitações de API são feitas, não com que rapidez os dados retornam do servidor.

Quando um cluster está sob carga pesada, ele pode enfileirar solicitações de API da IU do Element. Em raras circunstâncias, quando a resposta do sistema é significativamente atrasada, como uma conexão de rede lenta combinada com um cluster ocupado, você pode ser desconectado da IU do Element se o sistema não responder a solicitações de API em fila com rapidez suficiente. Se você for redirecionado para a tela de logout, você poderá fazer login novamente depois de rejeitar qualquer prompt de autenticação inicial do navegador. Ao retornar à página de visão geral, talvez você seja solicitado a fornecer credenciais de cluster se elas não forem salvas pelo navegador.

Ícones na interface do elemento

A interface do software NetApp Element exibe ícones para representar as ações que você pode executar nos recursos do sistema.

A tabela a seguir fornece uma referência rápida:

| Ícone | Descrição |
|---|--------------------|
|  | Ações |
|  | Backup para |
|  | Clone ou cópia |
|  | Eliminar ou purgar |
|  | Editar |
|  | Filtro |
|  | Emparelhar |
|  | Atualizar |
|  | Restaurar |

| | |
|---|--------------|
|  | Restaurar de |
|  | Reverter |
|  | Snapshot |

Fornecer feedback

Você pode ajudar a melhorar a interface do usuário da Web do software Element e resolver quaisquer problemas de interface do usuário usando o formulário de feedback que é acessível em toda a interface do usuário.

1. Em qualquer página da IU do elemento, clique no botão **Feedback**.
2. Introduza informações relevantes nos campos Summary (Resumo) e Description (Descrição).
3. Anexe quaisquer capturas de tela úteis.
4. Introduza um nome e um endereço de correio eletrônico.
5. Marque a caixa de seleção para incluir dados sobre seu ambiente atual.
6. Clique em **Enviar**.

Encontre mais informações

- ["Documentação do software SolidFire e Element"](#)
- ["Plug-in do NetApp Element para vCenter Server"](#)

Gerenciar contas

Nos sistemas de storage da SolidFire, os locatários podem usar contas para permitir que os clientes se conectem a volumes em um cluster. Quando você cria um volume, ele é atribuído a uma conta específica. Você também pode gerenciar contas de administrador de cluster para um sistema de storage SolidFire.

- ["Trabalhar com contas usando CHAP"](#)
- ["Gerenciar contas de usuários de administrador de cluster"](#)

Para mais informações

- ["Documentação do software SolidFire e Element"](#)
- ["Plug-in do NetApp Element para vCenter Server"](#)

Trabalhar com contas usando CHAP

Nos sistemas de storage da SolidFire, os locatários podem usar contas para permitir que

os clientes se conectam a volumes em um cluster. Uma conta contém a autenticação CHAP (Challenge-Handshake Authentication Protocol) necessária para acessar os volumes atribuídos a ela. Quando você cria um volume, ele é atribuído a uma conta específica.

Uma conta pode ter até dois mil volumes atribuídos a ela, mas um volume pode pertencer a apenas uma conta.

Crie uma conta

Você pode criar uma conta para permitir o acesso a volumes.

Cada nome de conta no sistema deve ser exclusivo.

1. Selecione **Gestão > Contas**.
2. Clique em **criar conta**.
3. Introduza um **Nome de utilizador**.
4. Na seção **CHAP Settings**, insira as seguintes informações:



Deixe os campos de credencial em branco para gerar automaticamente qualquer senha.

- **Segredo do Iniciador** para autenticação de sessão de nó CHAP.
 - **Segredo alvo** para autenticação de sessão de nó CHAP.
5. Clique em **criar conta**.

Ver detalhes da conta

Você pode visualizar a atividade de desempenho de contas individuais em um formato gráfico.

As informações do gráfico fornecem informações de e/S e taxa de transferência para a conta. Os níveis de atividade média e pico são mostrados em incrementos de períodos de relatório de 10 segundos. Essas estatísticas incluem atividade para todos os volumes atribuídos à conta.

1. Selecione **Gestão > Contas**.
2. Clique no ícone ações de uma conta.
3. Clique em **Ver detalhes**.

Aqui estão alguns dos detalhes:

- **Status:** O status da conta. Valores possíveis:
 - Ativo: Uma conta ativa.
 - Bloqueado: Uma conta bloqueada.
 - Removido: Uma conta que foi excluída e eliminada.
- **Volumes ativos:** O número de volumes ativos atribuídos à conta.
- **Compression:** A pontuação de eficiência de compressão para os volumes atribuídos à conta.
- **Desduplicação:** A pontuação de eficiência de desduplicação para os volumes atribuídos à conta.
- **Provisionamento fino:** A pontuação de eficiência de provisionamento fino para os volumes atribuídos à

conta.

- **Eficiência geral:** A pontuação geral de eficiência para os volumes atribuídos à conta.

Edite uma conta

Você pode editar uma conta para alterar o status, alterar os segredos CHAP ou modificar o nome da conta.

Modificar as configurações CHAP em uma conta ou remover iniciadores ou volumes de um grupo de acesso pode fazer com que os iniciadores percam o acesso aos volumes inesperadamente. Para verificar se o acesso ao volume não será perdido inesperadamente, efetue sempre logout de sessões iSCSI que serão afetadas por uma alteração de conta ou grupo de acesso e verifique se os iniciadores podem se reconectar aos volumes depois que quaisquer alterações nas configurações do iniciador e nas configurações do cluster tiverem sido concluídas.



Os volumes persistentes associados a serviços de gerenciamento são atribuídos a uma nova conta criada durante a instalação ou atualização. Se você estiver usando volumes persistentes, não modifique ou exclua a conta associada.

1. Selecione **Gestão > Contas**.
2. Clique no ícone ações de uma conta.
3. No menu resultante, selecione **Editar**.
4. **Opcional:** edite o **Nome de usuário**.
5. **Opcional:** clique na lista suspensa **Status** e selecione um status diferente.



Alterar o status para **bloqueado** termina todas as conexões iSCSI para a conta e a conta não está mais acessível. Os volumes associados à conta são mantidos; no entanto, os volumes não são detetáveis iSCSI.

6. **Opcional:** em **Configurações CHAP**, edite as credenciais **segredo do Iniciador** e **segredo do alvo** usadas para autenticação de sessão de nó.



Se você não alterar as credenciais **CHAP Settings**, elas permanecerão as mesmas. Se você deixar os campos de credenciais em branco, o sistema gera novas senhas.

7. Clique em **Salvar alterações**.

Eliminar uma conta

Você pode excluir uma conta quando ela não for mais necessária.

Exclua e limpe quaisquer volumes associados à conta antes de excluir a conta.



Os volumes persistentes associados a serviços de gerenciamento são atribuídos a uma nova conta criada durante a instalação ou atualização. Se você estiver usando volumes persistentes, não modifique ou exclua a conta associada.

1. Selecione **Gestão > Contas**.
2. Clique no ícone ações da conta que deseja excluir.
3. No menu resultante, selecione **Excluir**.

4. Confirme a ação.

Encontre mais informações

- ["Documentação do software SolidFire e Element"](#)
- ["Plug-in do NetApp Element para vCenter Server"](#)

Gerenciar contas de usuários de administrador de cluster

Você pode gerenciar contas de administrador de cluster para um sistema de armazenamento SolidFire criando, excluindo e editando contas de administrador de cluster, alterando a senha do administrador de cluster e configurando configurações LDAP para gerenciar o acesso do sistema para os usuários.

Tipos de conta de administrador de cluster de storage

Existem dois tipos de contas de administrador que podem existir em um cluster de storage que executa o software NetApp Element: A conta de administrador de cluster principal e uma conta de administrador de cluster.

- * Conta de administrador de cluster principal*

Esta conta de administrador é criada quando o cluster é criado. Esta conta é a conta administrativa primária com o mais alto nível de acesso ao cluster. Essa conta é análoga a um usuário root em um sistema Linux. Pode alterar a palavra-passe desta conta de administrador.

- **Conta de administrador de cluster**

Você pode dar a uma conta de administrador de cluster um intervalo limitado de acesso administrativo para executar tarefas específicas dentro de um cluster. As credenciais atribuídas a cada conta de administrador de cluster são usadas para autenticar solicitações de API e IU de elementos no sistema de storage.



É necessária uma conta de administrador de cluster local (não LDAP) para acessar os nós ativos em um cluster através da IU por nó. As credenciais da conta não são necessárias para acessar um nó que ainda não faz parte de um cluster.

Exibir detalhes do administrador do cluster

1. Para criar uma conta de administrador de cluster (não LDAP) em todo o cluster, execute as seguintes ações:
 - a. Clique em **Users > Cluster Admins**.
2. Na página Administradores de cluster da guia usuários, você pode exibir as seguintes informações.
 - **ID**: Número sequencial atribuído à conta de administrador do cluster.
 - **Nome de usuário**: O nome dado à conta de administrador do cluster quando ela foi criada.
 - **Access**: As permissões de usuário atribuídas à conta de usuário. Valores possíveis:
 - leia
 - relatórios

- nós
- unidades
- volumes
- contas
- ClusterAdmins
- administrador



Todas as permissões estão disponíveis para o tipo de acesso do administrador.

- **Type:** O tipo de administrador de cluster. Valores possíveis:
 - Cluster
 - LDAP
- **Atributos:** Se a conta de administrador de cluster foi criada usando a API Element, essa coluna mostrará os pares nome-valor que foram definidos usando esse método.

["Referência da API do software NetApp Element"](#) Consulte .

Crie uma conta de administrador de cluster

Você pode criar novas contas de administrador de cluster com permissões para permitir ou restringir o acesso a áreas específicas do sistema de armazenamento. Ao definir permissões de conta de administrador de cluster, o sistema concede direitos somente de leitura para quaisquer permissões que você não atribua ao administrador do cluster.

Se pretender criar uma conta de administrador de cluster LDAP, certifique-se de que o LDAP está configurado no cluster antes de começar.

["Ative a autenticação LDAP com a interface do usuário Element"](#)

Mais tarde, você pode alterar o Privileges de contas de administrador de cluster para geração de relatórios, nós, unidades, volumes, contas e acesso em nível de cluster. Quando você ativa uma permissão, o sistema atribui acesso de gravação para esse nível. O sistema concede ao usuário administrador acesso somente leitura para os níveis que você não selecionou.

Você também pode remover mais tarde qualquer conta de usuário de administrador de cluster criada por um administrador de sistema. Não é possível remover a conta de administrador do cluster principal criada quando o cluster foi criado.

1. Para criar uma conta de administrador de cluster (não LDAP) em todo o cluster, execute as seguintes ações:
 - a. Clique em **Users > Cluster Admins**.
 - b. Clique em **Create Cluster Admin**.
 - c. Selecione o tipo de usuário **Cluster**.
 - d. Introduza um nome de utilizador e uma palavra-passe para a conta e confirme a palavra-passe.
 - e. Selecione permissões de usuário para aplicar à conta.
 - f. Marque a caixa de seleção para concordar com o Contrato de Licença de Usuário final.
 - g. Clique em **Create Cluster Admin**.

2. Para criar uma conta de administrador de cluster no diretório LDAP, execute as seguintes ações:
 - a. Clique em **Cluster > LDAP**.
 - b. Certifique-se de que a Autenticação LDAP está ativada.
 - c. Clique em **testar autenticação do usuário** e copie o nome distinto que aparece para o usuário ou um dos grupos dos quais o usuário é membro para que você possa colá-lo mais tarde.
 - d. Clique em **Users > Cluster Admins**.
 - e. Clique em **Create Cluster Admin**.
 - f. Selecione o tipo de utilizador LDAP.
 - g. No campo Nome distinto, siga o exemplo na caixa de texto para inserir um nome distinto completo para o usuário ou grupo. Alternativamente, cole-o do nome distinto que você copiou anteriormente.

Se o nome distinto fizer parte de um grupo, qualquer usuário que seja membro desse grupo no servidor LDAP terá permissões dessa conta de administrador.

Para adicionar usuários ou grupos de administrador de cluster LDAP, o formato geral do nome de usuário é "LDAP: Nome distinto completo>".

- a. Selecione permissões de usuário para aplicar à conta.
- b. Marque a caixa de seleção para concordar com o Contrato de Licença de Usuário final.
- c. Clique em **Create Cluster Admin**.

Editar permissões de administrador do cluster

Você pode alterar o Privileges da conta de administrador do cluster para geração de relatórios, nós, unidades, volumes, contas e acesso em nível de cluster. Quando você ativa uma permissão, o sistema atribui acesso de gravação para esse nível. O sistema concede ao usuário administrador acesso somente leitura para os níveis que você não selecionou.

1. Clique em **Users > Cluster Admins**.
2. Clique no ícone ações do administrador do cluster que deseja editar.
3. Clique em **Editar**.
4. Selecione permissões de usuário para aplicar à conta.
5. Clique em **Salvar alterações**.

Alterar senhas para contas de administrador de cluster

Você pode usar a IU do elemento para alterar as senhas do administrador do cluster.

1. Clique em **Users > Cluster Admins**.
2. Clique no ícone ações do administrador do cluster que deseja editar.
3. Clique em **Editar**.
4. No campo alterar palavra-passe, introduza uma nova palavra-passe e confirme-a.
5. Clique em **Salvar alterações**.

Encontre mais informações

- ["Ative a autenticação LDAP com a interface do usuário Element"](#)
- ["Desativar LDAP"](#)
- ["Documentação do software SolidFire e Element"](#)
- ["Plug-in do NetApp Element para vCenter Server"](#)

Gerenciar LDAP

Você pode configurar o LDAP (Lightweight Directory Access Protocol) para habilitar a funcionalidade de login segura baseada em diretório para o storage SolidFire. Você pode configurar o LDAP no nível do cluster e autorizar usuários e grupos LDAP.

O gerenciamento do LDAP envolve a configuração da autenticação LDAP em um cluster do SolidFire usando um ambiente existente do Microsoft Active Directory e testar a configuração.



Você pode usar endereços IPv4 e IPv6.

A ativação do LDAP envolve as seguintes etapas de alto nível, descritas em detalhes:

1. **Etapas de pré-configuração completas para suporte LDAP.** Valide que você tem todos os detalhes necessários para configurar a autenticação LDAP.
2. **Ativar autenticação LDAP.** Use a IU do Element ou a API Element.
3. **Validar a configuração LDAP.** Opcionalmente, verifique se o cluster está configurado com os valores corretos executando o método API `GetLdapConfiguration` ou verificando a configuração LDAP usando a IU do elemento.
4. **Teste a autenticação LDAP** (com o `readonly` usuário). Teste se a configuração LDAP está correta executando o método API `TestLdapAuthentication` ou usando a IU do Element. Para este teste inicial, use o nome de usuário "AMAccountName" do `readonly` usuário. Isso validará se o cluster está configurado corretamente para autenticação LDAP e também validará se as `readonly` credenciais e o acesso estão corretos. Se esta etapa falhar, repita os passos 1 a 3.
5. **Teste a autenticação LDAP** (com uma conta de usuário que você deseja adicionar). Repita o setp 4 com uma conta de usuário que você deseja adicionar como administrador de cluster de elementos. Copie o `distinguished` nome (DN) ou o usuário (ou o grupo). Este DN será utilizado no passo 6.
6. **Adicione o administrador do cluster LDAP** (copie e cole o DN da etapa de autenticação LDAP de teste). Usando a IU do Element ou o método da API `AddLdapClusterAdmin`, crie um novo usuário de administrador de cluster com o nível de acesso apropriado. Para o nome de usuário, cole no DN completo que você copiou na Etapa 5. Isso garante que o DN esteja formatado corretamente.
7. **Teste o acesso de administrador do cluster.** Faça login no cluster usando o usuário de administrador de cluster LDAP recém-criado. Se tiver adicionado um grupo LDAP, pode iniciar sessão como qualquer utilizador nesse grupo.

Conclua as etapas de pré-configuração para suporte a LDAP

Antes de ativar o suporte LDAP no Element, você deve configurar um Windows Active Directory Server e executar outras tarefas de pré-configuração.

Passos

1. Configurar um Windows Active Directory Server.

2. * Opcional: * Ativar suporte LDAPS.
3. Crie usuários e grupos.
4. Crie uma conta de serviço somente leitura (como "somente leitura") a ser usada para pesquisar o diretório LDAP.

Ative a autenticação LDAP com a interface do usuário Element

Pode configurar a integração do sistema de armazenamento com um servidor LDAP existente. Isso permite que os administradores LDAP gerenciem centralmente o acesso ao sistema de storage para os usuários.

Você pode configurar o LDAP com a interface do usuário Element ou com a API Element. Este procedimento descreve como configurar o LDAP usando a IU do Element.

Este exemplo mostra como configurar a autenticação LDAP no SolidFire e usa `SearchAndBind` como o tipo de autenticação. O exemplo usa um único servidor ativo Directory do Windows Server 2012 R2.

Passos

1. Clique em **Cluster > LDAP**.
2. Clique em **Yes** para ativar a autenticação LDAP.
3. Clique em **Adicionar um servidor**.
4. Introduza o **Nome do anfitrião/endereço IP**.



Um número de porta personalizado opcional também pode ser inserido.

Por exemplo, para adicionar um número de porta personalizado, introduza [nome do anfitrião ou endereço ip>:<port number>

5. **Opcional:** Selecione **Use LDAPS Protocol**.
6. Insira as informações necessárias em **Configurações gerais**.

LDAP Servers

| | | |
|----------------------|---|------------------------|
| Host Name/IP Address | <input type="text" value="192.168.9.99"/> | Remove |
| | <input type="checkbox"/> Use LDAPS Protocol | |

[Add a Server](#)

General Settings

| | | |
|----------------------|---|--|
| Auth Type | <input type="text" value="Search and Bind"/> | ▼ |
| Search Bind DN | <input type="text" value="msmyth@thesmyths.ca"/> | |
| Search Bind Password | <input type="text" value="e.g. password"/> | <input type="checkbox"/> Show password |
| User Search Base DN | <input type="text" value="OU=Home users,DC=thesmyths,DC=ca"/> | |
| User Search Filter | <input type="text" value="(&(objectClass=person)((sAMAccountName=%USER"/> | |
| Group Search Type | <input type="text" value="Active Directory"/> | ▼ |
| Group Search Base DN | <input type="text" value="OU=Home users,DC=thesmyths,DC=ca"/> | |

[Save Changes](#)

7. Clique em **Ativar LDAP**.
8. Clique em **Test User Authentication** (testar autenticação do utilizador) se pretender testar o acesso ao servidor de um utilizador.
9. Copie o nome distinto e as informações do grupo de usuários que aparecem para uso posterior ao criar administradores de cluster.
10. Clique em **Salvar alterações** para salvar as novas configurações.
11. Para criar um usuário neste grupo para que qualquer pessoa possa fazer login, complete o seguinte:
 - a. Clique em **User > View**.

Create a New Cluster Admin



Select User Type

Cluster LDAP

Enter User Details

Distinguished Name

CN=StorageAdmins,OU=Home
users,DC=thesmyths,DC=ca

Select User Permissions

- | | |
|------------------------------------|--|
| <input type="checkbox"/> Reporting | <input type="checkbox"/> Volumes |
| <input type="checkbox"/> Nodes | <input type="checkbox"/> Accounts |
| <input type="checkbox"/> Drives | <input type="checkbox"/> Cluster Admin |

Accept the Following End User License Agreement

- Para o novo usuário, clique em **LDAP** para o tipo de usuário e cole o grupo que você copiou no campo Nome distinto.
- Selecione as permissões, normalmente todas as permissões.
- Role para baixo até o Contrato de Licença de Usuário final e clique em **Aceito**.
- Clique em **Create Cluster Admin**.

Agora você tem um usuário com o valor de um grupo do ative Directory.

Para testar isso, faça logout da IU do Element e faça login novamente como um usuário nesse grupo.

Ative a autenticação LDAP com a API Element

Pode configurar a integração do sistema de armazenamento com um servidor LDAP existente. Isso permite que os administradores LDAP gerenciem centralmente o acesso ao sistema de storage para os usuários.

Você pode configurar o LDAP com a interface do usuário Element ou com a API Element. Este procedimento descreve como configurar o LDAP usando a API Element.

Para utilizar a autenticação LDAP num cluster SolidFire, ative primeiro a autenticação LDAP no cluster utilizando o `EnableLdapAuthentication` método API.

Passos

1. Ative a autenticação LDAP primeiro no cluster usando o `EnableLdapAuthentication` método API.
2. Introduza as informações necessárias.

```
{
  "method": "EnableLdapAuthentication",
  "params": {
    "authType": "SearchAndBind",
    "groupSearchBaseDN": "dc=prodtest,dc=solidfire,dc=net",
    "groupSearchType": "ActiveDirectory",
    "searchBindDN": "SFReadOnly@prodtest.solidfire.net",
    "searchBindPassword": "ReadOnlyPW",
    "userSearchBaseDN": "dc=prodtest,dc=solidfire,dc=net ",
    "userSearchFilter":
    " (&(objectClass=person) (sAMAccountName=%USERNAME%)) "
    "serverURIs": [
      "ldap://172.27.1.189",
    ]
  },
  "id": "1"
}
```

3. Altere os valores dos seguintes parâmetros:

| Parâmetros utilizados | Descrição |
|--|--|
| AuthType: SearchAndBind | Determina que o cluster usará a conta de serviço readonly para primeiro procurar o usuário que está sendo autenticado e, posteriormente, vincular esse usuário se for encontrado e autenticado. |
| GroupSearchBaseDN: dc-prodtest,dc-SolidFire,DC-net | Especifica a localização na árvore LDAP para começar a procurar grupos. Para este exemplo, usamos a raiz da nossa árvore. Se a árvore LDAP for muito grande, talvez você queira definir isso como uma subárvore mais granular para diminuir os tempos de pesquisa. |
| UserSearchBaseDN: dc-prodtest,dc-SolidFire,DC-NET | Especifica a localização na árvore LDAP para começar a procurar usuários. Para este exemplo, usamos a raiz da nossa árvore. Se a árvore LDAP for muito grande, talvez você queira definir isso como uma subárvore mais granular para diminuir os tempos de pesquisa. |

| Parâmetros utilizados | Descrição |
|---|---|
| GroupSearchType: ActiveDirectory | Usa o servidor do Active Directory do Windows como servidor LDAP. |
| <pre>userSearchFilter: " (&(objectClass=person) (sAMAccountName=%USERNAME%)) "</pre> <p>Para usar o userPrincipalName (endereço de e-mail para login), você pode alterar o userSearchFilter para:</p> <pre>" (&(objectClass=person) (userPrincipalName=%USERNAME%)) "</pre> <p>Ou, para pesquisar userPrincipalName e sAMAccountName, você pode usar o seguinte userSearchFilter:</p> <pre>" (&(objectClass=person) (</pre> | (SAMAccountName) (userPrincipalName:%USERNAME%)" ---- |
| <p>Aproveita o sAMAccountName como nosso nome de usuário para fazer login no cluster do SolidFire. Essas configurações dizem ao LDAP que procure o nome de usuário especificado durante o login no atributo sAMAccountName e também limitam a pesquisa a entradas que têm "pessoa" como um valor no atributo objectClass.</p> | SearchBindDN |
| <p>Este é o nome distinto do usuário readonly que será usado para pesquisar o diretório LDAP. Para o diretório ativo, geralmente é mais fácil usar o userPrincipalName (formato de endereço de e-mail) para o usuário.</p> | SearchBindPassword |

Para testar isso, faça logout da IU do Element e faça login novamente como um usuário nesse grupo.

Ver detalhes do LDAP

Exibir informações LDAP na página LDAP na guia Cluster.



Tem de ativar o LDAP para visualizar estas definições de configuração LDAP.

1. Para exibir detalhes do LDAP com a IU do Element, clique em **Cluster > LDAP**.

- **Nome do host/endereço IP:** Endereço de um servidor de diretório LDAP ou LDAPS.
- **Auth Type:** O método de autenticação do usuário. Valores possíveis:
 - Ligação direta
 - Pesquisa e Bind
- **Pesquisar DN:** Um DN totalmente qualificado para fazer login para realizar uma pesquisa LDAP para o usuário (precisa de acesso ao diretório LDAP).
- **Pesquisar vincular senha:** Senha usada para autenticar o acesso ao servidor LDAP.
- **User Search base DN:** O DN base da árvore usada para iniciar a pesquisa do usuário. O sistema procura a subárvore a partir da localização especificada.
- **Filtro de pesquisa do usuário:** Insira o seguinte usando seu nome de domínio:


```
( & (objectClass=person) ( | (sAMAccountName=%USERNAME%) (userPrincipalName=%USERN
AME%) ) ) )
```
- **Tipo de pesquisa de grupo:** Tipo de pesquisa que controla o filtro de pesquisa de grupo padrão usado. Valores possíveis:
 - Ative Directory: Associação aninhada de todos os grupos LDAP de um usuário.
 - Sem grupos: Sem apoio de grupo.
 - DN do Membro: Grupos do tipo DN do Membro (nível único).
- **Group Search base DN:** O DN base da árvore usado para iniciar a pesquisa de grupo. O sistema procura a subárvore a partir da localização especificada.
- **Testar autenticação do usuário:** Depois que o LDAP estiver configurado, use-o para testar a autenticação do nome de usuário e senha para o servidor LDAP. Insira uma conta que já existe para testar isso. As informações de nome distinto e grupo de usuários são exibidas, que você pode copiar para uso posterior ao criar administradores de cluster.

Teste a configuração LDAP

Depois de configurar o LDAP, você deve testá-lo usando a IU do Element ou o método da API Element `TestLdapAuthentication`.

Passos

1. Para testar a configuração LDAP com a IU do Element, faça o seguinte:
 - a. Clique em **Cluster > LDAP**.
 - b. Clique em **Test LDAP Authentication** (testar autenticação LDAP).
 - c. Resolva quaisquer problemas usando as informações na tabela abaixo:

| Mensagem de erro | Descrição |
|-------------------|---|
| xLDAPUserNotFound | <ul style="list-style-type: none"> • O usuário que está sendo testado não foi encontrado na subárvore configurada <code>userSearchBaseDN</code>. • O <code>userSearchFilter</code> está configurado incorretamente. |

| Mensagem de erro | Descrição |
|---|--|
| <code>xLDAPBindFailed (Error: Invalid credentials)</code> | <ul style="list-style-type: none"> O nome de usuário que está sendo testado é um usuário LDAP válido, mas a senha fornecida está incorreta. O nome de utilizador que está a ser testado é um utilizador LDAP válido, mas a conta está atualmente desativada. |
| <code>xLDAPSearchBindFailed (Error: Can't contact LDAP server)</code> | O URI do servidor LDAP está incorreto. |
| <code>xLDAPSearchBindFailed (Error: Invalid credentials)</code> | O nome de utilizador ou palavra-passe só de leitura está configurado incorretamente. |
| <code>xLDAPSearchFailed (Error: No such object)</code> | O <code>userSearchBaseDN</code> não é um local válido na árvore LDAP. |
| <code>xLDAPSearchFailed (Error: Referral)</code> | <ul style="list-style-type: none"> O <code>userSearchBaseDN</code> não é um local válido na árvore LDAP. Os <code>userSearchBaseDN</code> e <code>groupSearchBaseDN</code> estão em uma ou aninhada. Isso pode causar problemas de permissão. A solução alternativa é incluir a UO nas entradas DN de base de usuário e grupo (por exemplo: <code>ou=storage, cn=company, cn=com</code>) |

2. Para testar a configuração LDAP com a API Element, faça o seguinte:

a. Chame o método `TestLdapAuthentication`.

```
{
  "method": "TestLdapAuthentication",
  "params": {
    "username": "admin1",
    "password": "admin1PASS"
  },
  "id": 1
}
```

b. Reveja os resultados. Se a chamada de API for bem-sucedida, os resultados incluem o nome distinto

do usuário especificado e uma lista de grupos nos quais o usuário é membro.

```
{
  "id": 1
  "result": {
    "groups": [
      "CN=StorageMgmt,OU=PTUsers,DC=prodtest,DC=solidfire,DC=net"
    ],
    "userDN": "CN=Admin1
Jones,OU=PTUsers,DC=prodtest,DC=solidfire,DC=net"
  }
}
```

Desativar LDAP

Você pode desativar a integração LDAP usando a IU do Element.

Antes de começar, deve anotar todas as definições de configuração, porque a desativação do LDAP apaga todas as definições.

Passos

1. Clique em **Cluster > LDAP**.
2. Clique em **não**.
3. Clique em **Desativar LDAP**.

Encontre mais informações

- ["Documentação do software SolidFire e Element"](#)
- ["Plug-in do NetApp Element para vCenter Server"](#)

Gerencie seu sistema

Você pode gerenciar seu sistema na IU do Element. Isso inclui a ativação da autenticação multifator, o gerenciamento de configurações de cluster, o suporte aos padrões de processamento de informações federais (FIPS) e o uso do gerenciamento de chaves externas.

- ["Ativar a autenticação multifator"](#)
- ["Configure as definições do cluster"](#)
- ["Criar um cluster compatível com unidades FIPS"](#)
- ["Comece a usar o gerenciamento de chaves externas"](#)

Para mais informações

- ["Documentação do software SolidFire e Element"](#)

- ["Plug-in do NetApp Element para vCenter Server"](#)

Ativar a autenticação multifator

A autenticação multifator (MFA) usa um provedor de identidade (IDP) de terceiros por meio da Security Assertion Markup Language (SAML) para gerenciar sessões de usuários. O MFA permite que os administradores configurem fatores adicionais de autenticação conforme necessário, como senha e mensagem de texto, senha e mensagem de e-mail.

Configurar a autenticação multifator

Você pode usar essas etapas básicas por meio da API Element para configurar seu cluster para usar a autenticação multifator.

Os detalhes de cada método de API podem ser encontrados no ["Referência da API do Element"](#).

1. Crie uma nova configuração de provedor de identidade (IDP) de terceiros para o cluster chamando o seguinte método de API e passando os metadados IDP no formato JSON: `CreateIdpConfiguration`

Os metadados IDP, em formato de texto simples, são recuperados do IDP de terceiros. Esses metadados precisam ser validados para garantir que estejam formatados corretamente em JSON. Existem vários aplicativos de formatador JSON disponíveis que você pode usar, por exemplo: <https://freeformatter.com/json-escape.html>.

2. Recupere metadados de cluster, via `spMetadataUrl`, para copiar para o IDP de terceiros chamando o seguinte método API: `ListIdpConfigurations`

`SpMetadataUrl` é um URL usado para recuperar metadados do provedor de serviços do cluster para o IDP, a fim de estabelecer um relacionamento de confiança.

3. Configure asserções SAML no IDP de terceiros para incluir o atributo `"NameID"` para identificar exclusivamente um usuário para o Registro de auditoria e para que o Logout único funcione corretamente.
4. Crie uma ou mais contas de usuário de administrador de cluster autenticadas por um IDP de terceiros para autorização chamando o seguinte método de API: `AddIdpClusterAdmin`



O nome de usuário do administrador do cluster IDP deve corresponder ao mapeamento de nome/valor do atributo SAML para o efeito desejado, como mostrado nos exemplos a seguir:

- `bob@company.com` — onde o IDP está configurado para liberar um endereço de e-mail nos atributos SAML.
 - Administrador de cluster - onde o IDP está configurado para liberar uma propriedade de grupo na qual todos os usuários devem ter acesso. Observe que o pareamento Nome/valor do atributo SAML diferencia maiúsculas de minúsculas para fins de segurança.
5. Ative o MFA para o cluster chamando o seguinte método de API: `EnableIdpAuthentication`

Encontre mais informações

- ["Documentação do software SolidFire e Element"](#)

- ["Plug-in do NetApp Element para vCenter Server"](#)

Informações adicionais para autenticação multifator

Você deve estar ciente das seguintes advertências em relação à autenticação multifator.

- Para atualizar os certificados IDP que não são mais válidos, você precisará usar um usuário admin que não seja IDP para chamar o seguinte método de API: `UpdateIdpConfiguration`
- MFA é incompatível com certificados com menos de 2048 bits de comprimento. Por padrão, um certificado SSL de 2048 bits é criado no cluster. Você deve evitar definir um certificado de tamanho menor ao chamar o método API: `SetSSLCertificate`



Se o cluster estiver usando um certificado com menos de 2048 bits de pré-atualização, o certificado do cluster deve ser atualizado com um certificado de 2048 bits ou superior após a atualização para o elemento 12,0 ou posterior.

- Os usuários de administração de IDP não podem ser usados para fazer chamadas de API diretamente (por exemplo, via SDKs ou Postman) ou para outras integrações (por exemplo, OpenStack Cinder ou vCenter Plug-in). Adicione usuários de administrador de cluster LDAP ou usuários de administrador de cluster local se você precisar criar usuários com essas habilidades.

Encontre mais informações

- ["Gerenciamento de storage com a API Element"](#)
- ["Documentação do software SolidFire e Element"](#)
- ["Plug-in do NetApp Element para vCenter Server"](#)

Configure as definições do cluster

Você pode exibir e alterar configurações de todo o cluster e executar tarefas específicas de cluster na guia Cluster da IU do elemento.

Você pode configurar configurações como limite de preenchimento de cluster, acesso de suporte, criptografia em repouso, volumes virtuais, SnapMirror e cliente de transmissão NTP.

Opções

- [Trabalhe com volumes virtuais](#)
- [Use a replicação do SnapMirror entre clusters Element e ONTAP](#)
- [Defina o limite máximo do cluster](#)
- [Ativar e desativar o acesso ao suporte](#)
- ["Como são calculados os limites de blockSpace para o elemento"](#)
- [Ativar e desativar a encriptação para um cluster](#)
- [Gerenciar os termos de uso banner](#)
- [Configurar servidores Network Time Protocol para o cluster a consultar](#)
- [Gerenciar SNMP](#)
- [Gerenciar unidades](#)

- [Gerenciar nós](#)
- [Gerenciar redes virtuais](#)
- [Veja os detalhes das portas Fibre Channel](#)

Encontre mais informações

- ["Documentação do software SolidFire e Element"](#)
- ["Plug-in do NetApp Element para vCenter Server"](#)

Ative e desative a criptografia em repouso para um cluster

Com clusters do SolidFire, é possível criptografar todos os dados em repouso armazenados em unidades de cluster. Você pode ativar a proteção de unidades com autcriptografia (SED) em todo o cluster usando ["criptografia baseada em hardware ou software em repouso"](#)o .

Você pode habilitar a criptografia de hardware em repouso usando a IU ou API do Element. A ativação do recurso de criptografia de hardware em repouso não afeta o desempenho ou a eficiência do cluster. Você pode ativar a criptografia de software em repouso usando apenas a API Element.

A criptografia baseada em hardware em repouso não é ativada por padrão durante a criação do cluster e pode ser ativada e desativada a partir da IU do Element.



Para clusters de storage all-flash do SolidFire, a criptografia de software em repouso deve ser ativada durante a criação do cluster e não pode ser desativada após a criação do cluster.

O que você vai precisar

- Tem o administrador de cluster Privileges para ativar ou alterar as definições de encriptação.
- Para criptografia baseada em hardware em repouso, você garantiu que o cluster esteja em estado íntegro antes de alterar as configurações de criptografia.
- Se você estiver desabilitando a criptografia, dois nós devem estar participando de um cluster para acessar a chave para desativar a criptografia em uma unidade.

Verifique a criptografia no status de repouso

Para ver o status atual da criptografia em repouso e/ou criptografia de software em repouso no cluster, use o ["GetClusterInfo"](#) método. Você pode usar o ["GetSoftwareEncryptionAtRestInfo"](#) método para obter informações que o cluster usa para criptografar dados em repouso.



O painel da IU do software Element no <https://<MVIP>> momento mostra apenas a criptografia em repouso para criptografia baseada em hardware.

Opções

- [Ative a criptografia baseada em hardware em repouso](#)
- [Ative a criptografia baseada em software em repouso](#)
- [Desative a criptografia baseada em hardware em repouso](#)

Ative a criptografia baseada em hardware em repouso



Para ativar a encriptação em repouso utilizando uma configuração de gestão de chaves externas, tem de ativar a encriptação em repouso através do "API". Ativar o uso do botão UI do elemento existente reverterá para o uso de chaves geradas internamente.

1. Na IU do elemento, selecione **Cluster > Settings**.
2. Selecione **Ativar encriptação em repouso**.

Ative a criptografia baseada em software em repouso



A encriptação de software em repouso não pode ser desativada depois de ativada no cluster.

1. Durante a criação do cluster, execute o "[criar método de cluster](#)" com `enableSoftwareEncryptionAtRest` definido como `true`.

Desative a criptografia baseada em hardware em repouso

1. Na IU do elemento, selecione **Cluster > Settings**.
2. Selecione **Desativar criptografia em repouso**.

Encontre mais informações

- "[Documentação do software SolidFire e Element](#)"
- "[Documentação para versões anteriores dos produtos NetApp SolidFire e Element](#)"

Defina o limite máximo do cluster

Você pode alterar o nível no qual o sistema gera um aviso de preenchimento do bloco de cluster usando os passos abaixo. Além disso, você pode usar o método API `ModifyClusterFullThreshold` para alterar o nível em que o sistema gera um aviso de bloco ou metadados.

O que você vai precisar

Você deve ter o administrador de cluster Privileges.

Passos

1. Clique em **Cluster > Settings**.
2. Na seção Configurações completas do cluster, insira uma porcentagem em **Levante um alerta de aviso quando a capacidade de `_%` permanecer antes que o Helix não consiga recuperar de uma falha de nó**.
3. Clique em **Salvar alterações**.

Encontre mais informações

["Como são calculados os limites de blockSpace para o elemento"](#)

Ativar e desativar o acesso ao suporte

Você pode habilitar o acesso ao suporte para permitir temporariamente o acesso da

equipe de suporte do NetApp aos nós de armazenamento via SSH para solução de problemas.

Você deve ter o administrador do cluster Privileges para alterar o acesso ao suporte.

1. Clique em **Cluster > Settings**.
2. Na secção Ativar/Desativar Acesso ao suporte, introduza a duração (em horas) que pretende permitir que o suporte tenha acesso.
3. Clique em **Ativar acesso ao suporte**.
4. **Opcional:** para desativar o acesso ao suporte, clique em **Desativar acesso ao suporte**.

Gerenciar os termos de uso banner

Você pode ativar, editar ou configurar um banner que contenha uma mensagem para o usuário.

Opções

[Ative o banner termos de uso](#) [Edite o banner termos de uso](#) [Desative o banner termos de uso](#)

Ative o banner termos de uso

Você pode habilitar um banner de termos de uso que aparece quando um usuário faz login na IU do Element. Quando o usuário clica no banner, uma caixa de diálogo de texto é exibida contendo a mensagem que você configurou para o cluster. O banner pode ser demitido a qualquer momento.

Você deve ter o administrador de cluster Privileges para habilitar a funcionalidade termos de uso.

1. Clique em **usuários > termos de uso**.
2. No formulário **termos de uso**, insira o texto a ser exibido para a caixa de diálogo termos de uso.



Não exceda 4096 caracteres.

3. Clique em **Ativar**.

Edite o banner termos de uso

Você pode editar o texto que um usuário vê ao selecionar o banner de login dos termos de uso.

O que você vai precisar

- Você deve ter o administrador de cluster Privileges para configurar os termos de uso.
- Certifique-se de que o recurso termos de uso está ativado.

Passos

1. Clique em **usuários > termos de uso**.
2. Na caixa de diálogo **termos de uso**, edite o texto que você deseja exibir.



Não exceda 4096 caracteres.

3. Clique em **Salvar alterações**.

Desative o banner termos de uso

Você pode desativar o banner termos de uso. Com o banner desativado, o usuário não é mais solicitado a aceitar os termos de uso ao usar a IU do elemento.

O que você vai precisar

- Você deve ter o administrador de cluster Privileges para configurar os termos de uso.
- Certifique-se de que os termos de uso estejam ativados.

Passos

1. Clique em **usuários > termos de uso**.
2. Clique em **Desativar**.

Defina o Network Time Protocol (Protocolo de hora de rede)

A configuração do NTP (Network Time Protocol) pode ser feita de duas maneiras: instrua cada nó em um cluster a ouvir transmissões ou instrua cada nó a consultar atualizações em um servidor NTP.

O NTP é usado para sincronizar relógios em uma rede. A ligação a um servidor NTP interno ou externo deve fazer parte da configuração inicial do cluster.

Configurar servidores Network Time Protocol para o cluster a consultar

Você pode instruir cada nó em um cluster a consultar um servidor NTP (Network Time Protocol) para obter atualizações. O cluster contacta apenas servidores configurados e solicita informações NTP a partir deles.

Configure o NTP no cluster para apontar para um servidor NTP local. Você pode usar o endereço IP ou o nome do host FQDN. O servidor NTP predefinido no momento da criação do cluster é definido como `us.pool.ntp.org`; no entanto, uma ligação a este site nem sempre pode ser feita dependendo da localização física do cluster SolidFire.

O uso do FQDN depende se as configurações de DNS do nó de armazenamento individual estão implementadas e operacionais. Para fazer isso, configure os servidores DNS em cada nó de armazenamento e certifique-se de que as portas estão abertas, revisando a página requisitos de porta de rede.

Pode introduzir até cinco servidores NTP diferentes.



Você pode usar endereços IPv4 e IPv6.

O que você vai precisar

Você deve ter o administrador de cluster Privileges para configurar essa configuração.

Passos

1. Configure uma lista de IPs e/ou FQDNs nas configurações do servidor.
2. Certifique-se de que o DNS está configurado corretamente nos nós.
3. Clique em **Cluster > Settings**.
4. Em Network Time Protocol Settings (Definições do protocolo de tempo de rede), selecione **no**, que utiliza a configuração NTP padrão.

5. Clique em **Salvar alterações**.

Encontre mais informações

- ["Documentação do software SolidFire e Element"](#)
- ["Plug-in do NetApp Element para vCenter Server"](#)

Configure o cluster para ouvir transmissões NTP

Usando o modo de broadcast, você pode instruir cada nó em um cluster para ouvir na rede mensagens de broadcast do Network Time Protocol (NTP) de um servidor específico.

O que você vai precisar

- Você deve ter o administrador de cluster Privileges para configurar essa configuração.
- Tem de configurar um servidor NTP na rede como um servidor de difusão.

Passos

1. Clique em **Cluster > Settings**.
2. Introduza o servidor NTP ou servidores que estão a utilizar o modo de transmissão na lista de servidores.
3. Em Network Time Protocol Settings (Definições do protocolo de tempo de rede), selecione **Yes** (Sim) para utilizar um cliente de difusão.
4. Para definir o cliente de broadcast, no campo **Server**, insira o servidor NTP configurado no modo broadcast.
5. Clique em **Salvar alterações**.

Encontre mais informações

- ["Documentação do software SolidFire e Element"](#)
- ["Plug-in do NetApp Element para vCenter Server"](#)

Gerenciar SNMP

Pode configurar o SNMP (Simple Network Management Protocol) no cluster.

Você pode selecionar um solicitante SNMP, selecionar qual versão do SNMP usar, identificar o usuário do modelo de segurança baseado no usuário SNMP (USM) e configurar traps para monitorar o cluster SolidFire. Você também pode visualizar e acessar arquivos de base de informações de gerenciamento.



Você pode usar endereços IPv4 e IPv6.

Detalhes SNMP

Na página SNMP do separador Cluster (Cluster), pode visualizar as seguintes informações.

• MIBs SNMP

Os ficheiros MIB que estão disponíveis para visualização ou transferência.

- * Configurações gerais do SNMP*

Pode ativar ou desativar o SNMP. Depois de ativar o SNMP, pode escolher qual versão utilizar. Se estiver a utilizar a versão 2, pode adicionar requestores e, se estiver a utilizar a versão 3, pode configurar utilizadores USM.

- * Configurações de intercetação SNMP*

Você pode identificar quais armadilhas você deseja capturar. Você pode definir o host, a porta e a cadeia de caracteres da comunidade para cada destinatário da armadilha.

Configurar um solicitante SNMP

Quando o SNMP versão 2 está ativado, pode ativar ou desativar um solicitante e configurar os solicitadores para receber pedidos SNMP autorizados.

1. Clique em **Cluster > SNMP**.
2. Em **General SNMP Settings**, clique em **Yes** para ativar o SNMP.
3. Na lista **versão**, selecione **versão 2**.
4. Na seção **requestors**, insira as informações **Community String** e **Network**.



Por padrão, a cadeia de caracteres da comunidade é pública e a rede é localhost. Você pode alterar essas configurações padrão.

5. **Opcional:** para adicionar outro solicitante, clique em **Add a Requestor** e insira as informações **Community String** e **Network**.
6. Clique em **Salvar alterações**.

Encontre mais informações

- [Configurar traps SNMP](#)
- [Exibir dados de objeto gerenciado usando arquivos da base de informações de gerenciamento](#)

Configurar um utilizador SNMP USM

Ao ativar o SNMP versão 3, tem de configurar um utilizador USM para receber pedidos SNMP autorizados.

1. Clique em **Cluster > SNMP**.
2. Em **General SNMP Settings**, clique em **Yes** para ativar o SNMP.
3. Na lista **versão**, selecione **versão 3**.
4. Na seção **USM Users**, introduza o nome, a palavra-passe e a frase-passe.
5. **Opcional:** para adicionar outro usuário USM, clique em **Adicionar um usuário USM** e insira o nome, a senha e a senha.
6. Clique em **Salvar alterações**.

Configurar traps SNMP

Os administradores de sistema podem usar traps SNMP, também chamados de notificações, para monitorar a integridade do cluster SolidFire.

Quando os traps SNMP estão ativados, o cluster SolidFire gera traps associados a entradas de log de eventos e alertas de sistema. Para receber notificações SNMP, você precisa escolher os traps que devem ser gerados e identificar os destinatários das informações da armadilha. Por padrão, não são geradas armadilhas.

1. Clique em **Cluster > SNMP**.
2. Selecione um ou mais tipos de traps na seção **SNMP Trap Settings** que o sistema deve gerar:
 - Armadilhas de falha do cluster
 - Armadilhas de falha resolvidas pelo cluster
 - Armadilhas de eventos de cluster
3. Na seção **destinatários da armadilha**, insira as informações do host, da porta e da cadeia de caracteres da comunidade para um destinatário.
4. **Opcional:** Para adicionar outro destinatário de armadilha, clique em **Adicionar um destinatário de armadilha** e insira informações de cadeia de caracteres de host, porta e comunidade.
5. Clique em **Salvar alterações**.

Exibir dados de objeto gerenciado usando arquivos da base de informações de gerenciamento

Você pode exibir e baixar os arquivos da base de informações de gerenciamento (MIB) usados para definir cada um dos objetos gerenciados. O recurso SNMP oferece suporte ao acesso somente leitura aos objetos definidos no SolidFire-StorageCluster-MIB.

Os dados estatísticos fornecidos no MIB mostram a atividade do sistema para o seguinte:

- Estatísticas de cluster
- Estatísticas de volume
- Volumes por estatísticas da conta
- Estatísticas dos nós
- Outros dados, como relatórios, erros e eventos do sistema

O sistema também suporta o acesso ao arquivo MIB que contém os pontos de acesso de nível superior (OIDS) para os produtos SF-Series.

Passos

1. Clique em **Cluster > SNMP**.
2. Em **MIBs SNMP**, clique no arquivo MIB que você deseja baixar.
3. Na janela de download resultante, abra ou salve o arquivo MIB.

Gerenciar unidades

Cada nó contém uma ou mais unidades físicas que são usadas para armazenar uma parte dos dados do cluster. O cluster utiliza a capacidade e o desempenho da unidade após a unidade ter sido adicionada com sucesso a um cluster. Você pode usar a IU do

Element para gerenciar unidades.

Para mais informações

- ["Documentação do software SolidFire e Element"](#)
- ["Plug-in do NetApp Element para vCenter Server"](#)

Detalhes da unidade

A página unidades na guia Cluster fornece uma lista das unidades ativas no cluster. Você pode filtrar a página selecionando a partir das guias Ativo, disponível, Remover, Apagar e Falha.

Quando inicializar um cluster pela primeira vez, a lista de unidades ativas fica vazia. Você pode adicionar unidades que não são atribuídas a um cluster e listadas na guia disponível após a criação de um novo cluster do SolidFire.

Os seguintes elementos aparecem na lista de unidades ativas.

- **ID da unidade**

O número sequencial atribuído à unidade.

- **ID do nó**

O número do nó atribuído quando o nó é adicionado ao cluster.

- **Nome do nó**

O nome do nó que abriga a unidade.

- **Slot**

O número do slot onde a unidade está fisicamente localizada.

- **Capacidade**

O tamanho da unidade, em GB.

- **Série**

O número de série da unidade.

- **Desgaste restante**

O indicador do nível de desgaste.

O sistema de armazenamento informa a quantidade aproximada de desgaste disponível em cada unidade de estado sólido (SSD) para gravar e apagar dados. Uma unidade que consumiu 5% dos ciclos de gravação e apagamento projetados relata 95% de desgaste restante. O sistema não atualiza automaticamente as informações de desgaste da unidade; você pode atualizar ou fechar e recarregar a página para atualizar as informações.

- **Tipo**

O tipo de unidade. O tipo pode ser bloco ou metadados.

Gerenciar nós

Você pode gerenciar o storage SolidFire e os nós Fibre Channel na página nós da guia Cluster.

Se um nó recém-adicionado representar mais de 50% da capacidade total do cluster, parte da capacidade desse nó será inutilizável ("encalhado"), de modo que esteja em conformidade com a regra de capacidade. Este continua a ser o caso até que mais armazenamento seja adicionado. Se um nó muito grande for adicionado que também desobedeça à regra de capacidade, o nó anteriormente encalhado não ficará mais encalhado, enquanto o nó recém-adicionado fica encalhado. A capacidade deve ser sempre adicionada em pares para evitar que isso aconteça. Quando um nó fica preso, uma falha de cluster apropriada é lançada.

Encontre mais informações

[Adicione um nó a um cluster](#)

Adicione um nó a um cluster

Você pode adicionar nós a um cluster quando for necessário mais storage ou após a criação do cluster. Os nós exigem configuração inicial quando são ativados pela primeira vez. Depois que o nó é configurado, ele aparece na lista de nós pendentes e você pode adicioná-lo a um cluster.

A versão do software em cada nó em um cluster deve ser compatível. Quando você adiciona um nó a um cluster, o cluster instala a versão do cluster do software NetApp Element no novo nó, conforme necessário.

Você pode adicionar nós de capacidades menores ou maiores a um cluster existente. Você pode adicionar funcionalidades de nós maiores a um cluster para permitir o crescimento de capacidade. Nós maiores adicionados a um cluster com nós menores devem ser adicionados em pares. Isso permite espaço suficiente para que o Double Helix mova os dados caso um dos nós maiores falhe. Você pode adicionar capacidades de nós menores a um cluster de nós maior para melhorar a performance.



Se um nó recém-adicionado representar mais de 50% da capacidade total do cluster, parte da capacidade desse nó será inutilizável ("encalhado"), de modo que esteja em conformidade com a regra de capacidade. Este continua a ser o caso até que mais armazenamento seja adicionado. Se um nó muito grande for adicionado que também desobedeça à regra de capacidade, o nó anteriormente encalhado não ficará mais encalhado, enquanto o nó recém-adicionado fica encalhado. A capacidade deve ser sempre adicionada em pares para evitar que isso aconteça. Quando um nó fica preso, a falha de cluster strandedCapacity é lançada.

["Vídeo do NetApp: Dimensione de acordo com os seus termos: Expandindo um cluster do SolidFire"](#)

Você pode adicionar nós aos dispositivos NetApp HCI.

Passos

1. Selecione **Cluster > nodes**.
2. Clique em **pendente** para ver a lista de nós pendentes.

Quando o processo de adição de nós estiver concluído, eles aparecem na lista ative Nodes. Até então, os nós pendentes aparecem na lista pendente Ativo.

O SolidFire instala a versão do software Element do cluster nos nós pendentes quando você os adiciona a um cluster. Isso pode levar alguns minutos.

3. Execute um dos seguintes procedimentos:

- Para adicionar nós individuais, clique no ícone **ações** para o nó que você deseja adicionar.
- Para adicionar vários nós, marque a caixa de seleção dos nós a serem adicionados e, em seguida, **ações em massa**. **Observação:** se o nó que você está adicionando tiver uma versão diferente do software Element que a versão em execução no cluster, o cluster atualiza assincronamente o nó para a versão do software Element que está sendo executada no master do cluster. Depois que o nó é atualizado, ele se adiciona automaticamente ao cluster. Durante esse processo assíncrono, o nó estará em um estado pendingActive.

4. Clique em **Add**.

O nó aparece na lista de nós ativos.

Encontre mais informações

[Controle de versão e compatibilidade de nós](#)

Controle de versão e compatibilidade de nós

A compatibilidade do nó é baseada na versão do software Element instalada em um nó. Os clusters de storage baseados no software Element fazem automaticamente uma imagem de um nó para a versão do software Element no cluster se o nó e o cluster não estiverem em versões compatíveis.

A lista a seguir descreve os níveis de significância da versão do software que compõem o número da versão do software Element:

- **Maior**

O primeiro número designa uma versão de software. Um nó com um número de componente principal não pode ser adicionado a um cluster contendo nós de um número de patch principal diferente, nem um cluster pode ser criado com nós de versões principais mistas.

- **Menor**

O segundo número designa recursos de software menores ou aprimoramentos aos recursos de software existentes que foram adicionados a uma versão principal. Este componente é incrementado dentro de um componente de versão principal para indicar que esta versão incremental não é compatível com quaisquer outras versões incrementais de software Element com um componente menor diferente. Por exemplo, 11,0 não é compatível com 11,1 e 11,1 não é compatível com 11,2.

- **Micro**

O terceiro número designa um patch compatível (versão incremental) para a versão do software Element representada pelos componentes major.minor. Por exemplo, 11.0.1 é compatível com 11,0.2, e 11.0.2 é compatível com 11,0.3.

Os números de versão maiores e menores devem corresponder para compatibilidade. Os números micro não têm de corresponder para compatibilidade.

Capacidade de cluster em um ambiente de nó misto

Você pode misturar diferentes tipos de nós em um cluster. As séries SF 2405, 3010, 4805, 6010, 9605, 9010, 19210, 38410 e H podem coexistir em um cluster.

O H-Series consiste em H610S-1, H610S-2, H610S-4 e H410S nós. Esses nós são capazes de 10GbE e 25GbE.

É melhor não misturar nós não criptografados e criptografados. Em um cluster de nós mistos, nenhum nó pode ser maior que 33% da capacidade total do cluster. Por exemplo, em um cluster com quatro nós SF-Series 4805, o maior nó que pode ser adicionado sozinho é um SF-Series 9605. O limite de capacidade do cluster é calculado com base na perda potencial do nó maior nessa situação.

A partir do elemento 12,0, os seguintes nós de storage da série SF não são suportados:

- SF3010
- SF6010
- SF9010

Se você atualizar um desses nós de storage para o elemento 12,0, verá um erro informando que esse nó não é compatível com o elemento 12,0.

Exibir detalhes do nó

Você pode exibir detalhes de nós individuais, como tags de serviço, detalhes da unidade e gráficos para estatísticas de utilização e unidade. A página nós da guia Cluster fornece a coluna versão onde você pode exibir a versão do software de cada nó.

Passos

1. Clique em **Cluster > nodes**.
2. Para exibir os detalhes de um nó específico, clique no ícone **ações** de um nó.
3. Clique em **Ver detalhes**.
4. Revise os detalhes do nó:
 - **Node ID**: O ID gerado pelo sistema para o nó.
 - **Nome do nó**: O nome do host para o nó.
 - **disponível 4K IOPS**: O IOPS configurado para o nó.
 - **Função do nó**: A função que o nó tem no cluster. Valores possíveis:
 - Mestre de cluster: O nó que executa tarefas administrativas em todo o cluster e contém o MVIP e o SVIP.
 - Nó do ensemble: Um nó que participa do cluster. Existem 3 ou 5 nós de ensemble dependendo do tamanho do cluster.
 - Fibre Channel: Um nó no cluster.
 - **Tipo de nó**: O tipo de modelo do nó.
 - **Unidades ativas**: O número de unidades ativas no nó.
 - **IP de gerenciamento**: O endereço IP de gerenciamento (MIP) atribuído ao nó para tarefas de administração de rede 1GbE ou 10GbE.

- **IP do cluster:** O endereço IP do cluster (CIP) atribuído ao nó usado para a comunicação entre nós no mesmo cluster.
- **IP de armazenamento:** O endereço IP de armazenamento (SIP) atribuído ao nó usado para descoberta de rede iSCSI e todo o tráfego de rede de dados.
- **ID VLAN de gerenciamento:** O ID virtual para a rede local de gerenciamento.
- **Storage VLAN ID:** O ID virtual para a rede local de armazenamento.
- **Versão:** A versão do software em execução em cada nó.
- **Porta de replicação:** A porta usada em nós para replicação remota.
- **Etiqueta de serviço:** O número exclusivo da etiqueta de serviço atribuído ao nó.

Veja os detalhes das portas Fibre Channel

Você pode exibir detalhes de portas Fibre Channel, como status, nome e endereço de porta, na página portas FC.

Exibir informações sobre as portas Fibre Channel conetadas ao cluster.

Passos

1. Clique em **Cluster > portas FC**.
2. Para filtrar informações nesta página, clique em **filtro**.
3. Reveja os detalhes:
 - **Node ID:** O nó que hospeda a sessão para a conexão.
 - **Nome do nó:** Nome do nó gerado pelo sistema.
 - **Slot:** Número do slot onde a porta Fibre Channel está localizada.
 - **HBA Port:** Porta física no adaptador de barramento de host Fibre Channel (HBA).
 - * WWNN*: O nome do nó mundial.
 - * WWPN*: O nome do porto mundial de destino.
 - * Switch WWN*: Nome mundial do switch Fibre Channel.
 - **Estado do porto:** Estado atual do porto.
 - **NPort ID:** O ID da porta do nó na malha Fibre Channel.
 - **Velocidade:** A velocidade negociada do Fibre Channel. Os valores possíveis são os seguintes:
 - 4Gbps
 - 8Gbps
 - 16Gbps

Encontre mais informações

- ["Documentação do software SolidFire e Element"](#)
- ["Plug-in do NetApp Element para vCenter Server"](#)

Gerenciar redes virtuais

A rede virtual no armazenamento SolidFire permite que o tráfego entre vários clientes

que estão em redes lógicas separadas seja conectado a um cluster. As conexões com o cluster são segregadas na pilha de rede através do uso da marcação VLAN.

Encontre mais informações

- [Adicione uma rede virtual](#)
- [Ative o encaminhamento e encaminhamento virtuais](#)
- [Edite uma rede virtual](#)
- [Editar VRF VLANs](#)
- [Eliminar uma rede virtual](#)

Adicione uma rede virtual

Você pode adicionar uma nova rede virtual a uma configuração de cluster para habilitar uma conexão de ambiente de alocação a vários clientes a um cluster executando o software Element.

O que você vai precisar

- Identifique o bloco de endereços IP que serão atribuídos às redes virtuais nos nós do cluster.
- Identificar um endereço de IP de rede de armazenamento (SVIP) que será usado como um ponto de extremidade para todo o tráfego de armazenamento NetApp Element.



Você deve considerar os seguintes critérios para esta configuração:

- As VLANs que não são compatíveis com VRF exigem que os iniciadores estejam na mesma sub-rede que o SVIP.
- As VLANs habilitadas para VRF não exigem que os iniciadores estejam na mesma sub-rede que o SVIP, e o roteamento é suportado.
- O SVIP padrão não requer que os iniciadores estejam na mesma sub-rede que o SVIP, e o roteamento é suportado.

Quando uma rede virtual é adicionada, uma interface para cada nó é criada e cada um requer um endereço IP de rede virtual. O número de endereços IP especificados ao criar uma nova rede virtual deve ser igual ou maior que o número de nós no cluster. Os endereços de rede virtual são provisionados em massa e atribuídos automaticamente a nós individuais. Não é necessário atribuir manualmente endereços de rede virtuais aos nós do cluster.

Passos

1. Clique em **Cluster > Network**.
2. Clique em **Create VLAN**.
3. Na caixa de diálogo **Create a New VLAN** (criar uma nova VLAN), insira valores nos seguintes campos:
 - **Nome VLAN**
 - *** VLAN Tag***
 - **SVIP**
 - **Máscara de rede**
 - (Opcional) **Descrição**

4. Introduza o endereço **IP inicial** para o intervalo de endereços IP em **blocos de endereços IP**.
5. Introduza o **size** do intervalo IP como o número de endereços IP a incluir no bloco.
6. Clique em **Adicionar um bloco** para adicionar um bloco não contínuo de endereços IP para esta VLAN.
7. Clique em **Create VLAN**.

Ver detalhes da rede virtual

Passos

1. Clique em **Cluster > Network**.
2. Reveja os detalhes.
 - **ID**: ID exclusiva da rede VLAN, que é atribuída pelo sistema.
 - **Nome**: Nome exclusivo atribuído pelo usuário para a rede VLAN.
 - **VLAN Tag**: Tag VLAN atribuída quando a rede virtual foi criada.
 - **SVIP**: Endereço IP virtual de armazenamento atribuído à rede virtual.
 - **Máscara de rede**: Máscara de rede para esta rede virtual.
 - **Gateway**: Endereço IP exclusivo de um gateway de rede virtual. A VRF deve estar ativada.
 - **VRF habilitado**: Indicação de se o roteamento virtual e o encaminhamento estão ativados ou não.
 - **IPs usados**: O intervalo de endereços IP de rede virtual usados para a rede virtual.

Ative o encaminhamento e encaminhamento virtuais

Você pode ativar o roteamento e encaminhamento virtual (VRF), o que permite que várias instâncias de uma tabela de roteamento existam em um roteador e funcionem simultaneamente. Esta funcionalidade está disponível apenas para redes de armazenamento.

Você pode ativar o VRF apenas no momento da criação de uma VLAN. Se você quiser voltar para não-VRF, você deve excluir e recriar a VLAN.

1. Clique em **Cluster > Network**.
2. Para ativar o VRF em uma nova VLAN, selecione **Create VLAN**.
 - a. Insira informações relevantes para o novo VRF/VLAN. Consulte Adicionar uma rede virtual.
 - b. Marque a caixa de seleção **Enable VRF** (Ativar VRF*).
 - c. **Opcional**: Insira um gateway.
3. Clique em **Create VLAN**.

Encontre mais informações

[Adicione uma rede virtual](#)

Edite uma rede virtual

Você pode alterar os atributos da VLAN, como nome da VLAN, máscara de rede e tamanho dos blocos de endereço IP. A tag VLAN e o SVIP não podem ser modificados para uma VLAN. O atributo gateway não é um parâmetro válido para VLANs não VRF.

Se houver iSCSI, replicação remota ou outras sessões de rede, a modificação pode falhar.

Ao gerenciar o tamanho dos intervalos de endereços IP da VLAN, você deve observar as seguintes limitações:

- Você só pode remover endereços IP do intervalo de endereços IP inicial atribuído no momento em que a VLAN foi criada.
- Você pode remover um bloco de endereço IP que foi adicionado após o intervalo de endereços IP inicial, mas não pode redimensionar um bloco IP removendo endereços IP.
- Quando você tenta remover endereços IP, do intervalo de endereços IP inicial ou em um bloco IP, que estão em uso por nós no cluster, a operação pode falhar.
- Não é possível reatribuir endereços IP específicos em uso a outros nós no cluster.

Você pode adicionar um bloco de endereços IP usando o seguinte procedimento:

1. Selecione **Cluster > Network**.
2. Selecione o ícone ações para a VLAN que você deseja editar.
3. Selecione **Editar**.
4. Na caixa de diálogo **Edit VLAN** (Editar VLAN), insira os novos atributos da VLAN.
5. Selecione **Adicionar um bloco** para adicionar um bloco não contínuo de endereços IP para a rede virtual.
6. Selecione **Salvar alterações**.

Link para solução de problemas de artigos da KB

Link para os artigos da base de dados de Conhecimento para obter ajuda com a solução de problemas com o gerenciamento de intervalos de endereços IP de VLAN.

- ["Aviso de IP duplicado depois de adicionar um nó de armazenamento na VLAN no cluster do elemento"](#)
- ["Como determinar quais IP de VLAN estão em uso e quais nós esses IP são atribuídos no elemento"](#)

Editar VRF VLANs

Você pode alterar atributos VRF VLAN, como nome da VLAN, máscara de rede, gateway e blocos de endereço IP.

1. Clique em **Cluster > Network**.
2. Clique no ícone ações da VLAN que você deseja editar.
3. Clique em **Editar**.
4. Insira os novos atributos para a VLAN VRF na caixa de diálogo **Edit VLAN** (Editar VLAN).
5. Clique em **Salvar alterações**.

Eliminar uma rede virtual

Você pode remover um objeto de rede virtual. Você deve adicionar os blocos de endereço a outra rede virtual antes de remover uma rede virtual.

1. Clique em **Cluster > Network**.
2. Clique no ícone ações da VLAN que você deseja excluir.

3. Clique em **Excluir**.
4. Confirme a mensagem.

Encontre mais informações

[Edite uma rede virtual](#)

Criar um cluster compatível com unidades FIPS

A segurança está se tornando cada vez mais crítica para a implantação de soluções em muitos ambientes de clientes. Os Federal Information Processing Standards (FIPS) são padrões para segurança e interoperabilidade de computadores. A criptografia com certificação FIPS 140-2 para dados em repouso é um componente da solução de segurança geral.

- ["Evite misturar nós para unidades FIPS"](#)
- ["Ative a criptografia em repouso"](#)
- ["Identificar se os nós estão prontos para o recurso unidades FIPS"](#)
- ["Ative o recurso unidades FIPS"](#)
- ["Verifique o status da unidade FIPS"](#)
- ["Solucionar problemas do recurso da unidade FIPS"](#)

Evite misturar nós para unidades FIPS

Para se preparar para ativar o recurso unidades FIPS, evite misturar nós onde alguns são capazes de unidades FIPS e outros não.

Um cluster é considerado compatível com unidades FIPS com base nas seguintes condições:

- Todas as unidades são certificadas como unidades FIPS.
- Todos os nós são nós de unidades FIPS.
- A encriptação em repouso (EAR) está ativada.
- O recurso unidades FIPS está ativado. Todas as unidades e nós devem ser capazes de FIPS e a criptografia em repouso deve estar habilitada para habilitar o recurso de unidade FIPS.

Ative a criptografia em repouso

Você pode ativar e desativar a criptografia em todo o cluster em repouso. Esta funcionalidade não está ativada por predefinição. Para dar suporte a unidades FIPS, é necessário habilitar a criptografia em repouso.

1. Na IU do software NetApp Element, clique em **Cluster > Configurações**.
2. Clique em **Ativar encriptação em repouso**.

Encontre mais informações

- [Ativar e desativar a encriptação para um cluster](#)

- ["Documentação do software SolidFire e Element"](#)
- ["Plug-in do NetApp Element para vCenter Server"](#)

Identificar se os nós estão prontos para o recurso unidades FIPS

Você deve verificar se todos os nós no cluster de storage estão prontos para dar suporte a unidades FIPS usando o método da API `GetFipsReport` do software NetApp Element.

O relatório resultante mostra um dos seguintes Estados:

- Nenhum: O nó não é capaz de dar suporte ao recurso de unidades FIPS.
- Parcial: O nó é capaz de FIPS, mas nem todas as unidades são unidades FIPS.
- Pronto: O nó é compatível com FIPS e todas as unidades são unidades FIPS ou nenhuma unidade está presente.

Passos

1. Usando a API Element, verifique se os nós e as unidades do cluster de storage são capazes de unidades FIPS inserindo:

```
GetFipsReport
```

2. Reveja os resultados, observando quaisquer nós que não exibiram um status de Pronto.
3. Para todos os nós que não exibiram o status Pronto, verifique se a unidade é capaz de suportar o recurso unidades FIPS:
 - Usando a API Element, digite: `GetHardwareList`
 - Observe o valor do **DriveEncryptionCapabilityType**. Se for "fips", o hardware poderá suportar o recurso unidades FIPS.

Consulte os detalhes sobre `GetFipsReport` ou `ListDriveHardware` na ["Referência da API do Element"](#).

4. Se a unidade não puder suportar o recurso unidades FIPS, substitua o hardware por hardware FIPS (nó ou unidades).

Encontre mais informações

- ["Documentação do software SolidFire e Element"](#)
- ["Plug-in do NetApp Element para vCenter Server"](#)

Ative o recurso unidades FIPS

Você pode habilitar o recurso unidades FIPS usando o método de API do software NetApp Element `EnableFeature`.

A criptografia em repouso deve estar habilitada no cluster e todos os nós e unidades devem ser capazes de FIPS, conforme indicado quando o `GetFipsReport` exibir um status Pronto para todos os nós.

Passo

1. Usando a API Element, ative o FIPS em todas as unidades inserindo:

```
EnableFeature params: FipsDrives
```

Encontre mais informações

- ["Gerencie o storage com a API Element"](#)
- ["Documentação do software SolidFire e Element"](#)
- ["Plug-in do NetApp Element para vCenter Server"](#)

Verifique o status da unidade FIPS

Você pode verificar se o recurso unidades FIPS está ativado no cluster usando o método de API do software NetApp Element `GetFeatureStatus`, que mostra se o status de unidades FIPS ativadas é verdadeiro ou falso.

1. Usando a API Element, verifique o recurso unidades FIPS no cluster inserindo:

```
GetFeatureStatus
```

2. Revise os resultados da `GetFeatureStatus` chamada de API. Se o valor de unidades FIPS ativadas for verdadeiro, o recurso unidades FIPS será ativado.

```
{"enabled": true,  
"feature": "FipsDrives"  
}
```

Encontre mais informações

- ["Gerencie o storage com a API Element"](#)
- ["Documentação do software SolidFire e Element"](#)
- ["Plug-in do NetApp Element para vCenter Server"](#)

Solucionar problemas do recurso da unidade FIPS

Usando a IU do software NetApp Element, você pode exibir alertas para obter informações sobre falhas do cluster ou erros no sistema relacionados ao recurso unidades FIPS.

1. Usando a IU do Element, selecione **Reporting > Alerts**.
2. Procure avarias no grupo de instrumentos, incluindo:
 - Unidades FIPS incompatíveis
 - O FIPS fica fora de conformidade
3. Para obter sugestões de resolução, consulte informações sobre o código de falha do cluster.

Encontre mais informações

- [Códigos de falha do cluster](#)

- ["Gerencie o storage com a API Element"](#)
- ["Documentação do software SolidFire e Element"](#)
- ["Plug-in do NetApp Element para vCenter Server"](#)

Ative o FIPS 140-2 para HTTPS no cluster

Você pode usar o método EnableFeature API para ativar o modo operacional FIPS 140-2 para comunicações HTTPS.

Com o software NetApp Element, você pode optar por ativar o modo operacional FIPS (Federal Information Processing Standards) 140-2 no cluster. Ativar este modo ativa o módulo de segurança criptográfica (NCSM) do NetApp e aproveita a criptografia com certificação FIPS 140-2 nível 1 para todas as comunicações via HTTPS para a IU e API do NetApp Element.



Depois de ativar o modo FIPS 140-2, ele não pode ser desativado. Quando o modo FIPS 140-2 está ativado, cada nó no cluster reinicializa e executa um autoteste, garantindo que o NCSM esteja corretamente ativado e funcionando no modo certificado FIPS 140-2. Isso causa uma interrupção nas conexões de gerenciamento e armazenamento no cluster. Você deve Planejar com cuidado e apenas ativar esse modo se seu ambiente precisar do mecanismo de criptografia que ele oferece.

Para obter mais informações, consulte as informações da API Element.

Veja a seguir um exemplo da solicitação de API para habilitar o FIPS:

```
{
  "method": "EnableFeature",
  "params": {
    "feature" : "fips"
  },
  "id": 1
}
```

Depois que este modo de funcionamento estiver ativado, todas as comunicações HTTPS utilizam as cifras aprovadas pelo FIPS 140-2.

Encontre mais informações

- [Cifras SSL](#)
- ["Gerencie o storage com a API Element"](#)
- ["Documentação do software SolidFire e Element"](#)
- ["Plug-in do NetApp Element para vCenter Server"](#)

Cifras SSL

As cifras SSL são algoritmos de criptografia usados pelos hosts para estabelecer uma comunicação segura. Existem cifras padrão que o software Element suporta e não

padrão quando o modo FIPS 140-2 está ativado.

As listas a seguir fornecem as cifras SSL (Secure Socket Layer) padrão suportadas pelo software Element e as cifras SSL suportadas quando o modo FIPS 140-2 está ativado:

- **FIPS 140-2 desativado**

TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (DH 2048) - A
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (DH 2048) - A
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (DH 2048) - A
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (DH 2048) - A
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (SECP256R1) - A
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (SECP256R1) - A
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (SECP256R1) - A
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (SECP256R1) - A
TLS_RSA_WITH_3DES_EDE_CBC_SHA (RSA 2048) - C
TLS_RSA_WITH_AES_128_CBC_SHA (RSA 2048) - A.
TLS_RSA_WITH_AES_128_CBC_SHA256 (RSA 2048) - A.
TLS_RSA_WITH_AES_128_GCM_SHA256 (RSA 2048) - A.
TLS_RSA_WITH_AES_256_CBC_SHA (RSA 2048) - A.
TLS_RSA_WITH_AES_256_CBC_SHA256 (RSA 2048) - A.
TLS_RSA_WITH_AES_256_GCM_SHA384 (RSA 2048) - A.
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (RSA 2048) - A
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (RSA 2048) - A
TLS_RSA_WITH_IDEA_CBC_SHA (RSA 2048) - A.
TLS_RSA_WITH_RC4_128_MD5 (RSA 2048) - C
TLS_RSA_WITH_RC4_128_SHA (RSA 2048) - C
TLS_RSA_WITH_SEED_CBC_SHA (RSA 2048) - A.

- **FIPS 140-2 ativado**

TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (DH 2048) - A
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (DH 2048) - A
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (DH 2048) - A

TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (DH 2048) - A

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (SECT571R1) - A

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (SECP256R1) - A

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (SECP256R1) - A

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (SECT571R1) - A

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (SECT571R1) - A

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (SECP256R1) - A

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (SECP256R1) - A

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (SECT571R1) - A

TLS_RSA_WITH_3DES_EDE_CBC_SHA (RSA 2048) - C

TLS_RSA_WITH_AES_128_CBC_SHA (RSA 2048) - A.

TLS_RSA_WITH_AES_128_CBC_SHA256 (RSA 2048) - A.

TLS_RSA_WITH_AES_128_GCM_SHA256 (RSA 2048) - A.

TLS_RSA_WITH_AES_256_CBC_SHA (RSA 2048) - A.

TLS_RSA_WITH_AES_256_CBC_SHA256 (RSA 2048) - A.

TLS_RSA_WITH_AES_256_GCM_SHA384 (RSA 2048) - A.

Encontre mais informações

[Ative o FIPS 140-2 para HTTPS no cluster](#)

Comece a usar o gerenciamento de chaves externas

O gerenciamento de chaves externas (EKM) fornece gerenciamento seguro de chaves de autenticação (AK) em conjunto com um servidor de chaves externas (EKS) fora do cluster. Os AKs são utilizados para bloquear e desbloquear unidades de encriptação automática (SEDs) quando "[criptografia em repouso](#)" o está ativado no cluster. O EKS fornece geração e armazenamento seguros dos AKs. O cluster utiliza o Key Management Interoperability Protocol (KMIP), um protocolo padrão definido PELA OASIS, para se comunicar com o EKS.

- "[Configurar o gerenciamento externo](#)"
- "[Rechavear criptografia de software na chave mestra em repouso](#)"
- "[Recuperar chaves de autenticação inacessíveis ou inválidas](#)"
- "[Comandos externos da API de gerenciamento de chaves](#)"

Encontre mais informações

- ["CreateCluster API que pode ser usada para habilitar a criptografia de software em repouso"](#)
- ["Documentação do software SolidFire e Element"](#)
- ["Documentação para versões anteriores dos produtos NetApp SolidFire e Element"](#)

Configurar o gerenciamento de chaves externas

Você pode seguir estas etapas e usar os métodos da API Element listados para configurar seu recurso de gerenciamento de chaves externas.

O que você vai precisar

- Se você estiver configurando o gerenciamento de chaves externas em combinação com a criptografia de software em repouso, habilitou a criptografia de software em repouso usando o ["CreateCluster"](#) método em um novo cluster que não contém volumes.

Passos

1. Estabeleça uma relação de confiança com o servidor de chave externa (EKS).
 - a. Crie um par de chaves públicas/privadas para o cluster de elementos que é usado para estabelecer uma relação de confiança com o servidor de chaves chamando o seguinte método de API: ["CreatePublicPrivateKeyPair"](#)
 - b. Obtenha o pedido de assinatura de certificado (CSR) que a Autoridade de Certificação precisa assinar. O CSR permite que o servidor de chaves verifique se o cluster do elemento que vai acessar as chaves é autenticado como o cluster do elemento. Chame o seguinte método API: ["GetClientCertificateSignRequest"](#)
 - c. Utilize a EKS/Certificate Authority para assinar a CSR recuperada. Consulte a documentação de terceiros para obter mais informações.
2. Crie um servidor e um provedor no cluster para se comunicar com o EKS. Um provedor de chaves define onde uma chave deve ser obtida, e um servidor define os atributos específicos do EKS que serão comunicados.
 - a. Crie um provedor de chaves onde os detalhes do servidor de chaves residirão chamando o seguinte método de API: ["CreateKeyProviderKmpip"](#)
 - b. Crie um servidor de chaves fornecendo o certificado assinado e o certificado de chave pública da Autoridade de Certificação chamando os seguintes métodos de API: ["CreateKeyServerKmpip"](#) ["TestKeyServerKmpip"](#)

Se o teste falhar, verifique a conectividade e a configuração do servidor. Em seguida, repita o teste.
 - c. Adicione o servidor de chaves ao contentor do provedor de chaves chamando os seguintes métodos de API: ["AddKeyServerToProviderKmpip"](#) ["TestKeyProviderKmpip"](#)

Se o teste falhar, verifique a conectividade e a configuração do servidor. Em seguida, repita o teste.
3. Execute uma das seguintes ações como próxima etapa para criptografia em repouso:
 - a. (Para criptografia de hardware em repouso) ative ["criptografia de hardware em repouso"](#) fornecendo a ID do provedor de chaves que contém o servidor de chaves usado para armazenar as chaves chamando o ["EnableEncryptionAtRest"](#) método API.



É necessário habilitar a criptografia em repouso por meio do ["API"](#). Ativar a criptografia em repouso usando o botão UI do elemento existente fará com que o recurso reverta para o uso de chaves geradas internamente.

- b. (Para criptografia de software em repouso) para ["criptografia de software em repouso"](#) utilizar o provedor de chaves recém-criado, passe o ID do provedor de chaves para o ["RekeySoftwareEncryptionAtRestMasterKey"](#) método API.

Encontre mais informações

- ["Ativar e desativar a encriptação para um cluster"](#)
- ["Documentação do software SolidFire e Element"](#)
- ["Documentação para versões anteriores dos produtos NetApp SolidFire e Element"](#)

Rechavear criptografia de software na chave mestra em repouso

Você pode usar a API Element para rechavear uma chave existente. Esse processo cria uma nova chave mestra de substituição para o servidor de gerenciamento de chaves externo. As chaves mestras são sempre substituídas por novas chaves mestras e nunca duplicadas ou substituídas.

Você pode precisar de rechavear como parte de um dos seguintes procedimentos:

- Crie uma nova chave como parte de uma alteração do gerenciamento de chaves internas para o gerenciamento de chaves externas.
- Crie uma nova chave como reação ou como proteção contra um evento relacionado à segurança.



Este processo é assíncrono e retorna uma resposta antes que a operação de rechavear esteja concluída. Você pode usar o ["GetAsyncResult"](#) método para poll o sistema para ver quando o processo foi concluído.

O que você vai precisar

- Você ativou a criptografia de software em repouso usando o ["CreateCluster"](#) método em um novo cluster que não contém volumes e não tem e/S Use `GetSoftwareEncryptionatRestInfo` para confirmar que o estado está `enabled` antes de prosseguir.
- Você tem ["estabeleceu uma relação de confiança"](#) entre o cluster SolidFire e um servidor de chave externa (EKS). Execute o ["TestKeyProviderKmip"](#) método para verificar se uma conexão com o provedor de chaves está estabelecida.

Passos

1. Execute o ["ListKeyProvidersKmip"](#) comando e copie o ID do provedor de chaves (`keyProviderID`).
2. Execute o ["RekeySoftwareEncryptionAtRestMasterKey"](#) com o `keyManagementType` parâmetro como `external` e `keyProviderID` como o número de ID do provedor de chaves da etapa anterior:

```
{
  "method": "rekeysoftwareencryptionatrestmasterkey",
  "params": {
    "keyManagementType": "external",
    "keyProviderID": "<ID number>"
  }
}
```

3. Copie o `asyncHandle` valor da `RekeySoftwareEncryptionAtRestMasterKey` resposta do comando.
4. Execute o `"GetAsyncResult"` comando com o `asyncHandle` valor da etapa anterior para confirmar a alteração na configuração. A partir da resposta do comando, você deve ver que a configuração de chave mestra mais antiga foi atualizada com novas informações de chave. Copie a nova ID do provedor de chaves para uso em uma etapa posterior.

```
{
  "id": null,
  "result": {
    "createTime": "2021-01-01T22:29:18Z",
    "lastUpdateTime": "2021-01-01T22:45:51Z",
    "result": {
      "keyToDecommission": {
        "keyID": "<value>",
        "keyManagementType": "internal"
      },
      "newKey": {
        "keyID": "<value>",
        "keyManagementType": "external",
        "keyProviderID": <value>
      },
      "operation": "Rekeying Master Key. Master Key management being transferred from Internal Key Management to External Key Management with keyProviderID=<value>",
      "state": "Ready"
    },
    "resultType": "RekeySoftwareEncryptionAtRestMasterKey",
    "status": "complete"
  }
}
```

5. Execute o `GetSoftwareEncryptionatRestInfo` comando para confirmar que os novos detalhes da chave, incluindo o `keyProviderID`, foram atualizados.

```
{
  "id": null,
  "result": {
    "masterKeyInfo": {
      "keyCreatedTime": "2021-01-01T22:29:18Z",
      "keyID": "<updated value>",
      "keyManagementType": "external",
      "keyProviderID": <value>
    },
    "rekeyMasterKeyAsyncResultID": <value>
    "status": "enabled",
    "version": 1
  },
}
```

Encontre mais informações

- ["Gerencie o storage com a API Element"](#)
- ["Documentação do software SolidFire e Element"](#)
- ["Documentação para versões anteriores dos produtos NetApp SolidFire e Element"](#)

Recuperar chaves de autenticação inacessíveis ou inválidas

Ocasionalmente, pode ocorrer um erro que requer a intervenção do utilizador. Em caso de erro, será gerada uma avaria no cluster (designada por código de avaria do cluster). Os dois casos mais prováveis são descritos aqui.

O cluster não consegue desbloquear as unidades devido a uma falha do cluster `KmipServerFault`.

Isso pode ocorrer quando o cluster inicializa pela primeira vez e o servidor de chaves está inacessível ou a chave necessária não está disponível.

1. Siga as etapas de recuperação nos códigos de falha do cluster (se houver).

Uma falha `sliceServiceUnHealthy` pode ser definida porque as unidades de metadados foram marcadas como com falha e colocadas no estado "disponível".

Passos para limpar:

1. Adicione as unidades novamente.
2. Após 3 a 4 minutos, verificar se a `sliceServiceUnhealthy` avaria foi apagada.

Consulte ["códigos de falha do cluster"](#) para obter mais informações.

Comandos externos da API de gerenciamento de chaves

Lista de todas as APIs disponíveis para gerenciar e configurar EKM.

Usado para estabelecer uma relação de confiança entre o cluster e servidores externos de propriedade do cliente:

- `CreatePublicPrivateKeyPair`
- `GetClientCertificateSignRequest`

Usado para definir os detalhes específicos de servidores externos de propriedade do cliente:

- `CreateKeyServerKmpip`
- `ModifyKeyServerKmpip`
- `DeleteKeyServerKmpip`
- `GetKeyServerKmpip`
- `ListKeyServersKmpip`
- `TestKeyServerKmpip`

Usado para criar e manter provedores-chave que gerenciam servidores de chave externos:

- `CreateKeyProviderKmpip`
- `DeleteKeyProviderKmpip`
- `AddKeyServerToProviderKmpip`
- `RemoveKeyServerFromProviderKmpip`
- `GetKeyProviderKmpip`
- `ListKeyProvidersKmpip`
- `RekeySoftwareEncryptionAtRestMasterKey`
- `TestKeyProviderKmpip`

Para obter informações sobre os métodos de API, "[Informações de referência da API](#)" consulte .

Gerenciar volumes e volumes virtuais

Você pode gerenciar os dados em um cluster executando o software Element na guia Gerenciamento na IU do Element. As funções de gerenciamento de cluster disponíveis incluem a criação e o gerenciamento de volumes de dados, grupos de acesso a volumes, iniciadores e políticas de qualidade do serviço (QoS).

- "[Trabalhe com volumes](#)"
- "[Trabalhe com volumes virtuais](#)"
- "[Trabalhar com grupos de acesso de volume e iniciadores](#)"

Para mais informações

- "[Documentação do software SolidFire e Element](#)"
- "[Plug-in do NetApp Element para vCenter Server](#)"

Trabalhe com volumes

O sistema SolidFire provisiona o storage usando volumes. Os volumes são dispositivos de bloco acessados pela rede por clientes iSCSI ou Fibre Channel. Na página volumes na guia Gerenciamento, você pode criar, modificar, clonar e excluir volumes em um nó. Você também pode exibir estatísticas sobre largura de banda de volume e uso de e/S.

Encontre mais informações

- ["Gerenciar políticas de qualidade de serviço"](#)
- ["Crie um volume"](#)
- ["Ver detalhes individuais do desempenho do volume"](#)
- ["Editar volumes ativos"](#)
- ["Eliminar um volume"](#)
- ["Restaurar um volume excluído"](#)
- ["Purgue um volume"](#)
- ["Clonar um volume"](#)
- ["Atribuir LUNs a volumes Fibre Channel"](#)
- ["Aplique uma política de QoS a volumes"](#)
- ["Remova a associação de política de QoS de um volume"](#)

Gerenciar políticas de qualidade de serviço

Uma política de qualidade do serviço (QoS) permite que você crie e salve uma configuração padronizada de qualidade do serviço que pode ser aplicada a muitos volumes. Você pode criar, editar e excluir políticas de QoS na página políticas de QoS na guia Gerenciamento.



Se você estiver usando políticas de QoS, não use QoS personalizado em um volume. A QoS personalizada substituirá e ajustará os valores da política de QoS para configurações de QoS de volume.

["Vídeo do NetApp: Políticas de qualidade de serviço do SolidFire"](#)

["Desempenho e qualidade do serviço"](#) Consulte .

- Crie uma política de QoS
- Editar uma política de QoS
- Excluir uma política de QoS

Crie uma política de QoS

Você pode criar políticas de QoS e aplicá-las ao criar volumes.

1. Selecione **Gerenciamento > políticas de QoS**.
2. Clique em **criar política de QoS**.

3. Introduza o **Nome da política**.
4. Insira os valores de IOPS mínimo*, ***IOPS máximo** e **IOPS** de explosão.
5. Clique em **criar política de QoS**.

Editar uma política de QoS

Você pode alterar o nome de uma política de QoS existente ou editar os valores associados à política. A alteração de uma política de QoS afeta todos os volumes associados à política.

1. Selecione **Gerenciamento > políticas de QoS**.
2. Clique no ícone ações da política de QoS que você deseja editar.
3. No menu resultante, selecione **Editar**.
4. Na caixa de diálogo **Editar política de QoS**, modifique as seguintes propriedades conforme necessário:
 - Nome da política
 - IOPS mín
 - IOPS máx
 - IOPS de explosão
5. Clique em **Salvar alterações**.

Excluir uma política de QoS

Você pode excluir uma política de QoS se ela não for mais necessária. Quando você exclui uma política de QoS, todos os volumes associados à política mantêm as configurações de QoS, mas tornam-se não associados a uma política.



Se você estiver tentando desassociar um volume de uma política de QoS, poderá alterar as configurações de QoS desse volume para personalizado.

1. Selecione **Gerenciamento > políticas de QoS**.
2. Clique no ícone ações da política de QoS que você deseja excluir.
3. No menu resultante, selecione **Excluir**.
4. Confirme a ação.

Encontre mais informações

- ["Remova a associação de política de QoS de um volume"](#)
- ["Documentação do software SolidFire e Element"](#)
- ["Plug-in do NetApp Element para vCenter Server"](#)

Gerenciar volumes

O sistema SolidFire provisiona o storage usando volumes. Os volumes são dispositivos de bloco acessados pela rede por clientes iSCSI ou Fibre Channel.

Na página volumes na guia Gerenciamento, você pode criar, modificar, clonar e excluir volumes em um nó.

Crie um volume

Você pode criar um volume e associar o volume a uma determinada conta. Cada volume deve ser associado a uma conta. Esta associação dá à conta acesso ao volume através dos iniciadores iSCSI usando as credenciais CHAP.

Você pode especificar configurações de QoS para um volume durante a criação.

1. Selecione **Management > volumes**.
2. Clique em **criar volume**.
3. Na caixa de diálogo **criar um novo volume**, insira o **Nome do volume**.
4. Introduza o tamanho total do volume.



A seleção padrão do tamanho do volume está em GB. Você pode criar volumes usando tamanhos medidos em GB ou GiB:

- 1GB 1 000 000 000 bytes
- 1GiB 1 073 741 824 bytes

5. Selecione um **tamanho do bloco** para o volume.
6. Clique na lista suspensa **Account** e selecione a conta que deve ter acesso ao volume.

Se uma conta não existir, clique no link **criar conta**, insira um novo nome de conta e clique em **criar**. A conta é criada e associada ao novo volume.



Se houver mais de 50 contas, a lista não será exibida. Comece a digitar e a função de preenchimento automático exibe valores possíveis para você escolher.

7. Para definir a **qualidade do serviço**, execute um dos seguintes procedimentos:
 - a. Em **Política**, você pode selecionar uma política de QoS existente, se disponível.
 - b. Em **Configurações personalizadas**, defina valores mínimos, máximos e de burst personalizados para IOPS ou use os valores de QoS padrão.

Os volumes que têm um valor máximo de IOPS ou Burst maior que 20.000 IOPS podem exigir alta profundidade da fila ou várias sessões para atingir esse nível de IOPS em um único volume.

8. Clique em **criar volume**.

Ver detalhes do volume

1. Selecione **Management > volumes**.
2. Reveja os detalhes.
 - **ID**: O ID gerado pelo sistema para o volume.
 - **Nome**: O nome dado ao volume quando foi criado.
 - **Conta**: O nome da conta atribuída ao volume.
 - **Grupos de acesso**: O nome do grupo de acesso ao volume ou grupos aos quais o volume pertence.
 - **Access**: O tipo de acesso atribuído ao volume quando foi criado. Valores possíveis:
 - Ler / escrever: Todas as leituras e gravações são aceitas.

- Somente leitura: Todas as atividades de leitura permitidas; não são permitidas gravações.
- Bloqueado: Apenas acesso de administrador permitido.
- ReplicationTarget: Designado como um volume de destino em um par de volumes replicado.
- **Usado:** A porcentagem de espaço usado no volume.
- * **Tamanho*:** O tamanho total (em GB) do volume.
- **Snapshots:** O número de instantâneos criados para o volume.
- **Política de QoS:** O nome e o link para a política de QoS definida pelo usuário.
- **IOPS mínimo:** O número mínimo de IOPS garantido para o volume.
- **IOPS máximo:** O número máximo de IOPS permitido para o volume.
- **IOPS de explosão:** O número máximo de IOPS permitido durante um curto período de tempo para o volume. Padrão: 15.000.
- **Atributos:** Atributos que foram atribuídos ao volume como um par chave/valor por meio de um método API.
- **512e:** Indicação de se 512e está ativado em um volume. Valores possíveis:
 - Sim
 - Não
- **Criado em:** A data e a hora em que o volume foi criado.

Ver detalhes individuais do volume

Você pode exibir estatísticas de desempenho para volumes individuais.

1. Selecione **Reporting > volume Performance**.
2. Na lista de volumes, clique no ícone ações de um volume.
3. Clique em **Ver detalhes**.

Uma bandeja aparece na parte inferior da página contendo informações gerais sobre o volume.

4. Para ver informações mais detalhadas sobre o volume, clique em **Ver mais detalhes**.

O sistema apresenta informações detalhadas, bem como gráficos de desempenho para o volume.

Editar volumes ativos

Você pode modificar atributos de volume, como valores de QoS, tamanho do volume e a unidade de medida na qual os valores de byte são calculados. Você também pode modificar o acesso à conta para uso de replicação ou restringir o acesso ao volume.

Você pode redimensionar um volume quando houver espaço suficiente no cluster nas seguintes condições:

- Condições normais de funcionamento.
- Erros de volume ou falhas estão sendo relatados.
- O volume está sendo clonado.
- O volume está sendo ressincido.

Passos

1. Selecione **Management > volumes**.
2. Na janela **Ativo**, clique no ícone ações do volume que deseja editar.
3. Clique em **Editar**.
4. * Opcional: * Alterar o tamanho total do volume.
 - Você pode aumentar, mas não diminuir, o tamanho do volume. Você só pode redimensionar um volume em uma única operação de redimensionamento. As operações de coleta de lixo e as atualizações de software não interrompem a operação de redimensionamento.
 - Se você estiver ajustando o tamanho do volume para replicação, primeiro deverá aumentar o tamanho do volume atribuído como destino de replicação. Em seguida, você pode redimensionar o volume de origem. O volume de destino pode ser maior ou igual em tamanho ao volume de origem, mas não pode ser menor.

A seleção padrão do tamanho do volume está em GB. Você pode criar volumes usando tamanhos medidos em GB ou GiB:

- 1GB 1 000 000 000 bytes
 - 1GiB 1 073 741 824 bytes
5. **Opcional:** Selecione um nível de acesso à conta diferente de um dos seguintes:
 - Somente leitura
 - Leitura/escrita
 - Bloqueado
 - Destino de replicação

6. **Opcional:** Selecione a conta que deve ter acesso ao volume.

Se a conta não existir, clique no link **criar conta**, insira um novo nome de conta e clique em **criar**. A conta é criada e associada ao volume.



Se houver mais de 50 contas, a lista não será exibida. Comece a digitar e a função de preenchimento automático exibe valores possíveis para você escolher.

7. **Opcional:** para alterar a seleção em **qualidade de Serviço**, faça um dos seguintes procedimentos:
 - a. Em **Política**, você pode selecionar uma política de QoS existente, se disponível.
 - b. Em **Configurações personalizadas**, defina valores mínimos, máximos e de burst personalizados para IOPS ou use os valores de QoS padrão.



Se você estiver usando políticas de QoS em um volume, poderá definir QoS personalizado para remover a afiliação da política de QoS com o volume. A QoS personalizada substituirá e ajustará os valores da política de QoS para configurações de QoS de volume.



Ao alterar os valores de IOPS, você deve aumentar em dezenas ou centenas. Os valores de entrada requerem números inteiros válidos.



Configure volumes com um valor de burst extremamente alto. Isso permite que o sistema processe cargas de trabalho sequenciais em blocos grandes ocasionais com mais rapidez, ao mesmo tempo em que restringe o IOPS contínuo de um volume.

8. Clique em **Salvar alterações**.

Eliminar um volume

Você pode excluir um ou mais volumes de um cluster de armazenamento de elementos.

O sistema não limpa imediatamente um volume eliminado; o volume permanece disponível durante cerca de oito horas. Se restaurar um volume antes de o sistema o purgar, o volume volta a ficar online e as ligações iSCSI são restauradas.

Se um volume usado para criar um snapshot for excluído, seus snapshots associados ficarão inativos. Quando os volumes de origem excluídos são removidos, os snapshots inativos associados também são removidos do sistema.



Volumes persistentes associados a serviços de gerenciamento são criados e atribuídos a uma nova conta durante a instalação ou atualização. Se você estiver usando volumes persistentes, não modifique ou exclua os volumes ou a conta associada.

Passos

1. Selecione **Management > volumes**.
2. Para excluir um único volume, execute as seguintes etapas:
 - a. Clique no ícone ações do volume que deseja excluir.
 - b. No menu resultante, clique em **Excluir**.
 - c. Confirme a ação.

O sistema move o volume para a área **Deleted** na página **volumes**.

3. Para excluir vários volumes, execute as seguintes etapas:
 - a. Na lista de volumes, marque a caixa ao lado de quaisquer volumes que você deseja excluir.
 - b. Clique em **ações em massa**.
 - c. No menu resultante, clique em **Excluir**.
 - d. Confirme a ação.

O sistema move os volumes para a área **Deleted** na página **volumes**.

Restaurar um volume excluído

Você pode restaurar um volume no sistema se ele tiver sido excluído, mas ainda não purgado. O sistema limpa automaticamente um volume cerca de oito horas depois de ter sido eliminado. Se o sistema tiver purgado o volume, não poderá restaurá-lo.

1. Selecione **Management > volumes**.
2. Clique na guia **Deleted** para exibir a lista de volumes excluídos.
3. Clique no ícone ações do volume que deseja restaurar.

- No menu resultante, clique em **Restaurar**.
- Confirme a ação.

O volume é colocado na lista **ativo** volumes e as conexões iSCSI ao volume são restauradas.

Purgue um volume

Quando um volume é purgado, ele é removido permanentemente do sistema. Todos os dados no volume são perdidos.

O sistema limpa automaticamente os volumes eliminados oito horas após a eliminação. No entanto, se você quiser limpar um volume antes da hora programada, você pode fazê-lo.

- Selecione **Management > volumes**.
- Clique no botão **Deleted**.
- Execute as etapas para limpar um único volume ou vários volumes.

| Opção | Passos |
|------------------------|--|
| Purgue um único volume | <ol style="list-style-type: none"> Clique no ícone ações do volume que deseja limpar. Clique em Purge. Confirme a ação. |
| Purgue vários volumes | <ol style="list-style-type: none"> Selecione os volumes que deseja limpar. Clique em ações em massa. No menu resultante, selecione Purge. Confirme a ação. |

Clonar um volume

Você pode criar um clone de um único volume ou vários volumes para fazer uma cópia pontual dos dados. Quando você clonar um volume, o sistema cria um snapshot do volume e cria uma cópia dos dados referenciados pelo snapshot. Este é um processo assíncrono, e a quantidade de tempo que o processo requer depende do tamanho do volume que você está clonando e da carga atual do cluster.

O cluster dá suporte a até duas solicitações de clone em execução por volume de cada vez e até oito operações de clone de volume ativo de cada vez. Solicitações além desses limites são enfileiradas para processamento posterior.



Os sistemas operacionais diferem em como tratam os volumes clonados. O VMware ESXi tratará um volume clonado como uma cópia de volume ou um volume instantâneo. O volume será um dispositivo disponível para usar para criar um novo datastore. Para obter mais informações sobre a montagem de volumes de clones e o manuseio de LUNs instantâneos, consulte a documentação da VMware no ["Montagem de uma cópia do datastore VMFS"](#) e ["Gerenciando armazenamentos de dados VMFS duplicados"](#).



Antes de truncar um volume clonado clonado clonando para um tamanho menor, certifique-se de preparar as partições para que elas se encaixem no volume menor.

Passos

1. Selecione **Management > volumes**.
2. Para clonar um único volume, execute as seguintes etapas:
 - a. Na lista de volumes na página **Ativo**, clique no ícone ações do volume que deseja clonar.
 - b. No menu resultante, clique em **Clone**.
 - c. Na janela **Clone volume**, insira um nome de volume para o volume recém clonado.
 - d. Selecione um tamanho e uma medida para o volume usando a caixa de rotação **tamanho do volume** e a lista.



A seleção padrão do tamanho do volume está em GB. Você pode criar volumes usando tamanhos medidos em GB ou GiB:

- 1GB 1 000 000 000 bytes
 - 1GiB 1 073 741 824 bytes
- e. Selecione o tipo de acesso para o volume recém clonado.
 - f. Selecione uma conta para associar ao volume recém-clonado na lista **conta**.



Você pode criar uma conta durante esta etapa se clicar no link **criar conta**, inserir um nome de conta e clicar em **criar**. O sistema adiciona automaticamente a conta à lista **Account** depois de criá-la.

3. Para clonar vários volumes, execute as seguintes etapas:
 - a. Na lista de volumes na página **Ativo**, marque a caixa ao lado de qualquer volume que você deseja clonar.
 - b. Clique em **ações em massa**.
 - c. No menu resultante, selecione **Clone**.
 - d. Na caixa de diálogo **Clone vários volumes**, insira um prefixo para os volumes clonados no campo **New volume Name Prefix**.
 - e. Selecione uma conta para associar aos volumes clonados na lista **conta**.
 - f. Selecione o tipo de acesso para os volumes clonados.
4. Clique em **Iniciar clonagem**.



Aumentar o tamanho de volume de um clone resulta em um novo volume com espaço livre adicional no final do volume. Dependendo de como você usa o volume, você pode precisar estender partições ou criar novas partições no espaço livre para usá-lo.

Para mais informações

- ["Documentação do software SolidFire e Element"](#)
- ["Plug-in do NetApp Element para vCenter Server"](#)

Atribuir LUNs a volumes Fibre Channel

Você pode alterar a atribuição de LUN para um volume Fibre Channel em um grupo de

acesso de volume. Você também pode fazer atribuições de LUN de volume Fibre Channel ao criar um grupo de acesso de volume.

A atribuição de novos LUNs Fibre Channel é uma função avançada e pode ter consequências desconhecidas no host de conexão. Por exemplo, a nova ID LUN pode não ser descoberta automaticamente no host e o host pode exigir uma nova verificação para descobrir a nova ID LUN.

1. Selecione **Gerenciamento > grupos de acesso**.
2. Clique no ícone ações do grupo de acesso que deseja editar.
3. No menu resultante, selecione **Editar**.
4. Em **Assign LUN IDs** na caixa de diálogo **Edit volume Access Group** (Editar grupo de acesso de volume), clique na seta na lista **LUN Assignments** (Atribuições de LUN).
5. Para cada volume na lista a que pretende atribuir um LUN, introduza um novo valor no campo **LUN** correspondente.
6. Clique em **Salvar alterações**.

Aplique uma política de QoS a volumes

Você pode aplicar em massa uma política de QoS existente a um ou mais volumes.

A política de QoS que você deseja aplicar em massa deve existir.

1. Selecione **Management > volumes**.
2. Na lista de volumes, marque a caixa ao lado de quaisquer volumes aos quais você deseja aplicar a política de QoS.
3. Clique em **ações em massa**.
4. No menu resultante, clique em **aplicar política de QoS**.
5. Selecione a política de QoS na lista suspensa.
6. Clique em **aplicar**.

Encontre mais informações

[Políticas de qualidade de Serviço](#)

Remova a associação de política de QoS de um volume

Você pode remover uma associação de política de QoS de um volume selecionando configurações de QoS personalizadas.

O volume que você deseja modificar deve estar associado a uma política de QoS.

1. Selecione **Management > volumes**.
2. Clique no ícone ações de um volume que contém uma política de QoS que você deseja modificar.
3. Clique em **Editar**.
4. No menu resultante em **qualidade do serviço**, clique em **Configurações personalizadas**.
5. Modifique **min IOPS**, **Max IOPS** e **Burst IOPS** ou mantenha as configurações padrão.
6. Clique em **Salvar alterações**.

Encontre mais informações

[Excluir uma política de QoS](#)

Trabalhe com volumes virtuais

Você pode exibir informações e executar tarefas para volumes virtuais e seus contentores de storage associados, pontos de extremidade de protocolo, ligações e hosts usando a IU do Element.

O sistema de storage do software NetApp Element é fornecido com o recurso volumes virtuais (vols) desativado. Você deve executar uma tarefa única de habilitar manualmente a funcionalidade do vSphere VVol por meio da IU do Element.

Depois de ativar a funcionalidade VVol, aparece uma guia VVols na interface do usuário que oferece monitoramento relacionado ao VVols e opções de gerenciamento limitadas. Além disso, um componente de software do lado do storage conhecido como Provedor VASA atua como um serviço de reconhecimento de armazenamento para o vSphere. A maioria dos comandos VVols, como criação, clonagem e edição do VVol, são iniciados por um host vCenter Server ou ESXi e traduzidos pelo provedor VASA para APIs do Element para o sistema de storage do software Element. Comandos para criar, excluir e gerenciar contentores de armazenamento e excluir volumes virtuais podem ser iniciados usando a IU do Element.

A maioria das configurações necessárias para o uso dos recursos do Virtual volumes com os sistemas de storage do software Element é feita no vSphere. Consulte o *Guia de configuração do VMware vSphere Virtual volumes for SolidFire Storage* para Registrar o provedor VASA no vCenter, criar e gerenciar datastores VVol e gerenciar o storage com base em políticas.



Não registre mais de um provedor NetApp Element VASA em uma única instância do vCenter. Quando um segundo provedor NetApp Element VASA é adicionado, isso torna todos os armazenamentos de dados VVOL inacessíveis.



O suporte DO VASA para vários vCenters está disponível como um patch de atualização se você já registrou um provedor VASA no vCenter. Para instalar, baixe o arquivo VASA39 .tar.gz do "[Transferências de software da NetApp](#)" site e siga as instruções no manifesto. O fornecedor NetApp Element VASA utiliza um certificado NetApp. Com esse patch, o certificado é usado não modificado pelo vCenter para oferecer suporte a vários vCenters para uso em VASA e VVols. Não modifique o certificado. Certificados SSL personalizados não são suportados pela VASA.

Encontre mais informações

- [Ativar volumes virtuais](#)
- [Ver detalhes do volume virtual](#)
- [Eliminar um volume virtual](#)
- [Crie um recipiente de armazenamento](#)
- [Edite um recipiente de armazenamento](#)
- [Excluir um recipiente de armazenamento](#)
- [Endpoints do protocolo](#)
- [Ligações](#)
- [Detalhes do host](#)

Ativar volumes virtuais

Você deve habilitar manualmente a funcionalidade volumes virtuais do vSphere (vols) por meio do software NetApp Element. O sistema de software Element vem com a funcionalidade vols desativada por padrão e não é automaticamente ativada como parte de uma nova instalação ou atualização. Ativar o recurso Vols é uma tarefa de configuração única.

O que você vai precisar

- O cluster deve estar executando o elemento 9,0 ou posterior.
- O cluster deve estar conectado a um ambiente ESXi 6,0 ou posterior compatível com o Vols.
- Se você estiver usando o elemento 11,3 ou posterior, o cluster deve estar conectado a um ambiente ESXi 6,0 atualização 3 ou posterior.



A ativação da funcionalidade vSphere Virtual volumes altera permanentemente a configuração do software Element. Você só deve habilitar a funcionalidade vols se o cluster estiver conectado a um ambiente compatível com VMware ESXi Vols. Você pode desativar o recurso Vols e restaurar as configurações padrão somente retornando o cluster à imagem de fábrica, que exclui todos os dados do sistema.

Passos

1. Selecione **clusters > Configurações**.
2. Localize as configurações específicas do cluster para volumes virtuais.
3. Clique em **Ativar volumes virtuais**.
4. Clique em **Sim** para confirmar a alteração de configuração de volumes virtuais.

A guia **Vols** aparece na IU do elemento.



Quando a funcionalidade do VVols está ativada, o cluster do SolidFire inicia o provedor VASA, abre a porta 8444 para tráfego VASA e cria pontos de extremidade de protocolo que podem ser descobertos pelo vCenter e por todos os hosts ESXi.

5. Copie o URL do provedor VASA a partir das configurações de volumes virtuais (VVols) em **clusters > Configurações**. Você usará este URL para Registrar o provedor VASA no vCenter.
6. Crie um contentor de armazenamento em **Vols > Storage Containers**.



Você precisa criar pelo menos um contêiner de storage para que as VMs possam ser provisionadas para um armazenamento de dados da VVol.

7. Selecione **Vols > Protocol Endpoints**.
8. Verifique se foi criado um ponto final de protocolo para cada nó no cluster.



Tarefas de configuração adicionais são necessárias no vSphere. Consulte o *Guia de configuração do VMware vSphere Virtual volumes for SolidFire Storage* para Registrar o provedor VASA no vCenter, criar e gerenciar datastores VVol e gerenciar o storage com base em políticas.

Encontre mais informações

["Guia de configuração do VMware vSphere Virtual volumes for SolidFire Storage"](#)

Ver detalhes do volume virtual

Você pode revisar as informações de volume virtual de todos os volumes virtuais ativos no cluster na IU do Element. Você também pode visualizar a atividade de desempenho de cada volume virtual, incluindo informações de entrada, saída, taxa de transferência, latência, profundidade da fila e volume.

O que você vai precisar

- Você deve ter habilitado a funcionalidade vols na IU do Element para o cluster.
- Você deve ter criado um contêiner de storage associado.
- Você deve ter configurado o cluster do vSphere para usar a funcionalidade do software Element Vols.
- Você deve ter criado pelo menos uma VM no vSphere.

Passos

1. Clique em **Vols > volumes virtuais**.

É apresentada a informação de todos os volumes virtuais ativos.

2. Clique no ícone **ações** para o volume virtual que você deseja revisar.
3. No menu resultante, selecione **Exibir detalhes**.

Detalhes

A página volumes virtuais da guia Vols fornece informações sobre cada volume virtual ativo no cluster, como ID do volume, ID do snapshot, ID do volume virtual pai e ID de volume virtual virtual.

- **ID do volume:** O ID do volume subjacente.
- **Snapshot ID:** O ID do instantâneo do volume subjacente. O valor é 0 se o volume virtual não representar um instantâneo SolidFire.
- **ID de volume virtual principal:** A ID de volume virtual do volume virtual pai. Se o ID for todos zeros, o volume virtual é independente sem nenhum link para um pai.
- **ID de volume Virtual:** O UUID do volume virtual.
- **Nome:** O nome atribuído ao volume virtual.
- *** Recipiente de armazenamento*:** O recipiente de armazenamento que possui o volume virtual.
- **Guest os Type:** Sistema operacional associado ao volume virtual.
- **Virtual volume Type:** O tipo de volume virtual: Config, dados, memória, troca ou outro.
- **Access:** As permissões de leitura e gravação atribuídas ao volume virtual.
- *** Tamanho*:** O tamanho do volume virtual em GB ou GiB.
- **Snapshots:** O número de snapshots associados. Clique no número para ligar aos detalhes do instantâneo.
- **Min IOPS:** A configuração mínima de QoS de IOPS do volume virtual.
- **IOPS máximo:** A configuração de QoS de IOPS máximo do volume virtual.

- **IOPS de explosão:** A configuração máxima de QoS de explosão do volume virtual.
- **VMW_VmID:** As informações nos campos anteriores a "VMW_" são definidas pela VMware.
- **Criar tempo:** A hora em que a tarefa de criação de volume virtual foi concluída.

Detalhes individuais do volume virtual

A página volumes virtuais na guia Vols fornece as seguintes informações de volume virtual quando você seleciona um volume virtual individual e exibe seus detalhes.

- **VMW_XXX:** As informações nos campos anteriores ao "VMW_" são definidas pela VMware.
- **ID de volume virtual principal:** A ID de volume virtual do volume virtual pai. Se o ID for todos zeros, o volume virtual é independente sem nenhum link para um pai.
- **ID de volume Virtual:** O UUID do volume virtual.
- **Virtual volume Type:** O tipo de volume virtual: Config, dados, memória, troca ou outro.
- **ID do volume:** O ID do volume subjacente.
- **Access:** As permissões de leitura e gravação atribuídas ao volume virtual.
- **Nome da conta:** Nome da conta que contém o volume.
- **Grupos de acesso:** Grupos de acesso de volume associados.
- **Tamanho total do volume:** Capacidade total provisionada em bytes.
- *** Blocos não-Zero*:** Número total de 4KiB blocos com dados após a última operação de coleta de lixo ter sido concluída.
- *** Zero Blocks*:** Número total de 4KiB blocos sem dados após a última rodada de operação de coleta de lixo ter sido concluída.
- **Snapshots:** O número de snapshots associados. Clique no número para ligar aos detalhes do instantâneo.
- **Min IOPS:** A configuração mínima de QoS de IOPS do volume virtual.
- **IOPS máximo:** A configuração de QoS de IOPS máximo do volume virtual.
- **IOPS de explosão:** A configuração máxima de QoS de explosão do volume virtual.
- **Enable 512:** Como os volumes virtuais sempre usam emulação de tamanho de bloco de 512 bytes, o valor é sempre sim.
- **Volumes emparelhados:** Indica se um volume está emparelhado.
- **Criar tempo:** A hora em que a tarefa de criação de volume virtual foi concluída.
- **Tamanho dos blocos:** Tamanho dos blocos no volume.
- *** Gravações desalinhadas*:** Para 512e volumes, o número de operações de gravação que não estavam em um limite de setor 4K. Números altos de gravações desalinhadas podem indicar alinhamento inadequado da partição.
- **Leituras desalinhadas:** Para 512e volumes, o número de operações de leitura que não estavam em um limite de setor 4K. Números altos de leituras desalinhadas podem indicar alinhamento inadequado da partição.
- **ScsiEUIDeviceID:** Identificador de dispositivo SCSI exclusivo globalmente para o volume em formato de 16 bytes baseado em EUI-64.
- **ScsiNAADeviceID:** Identificador de dispositivo SCSI exclusivo globalmente para o volume no formato estendido registrado IEEE NAA.

- * Atributos*: Lista de pares nome-valor no formato de objeto JSON.

Eliminar um volume virtual

Embora os volumes virtuais sempre devam ser excluídos da camada de gerenciamento do VMware, a funcionalidade para você excluir volumes virtuais é habilitada da IU do Element. Você só deve excluir um volume virtual da IU do Element quando for absolutamente necessário, como quando o vSphere não consegue limpar volumes virtuais no storage do SolidFire.

1. Selecione **Vols > volumes virtuais**.
2. Clique no ícone ações do volume virtual que você deseja excluir.
3. No menu resultante, selecione **Excluir**.



Você deve excluir um volume virtual da camada de gerenciamento do VMware para garantir que o volume virtual esteja devidamente desvinculado antes da exclusão. Você só deve excluir um volume virtual da IU do Element quando for absolutamente necessário, como quando o vSphere não consegue limpar volumes virtuais no storage do SolidFire. Se você excluir um volume virtual da IU do elemento, o volume será removido imediatamente.

4. Confirme a ação.
5. Atualize a lista de volumes virtuais para confirmar que o volume virtual foi removido.
6. **Opcional:** Selecione **Reporting > Event Log** para confirmar que a purga foi bem-sucedida.

Gerenciar contêineres de storage

Um contêiner de storage é uma representação do vSphere datastore criada em um cluster executando o software Element.

Os contêineres de storage são criados e vinculados às contas do NetApp Element. Um contêiner de armazenamento criado no Element Storage aparece como um datastore vSphere no vCenter e ESXi. Os contêineres de storage não alocam espaço no storage do Element. Eles são simplesmente usados para associar logicamente volumes virtuais.

Suporte para um máximo de quatro contêineres de storage por cluster. É necessário um mínimo de um contêiner de storage para habilitar o recurso Vols.

Crie um recipiente de armazenamento

Você pode criar contêineres de storage na IU do Element e descobri-los no vCenter. Você precisa criar pelo menos um contêiner de storage para começar a provisionar máquinas virtuais com suporte da VVol.

Antes de começar, ative a funcionalidade vols na IU do Element para o cluster.

Passos

1. Selecione **vols > Storage Containers**.
2. Clique no botão **Create Storage Containers**.
3. Insira as informações do recipiente de armazenamento na caixa de diálogo **criar um novo recipiente de armazenamento**:

- a. Introduza um nome para o recipiente de armazenamento.
- b. Configure os segredos do iniciador e do alvo para o CHAP.



Deixe os campos Configurações do CHAP em branco para gerar segredos automaticamente.

- c. Clique no botão **Create Storage Container** (criar contentor de armazenamento).
4. Verifique se o novo contentor de armazenamento aparece na lista na subguia **Containers de armazenamento**.



Como um ID de conta do NetApp Element é criado automaticamente e atribuído ao contentor de armazenamento, não é necessário criar uma conta manualmente.

Veja os detalhes do recipiente de armazenamento

Na página recipientes de armazenamento da guia Vols, você pode exibir informações de todos os contentores de armazenamento ativos no cluster.

- **ID da conta:** O ID da conta NetApp Element associada ao contentor de armazenamento.
- **Nome:** O nome do recipiente de armazenamento.
- **Status:** O status do recipiente de armazenamento. Valores possíveis:
 - Ativo: O recipiente de armazenamento está em uso.
 - Bloqueado: O recipiente de armazenamento está bloqueado.
- **Tipo PE:** O tipo de ponto de extremidade do protocolo (SCSI é o único protocolo disponível para o software Element).
- **Storage Container ID:** O UUID do contentor de armazenamento de volume virtual.
- **Volumes virtuais ativos:** O número de volumes virtuais ativos associados ao contentor de armazenamento.

Ver detalhes individuais do recipiente de armazenamento

Você pode exibir as informações do contentor de armazenamento de um contentor de armazenamento individual selecionando-as na página recipientes de armazenamento na guia vols.

- **ID da conta:** O ID da conta NetApp Element associada ao contentor de armazenamento.
- **Nome:** O nome do recipiente de armazenamento.
- **Status:** O status do recipiente de armazenamento. Valores possíveis:
 - Ativo: O recipiente de armazenamento está em uso.
 - Bloqueado: O recipiente de armazenamento está bloqueado.
- **Segredo do Iniciador CHAP:** O segredo exclusivo do CHAP para o iniciador.
- **Segredo alvo CHAP:** O segredo exclusivo CHAP para o alvo.
- **Storage Container ID:** O UUID do contentor de armazenamento de volume virtual.
- **Protocol Endpoint Type:** Indica o tipo de ponto de extremidade do protocolo (SCSI é o único protocolo disponível).

Edite um recipiente de armazenamento

Você pode modificar a autenticação CHAP do contentor de armazenamento na IU do Element.

1. Selecione **vols > Storage Containers**.
2. Clique no ícone **ações** do contentor de armazenamento que deseja editar.
3. No menu resultante, selecione **Editar**.
4. Em Configurações CHAP, edite as credenciais segredo do Iniciador e segredo de destino usadas para autenticação.



Se você não alterar as credenciais das Configurações CHAP, elas permanecerão as mesmas. Se você deixar os campos de credenciais em branco, o sistema gera automaticamente novos segredos.

5. Clique em **Salvar alterações**.

Excluir um recipiente de armazenamento

Você pode excluir contentores de armazenamento da IU do Element.

O que você vai precisar

Certifique-se de que todas as máquinas virtuais foram removidas do armazenamento de dados VVol.

Passos

1. Selecione **vols > Storage Containers**.
2. Clique no ícone **ações** do contentor de armazenamento que deseja excluir.
3. No menu resultante, selecione **Excluir**.
4. Confirme a ação.
5. Atualize a lista de contentores de armazenamento na subguia **Contentores de armazenamento** para confirmar que o contentor de armazenamento foi removido.

Endpoints do protocolo

Os endpoints de protocolo são pontos de acesso usados por um host para tratar do storage em um cluster que executa o software NetApp Element. Os endpoints de protocolo não podem ser excluídos ou modificados por um usuário, não estão associados a uma conta e não podem ser adicionados a um grupo de acesso de volume.

Um cluster que executa o software Element cria automaticamente um ponto de extremidade de protocolo por nó de storage no cluster. Por exemplo, um cluster de armazenamento de seis nós tem seis pontos finais de protocolo mapeados para cada host ESXi. Os pontos de extremidade do protocolo são gerenciados dinamicamente pelo software Element e são criados, movidos ou removidos conforme necessário sem qualquer intervenção. Os endpoints de protocolo são o destino para vários pathing e atuam como um proxy de e/S para LUNs subsidiários. Cada ponto de extremidade do protocolo consome um endereço SCSI disponível, tal como um destino iSCSI padrão. Os endpoints de protocolo aparecem como um dispositivo de armazenamento de bloco único (512 bytes) no cliente vSphere, mas este dispositivo de armazenamento não está disponível para ser formatado ou usado como armazenamento.

iSCSI é o único protocolo suportado. O protocolo Fibre Channel não é suportado.

Detalhes dos pontos de extremidade do protocolo

A página Protocol Endpoints (pontos de extremidade do protocolo) no separador VVols (Vols) fornece informações sobre o ponto de extremidade do protocolo.

- **ID principal do fornecedor**

A ID do provedor de endpoint de protocolo primário.

- **ID do fornecedor secundário**

A ID do provedor de endpoint de protocolo secundário.

- **ID do ponto final do protocolo**

O UUID do endpoint do protocolo.

- **Estado de ponto final do protocolo**

O estado do ponto de extremidade do protocolo. Os valores possíveis são os seguintes:

- Ativo: O ponto final do protocolo está em uso.
- Start (Iniciar): O ponto final do protocolo está a ser iniciado.
- Failover: O ponto final do protocolo falhou.
- Reservado: O ponto final do protocolo é reservado.

- **Tipo de fornecedor**

O tipo do provedor do ponto de extremidade do protocolo. Os valores possíveis são os seguintes:

- Primário
- Secundário

- *** SCSI NAA DEVICE ID***

O identificador de dispositivo SCSI exclusivo globalmente para o ponto de extremidade do protocolo no formato estendido registrado IEEE NAA.

Ligações

Para executar operações de e/S com um volume virtual, um host ESXi deve primeiro vincular o volume virtual.

O cluster do SolidFire escolhe um ponto de extremidade de protocolo ideal, cria uma ligação que associa o host ESXi e o volume virtual ao ponto de extremidade do protocolo e retorna a ligação ao host ESXi. Depois que estiver vinculado, o host ESXi pode executar operações de e/S com o volume virtual vinculado.

Detalhes das ligações

A página Bindings na guia Vols fornece informações de vinculação sobre cada volume virtual.

São apresentadas as seguintes informações:

- **ID do anfitrião**

O UUID para o host ESXi que hospeda volumes virtuais e é conhecido pelo cluster.

- **ID do ponto final do protocolo**

IDs de endpoint de protocolo que correspondem a cada nó no cluster SolidFire.

- **Ponto final do protocolo no ID da banda**

A ID do dispositivo SCSI NAA do ponto de extremidade do protocolo.

- **Tipo de ponto final do protocolo**

O tipo de ponto final do protocolo.

- **VVol Binding ID**

O UUID de vinculação do volume virtual.

- **VVol ID**

O identificador universal único (UUID) do volume virtual.

- **ID secundária VVol**

O ID secundário do volume virtual que é um ID LUN de segundo nível SCSI.

Detalhes do host

A página hosts na guia Vols fornece informações sobre os hosts do VMware ESXi que hospedam volumes virtuais.

São apresentadas as seguintes informações:

- **ID do anfitrião**

O UUID para o host ESXi que hospeda volumes virtuais e é conhecido pelo cluster.

- **Endereço do anfitrião**

O endereço IP ou o nome DNS do host ESXi.

- **Ligações**

IDs de vinculação para todos os volumes virtuais vinculados pelo host ESXi.

- **ID do cluster ESX**

O ID do cluster de host vSphere ou o vCenter GUID.

- **Iniciador IQNs**

IQNs do iniciador para o host de volume virtual.

- **IDs de endpoints do protocolo SolidFire**

Os endpoints do protocolo que estão atualmente visíveis para o host ESXi.

Trabalhar com grupos de acesso de volume e iniciadores

Pode utilizar iniciadores iSCSI ou iniciadores Fibre Channel para acessar aos volumes definidos nos grupos de acesso de volume.

É possível criar grupos de acesso mapeando IQNs do iniciador iSCSI ou WWPNs Fibre Channel em uma coleção de volumes. Cada IQN que você adicionar a um grupo de acesso pode acessar cada volume no grupo sem exigir autenticação CHAP.

Existem dois tipos de métodos de autenticação CHAP:

- Autenticação CHAP em nível de conta: Você pode atribuir autenticação CHAP para a conta.
- Autenticação CHAP no nível do iniciador: Você pode atribuir um alvo CHAP exclusivo e segredos para iniciadores específicos sem estar vinculado a um único CHAP em uma única conta. Esta autenticação CHAP no nível do iniciador substitui credenciais no nível da conta.

Opcionalmente, com o CHAP por iniciador, você pode aplicar a autorização do iniciador e a autenticação CHAP por iniciador. Essas opções podem ser definidas por iniciador e um grupo de acesso pode conter uma combinação de iniciadores com diferentes opções.

Cada WWPN que você adicionar a um grupo de acesso permite o acesso à rede Fibre Channel aos volumes no grupo de acesso.



Os grupos de acesso ao volume têm os seguintes limites:

- Um máximo de 64 IQNs ou WWPNs são permitidos em um grupo de acesso.
- Um grupo de acesso pode ser composto por um máximo de 2000 volumes.
- Um IQN ou WWPN só pode pertencer a um grupo de acesso.
- Um único volume pode pertencer a um máximo de quatro grupos de acesso.

Encontre mais informações

- [Crie um grupo de acesso ao volume](#)
- [Adicionar volumes a um grupo de acesso](#)
- [Remover volumes de um grupo de acesso](#)
- [Crie um iniciador](#)
- [Edite um iniciador](#)
- [Adicione um único iniciador a um grupo de acesso ao volume](#)
- [Adicione vários iniciadores a um grupo de acesso de volume](#)
- [Remover iniciadores de um grupo de acesso](#)
- [Eliminar um grupo de acesso](#)
- [Eliminar um iniciador](#)


Crie um grupo de acesso ao volume


Você pode criar grupos de acesso de volume mapeando iniciadores para uma coleção de volumes para acesso seguro. Em seguida, você pode conceder acesso aos volumes no grupo com um segredo iniciador CHAP de conta e segredo de destino.

Se você usar CHAP baseado em iniciador, poderá adicionar credenciais CHAP para um único iniciador em um grupo de acesso de volume, fornecendo mais segurança. Isso permite que você aplique essa opção para grupos de acesso de volume que já existem.

Passos

1. Clique em **Gerenciamento > grupos de acesso**.
2. Clique em **Create Access Group**.
3. Digite um nome para o grupo de acesso ao volume no campo **Nome**.
4. Adicione um iniciador ao grupo de acesso ao volume de uma das seguintes maneiras:

| Opção | Descrição |
|--|--|
| Adicionando um iniciador Fibre Channel | <p>a. Em Adicionar iniciadores, selecione um iniciador Fibre Channel existente na lista iniciadores de Fibre Channel não vinculados.</p> <p>b. Clique em Add FC Initiator.</p> <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"><p> Você pode criar um iniciador durante esta etapa se clicar no link Create Initiator, inserir um nome de iniciador e clicar em Create. O sistema adiciona automaticamente o iniciador à lista de iniciadores depois de criá-lo.</p></div> <p>Uma amostra do formato é a seguinte:</p> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0; background-color: #f0f0f0;"><code>5f:47:ac:c0:5c:74:d4:02</code></div> |

| Opção | Descrição |
|------------------------------|--|
| Adicionar um iniciador iSCSI | <p>Em Adicionar iniciadores, selecione um iniciador existente na lista de iniciadores. Observação: você pode criar um iniciador durante esta etapa se clicar no link criar Iniciador, inserir um nome de iniciador e clicar em criar. O sistema adiciona automaticamente o iniciador à lista de iniciadores depois de criá-lo.</p> <p>Uma amostra do formato é a seguinte:</p> <pre>iqn.2010-01.com.solidfire:c2r9.fc0.2100000e1e09bb8b</pre> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;">  <p>Você pode encontrar o iniciador IQN para cada volume selecionando Exibir detalhes no menu ações para o volume na lista Gerenciamento > volumes > Ativo.</p> </div> <p>Quando você modifica um iniciador, você pode alternar o atributo requidCHAP para true, o que permite definir o segredo do iniciador de destino. Para obter detalhes, consulte informações de API sobre o método API ModifyInitiator.</p> <p>"Gerencie o storage com a API Element"</p> |

5. **Opcional:** Adicione mais iniciadores conforme necessário.
6. Em Adicionar volumes, selecione um volume na lista **volumes**.

O volume aparece na lista **volumes anexados**.
7. **Opcional:** Adicione mais volumes conforme necessário.
8. Clique em **Create Access Group**.

Encontre mais informações

[Adicionar volumes a um grupo de acesso](#)

Ver detalhes do grupo de acesso individual

Você pode exibir detalhes de um grupo de acesso individual, como volumes anexados e iniciadores, em um formato gráfico.

1. Clique em **Gerenciamento > grupos de acesso**.
2. Clique no ícone ações de um grupo de acesso.
3. Clique em **Ver detalhes**.

Detalhes do grupo de acesso ao volume

A página grupos de acesso na guia Gerenciamento fornece informações sobre grupos de acesso de volume.

São apresentadas as seguintes informações:

- **ID:** O ID gerado pelo sistema para o grupo de acesso.
- **Nome:** O nome dado ao grupo Access quando ele foi criado.
- **Volumes ativos:** O número de volumes ativos no grupo Access.
- **Compression:** A pontuação de eficiência de compressão para o grupo Access.
- **Desduplicação:** A pontuação de eficiência de desduplicação para o grupo de acesso.
- **Provisionamento fino:** A pontuação de eficiência de provisionamento fino para o grupo de acesso.
- **Eficiência geral:** A pontuação geral de eficiência para o grupo de acesso.
- **Iniciadores:** O número de iniciadores conectados ao grupo Access.

Adicionar volumes a um grupo de acesso

Você pode adicionar volumes a um grupo de acesso de volume. Cada volume pode pertencer a mais de um grupo de acesso de volume; você pode ver os grupos aos quais cada volume pertence na página **volumes ativos**.

Você também pode usar este procedimento para adicionar volumes a um grupo de acesso ao volume Fibre Channel.

1. Clique em **Gerenciamento > grupos de acesso**.
2. Clique no ícone ações do grupo de acesso ao qual deseja adicionar volumes.
3. Clique no botão **Editar**.
4. Em Adicionar volumes, selecione um volume na lista **volumes**.

Você pode adicionar mais volumes repetindo esta etapa.

5. Clique em **Salvar alterações**.

Remover volumes de um grupo de acesso

Quando você remove um volume de um grupo de acesso, o grupo não tem mais acesso a esse volume.

Modificar as configurações CHAP em uma conta ou remover iniciadores ou volumes de um grupo de acesso pode fazer com que os iniciadores percam o acesso aos volumes inesperadamente. Para verificar se o acesso ao volume não será perdido inesperadamente, saia sempre das sessões iSCSI que serão afetadas por uma alteração de conta ou grupo de acesso e verifique se os iniciadores podem se reconectar aos volumes depois que quaisquer alterações nas configurações do iniciador e nas configurações do cluster tiverem sido concluídas.

1. Clique em **Gerenciamento > grupos de acesso**.
2. Clique no ícone ações do grupo de acesso do qual deseja remover volumes.
3. Clique em **Editar**.
4. Em Adicionar volumes na caixa de diálogo **Edit volume Access Group** (Editar grupo de acesso ao volume*), clique na seta na lista **Attached volumes** (volumes anexados).
5. Selecione o volume que deseja remover da lista e clique no ícone **x** para remover o volume da lista.

Você pode remover mais volumes repetindo esta etapa.

6. Clique em **Salvar alterações**.

Crie um iniciador

Você pode criar iniciadores iSCSI ou Fibre Channel e, opcionalmente, atribuí-los aliases.

Você também pode atribuir atributos CHAP baseados em iniciador usando uma chamada de API. Para adicionar um nome de conta CHAP e credenciais por iniciador, você deve usar a `CreateInitiator` chamada API para remover e adicionar acesso CHAP e atributos. O acesso do iniciador pode ser restrito a uma ou mais VLANs especificando um ou mais `virtualNetworkIDs` por meio das `CreateInitiators` chamadas da API e `ModifyInitiators`. Se nenhuma rede virtual for especificada, o iniciador poderá acessar todas as redes.

Para obter detalhes, consulte as informações de referência da API. "[Gerencie o storage com a API Element](#)"

Passos

1. Clique em **Management > Initiators**.
2. Clique em **Create Initiator**.
3. Execute as etapas para criar um único iniciador ou vários iniciadores:

| Opção | Passos |
|-------------------------|--|
| Crie um único iniciador | <ol style="list-style-type: none">a. Clique em criar um único Iniciador.b. Introduza o IQN ou WWPN para o iniciador no campo IQN/WWPN.c. Digite um nome amigável para o iniciador no campo Alias.d. Clique em Create Initiator. |
| Crie vários iniciadores | <ol style="list-style-type: none">a. Clique em Bulk Create Initiators.b. Insira uma lista de IQNs ou WWPNs na caixa de texto.c. Clique em Adicionar iniciadores.d. Escolha um iniciador da lista resultante e clique no ícone Adicionar correspondente na coluna Alias para adicionar um alias para o iniciador.e. Clique na marca de seleção para confirmar o novo alias.f. Clique em criar iniciadores. |

Edite um iniciador

Você pode alterar o alias de um iniciador existente ou adicionar um alias se um ainda não existir.

Para adicionar um nome de conta CHAP e credenciais por iniciador, você deve usar a `ModifyInitiator` chamada API para remover e adicionar acesso CHAP e atributos.

"[Gerencie o storage com a API Element](#)"Consulte .

Passos

1. Clique em **Management > Initiators**.

2. Clique no ícone ações do iniciador que deseja editar.
3. Clique em **Editar**.
4. Insira um novo alias para o iniciador no campo **Alias**.
5. Clique em **Salvar alterações**.

Adicione um único iniciador a um grupo de acesso ao volume

Você pode adicionar um iniciador a um grupo de acesso de volume existente.

Quando você adiciona um iniciador a um grupo de acesso de volume, o iniciador tem acesso a todos os volumes nesse grupo de acesso de volume.



Você pode encontrar o iniciador para cada volume clicando no ícone ações e selecionando **Exibir detalhes** para o volume na lista volumes ativos.

Se você usar CHAP baseado em iniciador, poderá adicionar credenciais CHAP para um único iniciador em um grupo de acesso de volume, fornecendo mais segurança. Isso permite que você aplique essa opção para grupos de acesso de volume que já existem.

Passos

1. Clique em **Gerenciamento > grupos de acesso**.
2. Clique no ícone **ações** para o grupo de acesso que deseja editar.
3. Clique em **Editar**.
4. Para adicionar um iniciador Fibre Channel ao grupo de acesso ao volume, execute as seguintes etapas:
 - a. Em Adicionar iniciadores, selecione um iniciador Fibre Channel existente na lista **iniciadores de Fibre Channel não vinculados**.
 - b. Clique em **Add FC Initiator**.



Você pode criar um iniciador durante esta etapa se clicar no link **Create Initiator**, inserir um nome de iniciador e clicar em **Create**. O sistema adiciona automaticamente o iniciador à lista **iniciadores** depois de criá-lo.

Uma amostra do formato é a seguinte:

```
5f:47:ac:c0:5c:74:d4:02
```

5. Para adicionar um iniciador iSCSI ao grupo de acesso ao volume, em Adicionar iniciadores, selecione um iniciador existente na lista **iniciadores**.



Você pode criar um iniciador durante esta etapa se clicar no link **Create Initiator**, inserir um nome de iniciador e clicar em **Create**. O sistema adiciona automaticamente o iniciador à lista **iniciadores** depois de criá-lo.

O formato aceito de um iniciador IQN é o seguinte: `iqn.yyyy-mm`, em que `y` e `m` são dígitos, seguido de texto que deve conter apenas dígitos, caracteres alfabéticos em letras minúsculas, um ponto (`.`), dois pontos (`:`) ou traço (`-`).

Uma amostra do formato é a seguinte:

```
iqn.2010-01.com.solidfire:c2r9.fc0.2100000e1e09bb8b
```



Você pode encontrar o iniciador IQN para cada volume na página **Management > volumes** ativos volumes clicando no ícone ações e selecionando **View Details** para o volume.

6. Clique em **Salvar alterações**.

Adicione vários iniciadores a um grupo de acesso de volume

Você pode adicionar vários iniciadores a um grupo de acesso de volume existente para permitir o acesso a volumes no grupo de acesso de volume com ou sem exigir autenticação CHAP.

Quando você adiciona iniciadores a um grupo de acesso de volume, os iniciadores têm acesso a todos os volumes nesse grupo de acesso de volume.



Você pode encontrar o iniciador para cada volume clicando no ícone ações e em **Exibir detalhes** para o volume na lista volumes ativos.

Você pode adicionar vários iniciadores a um grupo de acesso de volume existente para habilitar o acesso a volumes e atribuir credenciais CHAP exclusivas para cada iniciador dentro desse grupo de acesso de volume. Isso permite que você aplique essa opção para grupos de acesso de volume que já existem.

Você pode atribuir atributos CHAP baseados em iniciador usando uma chamada de API. Para adicionar um nome de conta CHAP e credenciais por iniciador, você deve usar a chamada API `ModifyInitiator` para remover e adicionar acesso e atributos CHAP.

Para obter detalhes, "[Gerencie o storage com a API Element](#)" consulte .

Passos

1. Clique em **Management > Initiators**.
2. Selecione os iniciadores que pretende adicionar a um grupo de acesso.
3. Clique no botão **ações em massa**.
4. Clique em **Add to volume Access Group**.
5. Na caixa de diálogo Adicionar ao Grupo de Acesso por volume, selecione um grupo de acesso na lista **Grupo de Acesso por volume**.
6. Clique em **Add**.

Remover iniciadores de um grupo de acesso

Quando você remove um iniciador de um grupo de acesso, ele não pode mais acessar os volumes nesse grupo de acesso de volume. O acesso normal à conta ao volume não é interrompido.

Modificar as configurações CHAP em uma conta ou remover iniciadores ou volumes de um grupo de acesso pode fazer com que os iniciadores percam o acesso aos volumes inesperadamente. Para verificar se o acesso

ao volume não será perdido inesperadamente, saia sempre das sessões iSCSI que serão afetadas por uma alteração de conta ou grupo de acesso e verifique se os iniciadores podem se reconectar aos volumes depois que quaisquer alterações nas configurações do iniciador e nas configurações do cluster tiverem sido concluídas.

Passos

1. Clique em **Gerenciamento > grupos de acesso**.
2. Clique no ícone **ações** do grupo de acesso que deseja remover.
3. No menu resultante, selecione **Editar**.
4. Em Adicionar iniciadores na caixa de diálogo **Editar Grupo de Acesso por volume**, clique na seta na lista **iniciadores**.
5. Selecione o ícone x para cada iniciador que deseja remover do grupo de acesso.
6. Clique em **Salvar alterações**.

Eliminar um grupo de acesso

Você pode excluir um grupo de acesso quando ele não for mais necessário. Não é necessário excluir IDs de Iniciador e IDs de volume do grupo de acesso de volume antes de excluir o grupo. Depois de eliminar o grupo de acesso, o acesso do grupo aos volumes é descontinuado.

1. Clique em **Gerenciamento > grupos de acesso**.
2. Clique no ícone **ações** do grupo de acesso que deseja excluir.
3. No menu resultante, clique em **Excluir**.
4. Para excluir também os iniciadores associados a esse grupo de acesso, marque a caixa de seleção **Excluir iniciadores neste grupo de acesso**.
5. Confirme a ação.

Eliminar um iniciador

Você pode excluir um iniciador depois que ele não for mais necessário. Quando você exclui um iniciador, o sistema o remove de qualquer grupo de acesso de volume associado. Quaisquer conexões usando o iniciador permanecem válidas até que a conexão seja redefinida.

Passos

1. Clique em **Management > Initiators**.
2. Execute as etapas para excluir um único iniciador ou vários iniciadores:

| Opção | Passos |
|-----------------------------|---|
| Eliminar um único iniciador | <ol style="list-style-type: none">a. Clique no ícone ações do iniciador que deseja excluir.b. Clique em Excluir.c. Confirme a ação. |

| Opção | Passos |
|-----------------------------|--|
| Eliminar vários iniciadores | <ol style="list-style-type: none"> Marque as caixas de seleção ao lado dos iniciadores que deseja excluir. Clique no botão ações em massa. No menu resultante, selecione Excluir. Confirme a ação. |

Proteja seus dados

O software NetApp Element permite proteger seus dados de várias maneiras com funcionalidades como snapshots para volumes individuais ou grupos de volumes, replicação entre clusters e volumes executados no Element e replicação para sistemas ONTAP.

- **Instantâneos**

A proteção de dados somente snapshot replica os dados alterados em momentos específicos para um cluster remoto. Somente os snapshots criados no cluster de origem são replicados. As gravações ativas do volume de origem não são.

[Use snapshots de volume para proteção de dados](#)

- **Replicação remota entre clusters e volumes em execução no Element**

Você pode replicar dados de volume de forma síncrona ou assíncrona de qualquer cluster em um par de cluster executado no Element para cenários de failover e failback.

[Executar replicação remota entre clusters que executam o software NetApp Element](#)

- **Replicação entre clusters Element e ONTAP usando a tecnologia SnapMirror**

Com a tecnologia NetApp SnapMirror, é possível replicar snapshots que foram obtidos usando o Element para o ONTAP para fins de recuperação de desastres. Em uma relação SnapMirror, Element é um endpoint e ONTAP é o outro.

[Use a replicação do SnapMirror entre clusters Element e ONTAP](#)

- * Faça backup e restaure volumes de lojas de objetos SolidFire, S3 ou Swift*

Você pode fazer backup e restaurar volumes para outro storage SolidFire, bem como armazenamentos de objetos secundários que são compatíveis com Amazon S3 ou OpenStack Swift.

[Faça backup e restaure volumes para armazenamentos de objetos SolidFire, S3 ou Swift](#)

Para mais informações

- ["Documentação do software SolidFire e Element"](#)
- ["Plug-in do NetApp Element para vCenter Server"](#)

Use snapshots de volume para proteção de dados

Um instantâneo de volume é uma cópia pontual de um volume. Você pode tirar um instantâneo de um volume e usar o instantâneo mais tarde se precisar rolar um volume de volta para o estado em que ele estava no momento em que o snapshot foi criado.

Os snapshots são semelhantes aos clones de volume. No entanto, os instantâneos são simplesmente réplicas de metadados de volume, para que você não possa montar ou gravar neles. A criação de um snapshot de volume também exige apenas uma pequena quantidade de recursos e espaço do sistema, o que torna a criação de snapshot mais rápida do que a clonagem.

Você pode tirar um instantâneo de um volume individual ou de um conjunto de volumes.

Opcionalmente, replique snapshots para um cluster remoto e use-os como uma cópia de backup do volume. Isso permite reverter um volume para um ponto específico no tempo usando o instantâneo replicado. Como alternativa, você pode criar um clone de um volume a partir de um snapshot replicado.

Encontre mais informações

- [Use snapshots de volume individuais para proteção de dados](#)
- [Uso de snapshots de grupo para tarefa de proteção de dados](#)
- [Agendar um instantâneo](#)

Use snapshots de volume individuais para proteção de dados

Um instantâneo de volume é uma cópia pontual de um volume. Você pode usar um volume individual em vez de um grupo de volumes para o snapshot.

Encontre mais informações

- [Criar um instantâneo de volume](#)
- [Editar retenção de instantâneos](#)
- [Eliminar um instantâneo](#)
- [Clonar um volume de um snapshot](#)
- [Reverter um volume para um instantâneo](#)
- [Fazer backup de um instantâneo de volume para um armazenamento de objetos do Amazon S3](#)
- [Fazer backup de um instantâneo de volume para um armazenamento de objetos OpenStack Swift](#)
- [Fazer backup de um instantâneo de volume para um cluster SolidFire](#)

Criar um instantâneo de volume

Você pode criar um instantâneo de um volume ativo para preservar a imagem do volume a qualquer momento. Você pode criar até 32 snapshots para um único volume.

1. Clique em **Management > volumes**.
2. Clique no ícone **ações** do volume que deseja usar para o instantâneo.
3. No menu resultante, selecione **Snapshot**.

4. Na caixa de diálogo **Create Snapshot of volume** (criar instantâneo de volume), insira o novo nome do instantâneo.
5. **Opcional:** Selecione a caixa de seleção **incluir instantâneo na replicação quando emparelhado** para garantir que o instantâneo seja capturado na replicação quando o volume pai estiver emparelhado.
6. Para definir a retenção para o instantâneo, selecione uma das seguintes opções:
 - Clique em **manter para sempre** para manter o instantâneo no sistema indefinidamente.
 - Clique em **Definir período de retenção** e use as caixas de rotação de data para escolher um período de tempo para o sistema reter o instantâneo.
7. Para fazer um instantâneo único e imediato, execute as seguintes etapas:
 - a. Clique em **Take Snapshot Now**.
 - b. Clique em **Create Snapshot** (criar instantâneo).
8. Para agendar a execução do instantâneo em um momento futuro, execute as seguintes etapas:
 - a. Clique em **criar agendamento instantâneo**.
 - b. Introduza um **novo nome do programa**.
 - c. Escolha um **tipo de agendamento** na lista.
 - d. **Opcional:** Selecione a caixa de seleção **Agendamento recorrente** para repetir o snapshot agendado periodicamente.
 - e. Clique em **Create Schedule**.

Encontre mais informações

[Agendar um instantâneo](#)

Editar retenção de instantâneos

Pode alterar o período de retenção de um instantâneo para controlar quando ou se o sistema eliminar instantâneos. O período de retenção especificado começa quando você insere o novo intervalo. Quando você define um período de retenção, pode selecionar um período que começa no momento atual (a retenção não é calculada a partir do tempo de criação do instantâneo). Você pode especificar intervalos em minutos, horas e dias.

Passos

1. Clique em **proteção de dados > instantâneos**.
2. Clique no ícone **ações** para o instantâneo que você deseja editar.
3. No menu resultante, clique em **Editar**.
4. **Opcional:** Selecione a caixa de seleção **incluir instantâneo na replicação quando emparelhado**** para garantir que o instantâneo seja capturado na replicação quando o volume pai estiver emparelhado.
5. **Opcional:** Selecione uma opção de retenção para o instantâneo:
 - Clique em **manter para sempre** para manter o instantâneo no sistema indefinidamente.
 - Clique em **Definir período de retenção** e use as caixas de rotação de data para selecionar um período de tempo para que o sistema retenha o instantâneo.
6. Clique em **Salvar alterações**.

Eliminar um instantâneo

Você pode excluir um snapshot de volume de um cluster de storage executando o software Element. Quando você exclui um instantâneo, o sistema o remove imediatamente.

Você pode excluir snapshots que estão sendo replicados do cluster de origem. Se um instantâneo estiver a sincronizar com o cluster de destino quando o eliminar, a replicação de sincronização é concluída e o instantâneo é eliminado do cluster de origem. O instantâneo não é eliminado do cluster de destino.

Você também pode excluir snapshots que foram replicados para o destino do cluster de destino. O instantâneo excluído é mantido em uma lista de instantâneos excluídos no destino até que o sistema detete que você excluiu o instantâneo no cluster de origem. Quando o destino deteta que você excluiu o instantâneo de origem, o destino interrompe a replicação do instantâneo.

Quando você exclui um snapshot do cluster de origem, o snapshot do cluster de destino não é afetado (o reverso também é verdadeiro).

1. Clique em **proteção de dados > instantâneos**.
2. Clique no ícone **ações** para o instantâneo que deseja excluir.
3. No menu resultante, selecione **Excluir**.
4. Confirme a ação.

Clone um volume de um snapshot

Você pode criar um novo volume a partir de um instantâneo de um volume. Quando você faz isso, o sistema usa as informações de snapshot para clonar um novo volume usando os dados contidos no volume no momento em que o snapshot foi criado. Este processo armazena informações sobre outros instantâneos do volume no volume recém-criado.

1. Clique em **proteção de dados > instantâneos**.
2. Clique no ícone **ações** para o instantâneo que você deseja usar para o clone de volume.
3. No menu resultante, clique em **Clone volume from Snapshot**.
4. Insira um **Nome do volume** na caixa de diálogo **Clone volume from Snapshot** (Clonar volume de instantâneo).
5. Selecione um **tamanho total** e unidades de tamanho para o novo volume.
6. Selecione um tipo **Access** para o volume.
7. Selecione uma **conta** na lista para associar ao novo volume.
8. Clique em **Iniciar clonagem**.

Reverter um volume para um instantâneo

Você pode reverter um volume para um instantâneo anterior a qualquer momento. Isso reverte todas as alterações feitas no volume desde que o snapshot foi criado.

Passos

1. Clique em **proteção de dados > instantâneos**.
2. Clique no ícone **ações** para o instantâneo que você deseja usar para a reversão de volume.

3. No menu resultante, selecione **Rollback volume to Snapshot**.
4. **Opcional:** para salvar o estado atual do volume antes de voltar para o instantâneo:
 - a. Na caixa de diálogo **Reverter para instantâneo**, selecione **Salvar o estado atual do volume como instantâneo**.
 - b. Introduza um nome para o novo instantâneo.
5. Clique em **Rollback Snapshot**.

Fazer backup de um instantâneo de volume

Você pode usar o recurso de backup integrado para fazer backup de um instantâneo de volume. É possível fazer backup de snapshots de um cluster do SolidFire para um armazenamento de objetos externo ou para outro cluster do SolidFire. Ao fazer backup de um snapshot em um armazenamento de objetos externo, você deve ter uma conexão com o armazenamento de objetos que permita operações de leitura/gravação.

- ["Faça backup de um snapshot de volume em um armazenamento de objetos do Amazon S3"](#)
- ["Fazer backup de um snapshot de volume para um armazenamento de objetos OpenStack Swift"](#)
- ["Fazer backup de um snapshot de volume em um cluster SolidFire"](#)

Faça backup de um snapshot de volume em um armazenamento de objetos do Amazon S3

Você pode fazer backup de snapshots do SolidFire em armazenamentos de objetos externos compatíveis com o Amazon S3.

1. Clique em **proteção de dados > instantâneos**.
2. Clique no ícone **ações** para o instantâneo que você deseja fazer backup.
3. No menu resultante, clique em **Backup to**.
4. Na caixa de diálogo **Backup integrado** em **Backup to**, selecione **S3**.
5. Selecione uma opção em **Data Format**:
 - *** Nativo***: Um formato compactado legível apenas pelos sistemas de armazenamento SolidFire.
 - **Uncompressed**: Um formato não comprimido compatível com outros sistemas.
6. Insira um nome de host para usar para acessar o armazenamento de objetos no campo **Nome de host**.
7. Insira um ID de chave de acesso para a conta no campo **ID de chave de acesso**.
8. Digite a chave de acesso secreta para a conta no campo **chave de acesso secreta**.
9. Introduza o bucket S3 no qual pretende guardar a cópia de segurança no campo **S3 Bucket**.
10. **Opcional:** Insira um nametag para anexar ao prefixo no campo **nametag**.
11. Clique em **Iniciar leitura**.

Fazer backup de um snapshot de volume para um armazenamento de objetos OpenStack Swift

Você pode fazer backup de snapshots do SolidFire para armazenamentos de objetos secundários que são compatíveis com o OpenStack Swift.

1. Clique em **proteção de dados > instantâneos**.

2. Clique no ícone **ações** para o instantâneo que você deseja fazer backup.
3. No menu resultante, clique em **Backup to**.
4. Na caixa de diálogo **Backup integrado**, em **Backup to**, selecione **Swift**.
5. Selecione uma opção em **Data Format**:
 - * Nativo*: Um formato compactado legível apenas pelos sistemas de armazenamento SolidFire.
 - **Uncompressed**: Um formato não comprimido compatível com outros sistemas.
6. Insira um **URL** para usar para acessar o armazenamento de objetos.
7. Digite um **Nome de usuário** para a conta.
8. Introduza a **chave de autenticação** para a conta.
9. Insira o **container** no qual deseja armazenar o backup.
10. **Opcional**: Insira um **nametag**.
11. Clique em **Iniciar leitura**.

Fazer backup de um snapshot de volume em um cluster SolidFire

É possível fazer backup de snapshots de volume que residem em um cluster SolidFire para um cluster SolidFire remoto.

Certifique-se de que os clusters de origem e destino estejam emparelhados.

Ao fazer backup ou restaurar de um cluster para outro, o sistema gera uma chave para ser usada como autenticação entre os clusters. Essa chave de gravação de volume em massa permite que o cluster de origem se autentique com o cluster de destino, fornecendo um nível de segurança ao gravar no volume de destino. Como parte do processo de backup ou restauração, você precisa gerar uma chave de gravação de volume em massa a partir do volume de destino antes de iniciar a operação.

1. No cluster de destino, clique em **Management > volumes**.
2. Clique no ícone **ações** para o volume de destino.
3. No menu resultante, clique em **Restaurar de**.
4. Na caixa de diálogo **Restauração integrada** em **Restaurar de**, selecione **SolidFire**.
5. Selecione um formato de dados em **Data Format**:
 - * Nativo*: Um formato compactado legível apenas pelos sistemas de armazenamento SolidFire.
 - **Uncompressed**: Um formato não comprimido compatível com outros sistemas.
6. Clique em **Generate Key**.
7. Copie a chave da caixa **Bulk volume Write Key** para a área de transferência.
8. No cluster de origem, clique em **proteção de dados > instantâneos**.
9. Clique no ícone **ações** do instantâneo que você deseja usar para o backup.
10. No menu resultante, clique em **Backup to**.
11. Na caixa de diálogo Backup integrado** em **Backup to**, selecione **SolidFire**.
12. Selecione o mesmo formato de dados selecionado anteriormente no campo **Data Format**.
13. Introduza o endereço IP virtual de gestão do cluster do volume de destino no campo **Remote Cluster MVIP**.

14. Introduza o nome de utilizador do cluster remoto no campo **Nome de utilizador do cluster remoto**.
15. Introduza a palavra-passe do cluster remoto no campo **Palavra-passe do cluster remoto**.
16. No campo **Bulk volume Write Key** (chave de gravação de volume em massa), cole a chave que você gerou no cluster de destino anteriormente.
17. Clique em **Iniciar leitura**.

Uso de snapshots de grupo para tarefa de proteção de dados

Você pode criar um snapshot de grupo de um conjunto relacionado de volumes para preservar uma cópia pontual dos metadados para cada volume. Você pode usar o snapshot de grupo no futuro como um backup ou reversão para restaurar o estado do grupo de volumes para um estado anterior.

Encontre mais informações

- [Criar um instantâneo de grupo](#)
- [Editar instantâneos de grupo](#)
- [Editar membros do instantâneo do grupo](#)
- [Eliminar um instantâneo de grupo](#)
- [Reverter volumes para um instantâneo de grupo](#)
- [Clonar vários volumes](#)
- [Clonar vários volumes de um snapshot de grupo](#)

Detalhes do instantâneo do grupo

A página instantâneos de grupo na guia proteção de dados fornece informações sobre os instantâneos de grupo.

- **ID**

A ID gerada pelo sistema para o instantâneo do grupo.

- **UUID**

A ID exclusiva do instantâneo do grupo.

- **Nome**

Nome definido pelo usuário para o instantâneo do grupo.

- **Criar tempo**

A hora em que o instantâneo do grupo foi criado.

- **Status**

O estado atual do instantâneo. Valores possíveis:

- **Preparação:** O instantâneo está sendo preparado para uso e ainda não é gravável.

- Feito: Este instantâneo terminou a preparação e agora é utilizável.
- Ativo: O instantâneo é o ramo ativo.
- * Número de volumes*

O número de volumes no grupo.

- **Reter até**

O dia e a hora em que o instantâneo será eliminado.

- **Replicação remota**

Indicação de se o instantâneo está ou não ativado para replicação para um cluster SolidFire remoto.
Valores possíveis:

- Ativado: O instantâneo está ativado para replicação remota.
- Desativado: O instantâneo não está ativado para replicação remota.

Criando um instantâneo de grupo

Você pode criar um snapshot de um grupo de volumes e também criar uma programação de snapshot de grupo para automatizar snapshots de grupo. Um snapshot de um único grupo pode consistentemente snapshot de até 32 volumes de uma só vez.

Passos

1. Clique em **Management > volumes**.
2. Use as caixas de seleção para selecionar vários volumes para um grupo de volumes.
3. Clique em **ações em massa**.
4. Clique em **Group Snapshot**.
5. Insira um novo nome de instantâneo de grupo na caixa de diálogo criar instantâneo de grupo de volumes.
6. **Opcional:** Selecione a caixa de seleção **incluir cada membro de instantâneo de grupo na replicação quando emparelhado** para garantir que cada instantâneo seja capturado na replicação quando o volume pai for emparelhado.
7. Selecione uma opção de retenção para o instantâneo do grupo:
 - Clique em **manter para sempre** para manter o instantâneo no sistema indefinidamente.
 - Clique em **Definir período de retenção** e use as caixas de rotação de data para escolher um período de tempo para o sistema reter o instantâneo.
8. Para fazer um instantâneo único e imediato, execute as seguintes etapas:
 - a. Clique em **Take Group Snapshot Now**.
 - b. Clique em **Create Group Snapshot**.
9. Para agendar a execução do instantâneo em um momento futuro, execute as seguintes etapas:
 - a. Clique em **Create Group Snapshot Schedule**.
 - b. Introduza um **novo nome do programa**.
 - c. Selecione um **tipo de agendamento** na lista.
 - d. **Opcional:** Selecione a caixa de seleção **Agendamento recorrente** para repetir o snapshot agendado

periodicamente.

e. Clique em **Create Schedule**.

Editar instantâneos de grupo

Você pode editar as configurações de replicação e retenção para snapshots de grupo existentes.

1. Clique em **proteção de dados > instantâneos de grupo**.
2. Clique no ícone ações do instantâneo do grupo que deseja editar.
3. No menu resultante, selecione **Editar**.
4. **Opcional:** para alterar a configuração de replicação para o instantâneo do grupo:
 - a. Clique em **Editar** ao lado de **replicação atual**.
 - b. Marque a caixa de seleção **incluir cada membro de instantâneo de grupo na replicação quando emparelhado** para garantir que cada instantâneo seja capturado na replicação quando o volume pai estiver emparelhado.
5. **Opcional:** para alterar a configuração de retenção para o instantâneo de grupo, selecione uma das seguintes opções:
 - a. Clique em **Editar** ao lado de **retenção atual**.
 - b. Selecione uma opção de retenção para o instantâneo do grupo:
 - Clique em **manter para sempre** para manter o instantâneo no sistema indefinidamente.
 - Clique em **Definir período de retenção** e use as caixas de rotação de data para escolher um período de tempo para o sistema reter o instantâneo.
6. Clique em **Salvar alterações**.

Eliminar um instantâneo de grupo

Pode eliminar um instantâneo de grupo do sistema. Ao excluir o instantâneo de grupo, você pode escolher se todos os instantâneos associados ao grupo são excluídos ou retidos como instantâneos individuais.

Se eliminar um volume ou instantâneo que seja membro de um instantâneo de grupo, já não poderá voltar ao instantâneo de grupo. No entanto, você pode reverter cada volume individualmente.

1. Clique em **proteção de dados > instantâneos de grupo**.
2. Clique no ícone ações do instantâneo que deseja excluir.
3. No menu resultante, clique em **Excluir**.
4. Selecione uma das seguintes opções na caixa de diálogo de confirmação:
 - Clique em **Excluir instantâneo de grupo E todos os membros de instantâneo de grupo** para excluir o instantâneo de grupo e todos os instantâneos de membros.
 - Clique em **reter membros de instantâneos do grupo como instantâneos individuais** para excluir o instantâneo do grupo, mas manter todos os instantâneos dos membros.
5. Confirme a ação.

Reverter volumes para um instantâneo de grupo

Você pode reverter um grupo de volumes a qualquer momento para um instantâneo de grupo.

Quando você reverte um grupo de volumes, todos os volumes do grupo são restaurados para o estado em que estavam no momento em que o snapshot do grupo foi criado. Reverter também restaura os tamanhos de volume para o tamanho gravado no instantâneo original. Se o sistema tiver purgado um volume, todos os instantâneos desse volume também foram excluídos no momento da limpeza; o sistema não restaura nenhum instantâneo de volume excluído.

1. Clique em **proteção de dados > instantâneos de grupo**.
2. Clique no ícone ações do instantâneo do grupo que você deseja usar para a reversão de volume.
3. No menu resultante, selecione **Rollback volumes para Group Snapshot**.
4. **Opcional:** Para salvar o estado atual dos volumes antes de voltar para o snapshot:
 - a. Na caixa de diálogo **Reverter para instantâneo**, selecione **Salvar estado atual dos volumes como instantâneo de grupo**.
 - b. Introduza um nome para o novo instantâneo.
5. Clique em **Rollback Group Snapshot**.

Editando membros do instantâneo do grupo

Você pode editar as configurações de retenção para membros de um instantâneo de grupo existente.

1. Clique em **proteção de dados > instantâneos**.
2. Clique na guia **Membros**.
3. Clique no ícone ações do membro instantâneo do grupo que deseja editar.
4. No menu resultante, selecione **Editar**.
5. Para alterar a configuração de replicação para o instantâneo, selecione uma das seguintes opções:
 - Clique em **manter para sempre** para manter o instantâneo no sistema indefinidamente.
 - Clique em **Definir período de retenção** e use as caixas de rotação de data para escolher um período de tempo para o sistema reter o instantâneo.
6. Clique em **Salvar alterações**.

Clonar vários volumes

Você pode criar vários clones de volume em uma única operação para criar uma cópia pontual dos dados em um grupo de volumes.

Ao clonar um volume, o sistema cria um snapshot do volume e cria um novo volume a partir dos dados no snapshot. Você pode montar e gravar no novo clone de volume. Clonar vários volumes é um processo assíncrono e leva uma quantidade variável de tempo, dependendo do tamanho e número dos volumes que estão sendo clonados.

O tamanho do volume e a carga atual do cluster afetam o tempo necessário para concluir uma operação de clonagem.

Passos

1. Clique em **Management > volumes**.
2. Clique na guia **Ativo**.
3. Use as caixas de seleção para selecionar vários volumes, criando um grupo de volumes.
4. Clique em **ações em massa**.
5. Clique em **Clone** no menu resultante.
6. Insira um **prefixo de nome de volume novo** na caixa de diálogo **Clone vários volumes**.

O prefixo é aplicado a todos os volumes do grupo.

7. **Opcional:** Selecione uma conta diferente à qual o clone pertencerá.

Se você não selecionar uma conta, o sistema atribuirá os novos volumes à conta de volume atual.

8. **Opcional:** Selecione um método de acesso diferente para os volumes no clone.

Se não selecionar um método de acesso, o sistema utiliza o acesso de volume atual.

9. Clique em **Iniciar clonagem**.

Clonar vários volumes de um snapshot de grupo

Você pode clonar um grupo de volumes a partir de um snapshot de grupo pontual. Esta operação requer que um instantâneo de grupo dos volumes já exista, porque o instantâneo de grupo é usado como base para criar os volumes. Depois de criar os volumes, você pode usá-los como qualquer outro volume no sistema.

O tamanho do volume e a carga atual do cluster afetam o tempo necessário para concluir uma operação de clonagem.

1. Clique em **proteção de dados > instantâneos de grupo**.
2. Clique no ícone **ações** do instantâneo de grupo que você deseja usar para os clones de volume.
3. No menu resultante, selecione **Clone volumes a partir de Group Snapshot**.
4. Insira um **prefixo de nome de volume novo** na caixa de diálogo **Clone volumes a partir de instantâneo de grupo**.

O prefixo é aplicado a todos os volumes criados a partir do instantâneo do grupo.

5. **Opcional:** Selecione uma conta diferente à qual o clone pertencerá.

Se você não selecionar uma conta, o sistema atribuirá os novos volumes à conta de volume atual.

6. **Opcional:** Selecione um método de acesso diferente para os volumes no clone.

Se não selecionar um método de acesso, o sistema utiliza o acesso de volume atual.

7. Clique em **Iniciar clonagem**.

Agendar um instantâneo

Você pode proteger os dados em um volume ou em um grupo de volumes agendando instantâneos de volume em intervalos especificados. Você pode agendar snapshots de volume único ou snapshots de grupo para serem executados automaticamente.

Ao configurar uma programação de instantâneos, você pode escolher entre intervalos de tempo com base em dias da semana ou dias do mês. Você também pode especificar os dias, horas e minutos antes que o próximo snapshot ocorra. Você pode armazenar os snapshots resultantes em um sistema de storage remoto se o volume estiver sendo replicado.

Encontre mais informações

- [Criar uma agenda de instantâneos](#)
- [Editar uma agenda de instantâneos](#)
- [Eliminar uma agenda de instantâneos](#)
- [Copiar uma agenda de instantâneos](#)

Detalhes do agendamento do Snapshot

Na página proteção de dados > agendas, pode visualizar as seguintes informações na lista de agendas de instantâneos.

- **ID**

A ID gerada pelo sistema para o instantâneo.

- **Tipo**

O tipo de programação. Instantâneo é atualmente o único tipo suportado.

- **Nome**

O nome dado à programação quando foi criada. Os nomes de agendamento instantâneo podem ter até 223 caracteres de comprimento e conter caracteres a-z, 0-9 e traço (-).

- **Frequência**

A frequência em que o programa é executado. A frequência pode ser definida em horas e minutos, semanas ou meses.

- **Recorrente**

Indicação de se o programa deve ser executado apenas uma vez ou em intervalos regulares.

- **Manualmente em pausa**

Indicação de se o agendamento foi ou não pausado manualmente.

- **IDs de volume**

A ID do volume que a programação usará quando a programação for executada.

- **Último Run**

A última vez que a programação foi executada.

- **Estado da última corrida**

O resultado da última execução do cronograma. Valores possíveis:

- Sucesso
- Falha

Criar uma agenda de instantâneos

Você pode agendar um instantâneo de um volume ou volumes para que ocorra automaticamente em intervalos especificados.

Ao configurar uma programação de instantâneos, você pode escolher entre intervalos de tempo com base em dias da semana ou dias do mês. Você também pode criar uma programação recorrente e especificar os dias, horas e minutos antes do próximo snapshot ocorrer.

Se você agendar um snapshot para ser executado em um período de tempo que não é divisível em 5 minutos, o snapshot será executado no próximo período de tempo que é divisível em 5 minutos. Por exemplo, se você agendar um snapshot para ser executado às 12:42:00 UTC, ele será executado às 12:45:00 UTC. Não é possível programar um instantâneo para ser executado em intervalos inferiores a 5 minutos.

Passos

1. Clique em **proteção de dados > horários**.
2. Clique em **Create Schedule**.
3. No campo **IDs de volume CSV**, insira um único ID de volume ou uma lista separada por vírgulas de IDs de volume a incluir na operação de snapshot.
4. Introduza um novo nome de programação.
5. Selecione um tipo de agendamento e defina o agendamento nas opções fornecidas.
6. **Opcional:** Selecione **Agendamento recorrente** para repetir o agendamento de snapshot indefinidamente.
7. **Opcional:** Digite um nome para o novo snapshot no campo **novo Nome do instantâneo**.

Se você deixar o campo em branco, o sistema usará a hora e a data da criação do instantâneo como nome.

8. **Opcional:** Selecione a caixa de seleção **incluir instantâneos na replicação quando emparelhado** para garantir que os instantâneos sejam capturados na replicação quando o volume pai estiver emparelhado.
9. Para definir a retenção para o instantâneo, selecione uma das seguintes opções:
 - Clique em **manter para sempre** para manter o instantâneo no sistema indefinidamente.
 - Clique em **Definir período de retenção** e use as caixas de rotação de data para escolher um período de tempo para o sistema reter o instantâneo.
10. Clique em **Create Schedule**.

Editar uma agenda de instantâneos

Você pode modificar programações de snapshot existentes. Após a modificação, na

próxima vez que o agendamento for executado, ele usará os atributos atualizados. Todos os instantâneos criados pela programação original permanecem no sistema de armazenamento.

Passos

1. Clique em **proteção de dados > horários**.
2. Clique no ícone **ações** para a programação que deseja alterar.
3. No menu resultante, clique em **Editar**.
4. No campo **IDs de volume CSV**, modifique o ID de volume único ou a lista separada por vírgulas de IDs de volume atualmente incluídas na operação de snapshot.
5. Para pausar ou retomar o agendamento, selecione uma das seguintes opções:
 - Para pausar uma programação ativa, selecione **Sim** na lista **Pausar manualmente a programação**.
 - Para retomar um agendamento em pausa, selecione **não** na lista **Pausar manualmente o agendamento**.
6. Digite um nome diferente para a programação no campo **New Schedule Name**, se desejado.
7. Para alterar a programação a ser executada em diferentes dias da semana ou mês, selecione **tipo de programação** e altere a programação nas opções fornecidas.
8. **Opcional:** Selecione **Agendamento recorrente** para repetir o agendamento de snapshot indefinidamente.
9. **Opcional:** Digite ou modifique o nome do novo snapshot no campo **Nome do novo snapshot**.

Se você deixar o campo em branco, o sistema usará a hora e a data da criação do instantâneo como nome.

10. **Opcional:** Selecione a caixa de seleção **incluir instantâneos na replicação quando emparelhado** para garantir que os instantâneos sejam capturados na replicação quando o volume pai estiver emparelhado.
11. Para alterar a configuração de retenção, selecione uma das seguintes opções:
 - Clique em **manter para sempre** para manter o instantâneo no sistema indefinidamente.
 - Clique em **Definir período de retenção** e use as caixas de rotação de data para selecionar um período de tempo para que o sistema retenha o instantâneo.
12. Clique em **Salvar alterações**.

Copiar uma agenda de instantâneos

Você pode copiar uma programação e manter seus atributos atuais.

1. Clique em **proteção de dados > horários**.
2. Clique no ícone **ações** da programação que deseja copiar.
3. No menu resultante, clique em **fazer uma cópia**.

A caixa de diálogo **Create Schedule** é exibida, preenchida com os atributos atuais da programação.

4. **Opcional:** Digite um nome e atributos atualizados para a nova programação.
5. Clique em **Create Schedule**.

Eliminar uma agenda de instantâneos

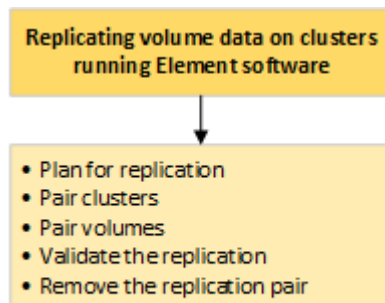
Pode eliminar uma agenda de instantâneos. Depois de excluir a programação, ela não executa nenhum instantâneo agendado futuro. Todos os snapshots que foram criados pela programação permanecem no sistema de storage.

1. Clique em **proteção de dados > horários**.
2. Clique no ícone **ações** da programação que deseja excluir.
3. No menu resultante, clique em **Excluir**.
4. Confirme a ação.

Executar replicação remota entre clusters que executam o software NetApp Element

Para clusters que executam o software Element, a replicação em tempo real permite a criação rápida de cópias remotas de dados de volume. É possível emparelhar um cluster de storage com até quatro outros clusters de storage. É possível replicar dados de volume de forma síncrona ou assíncrona de qualquer cluster em um par de cluster para cenários de failover e failback.

O processo de replicação inclui estas etapas:



- "Planeje o cluster e o emparelhamento de volume para replicação em tempo real"
- "Emparelhe clusters para replicação"
- "Emparelhar volumes"
- "Valide a replicação de volume"
- "Excluir uma relação de volume após a replicação"
- "Gerenciar relacionamentos de volume"

Planeje o cluster e o emparelhamento de volume para replicação em tempo real

A replicação remota em tempo real requer o emparelhamento de dois clusters de storage que executam o software Element, o emparelhamento de volumes em cada cluster e a validação da replicação. Após a conclusão da replicação, você deve excluir a relação de volume.

O que você vai precisar

- Você deve ter o Privileges do administrador de cluster para um ou ambos os clusters sendo emparelhados.
- Todos os endereços IP de nó em redes de gerenciamento e armazenamento para clusters emparelhados são roteados entre si.
- A MTU de todos os nós emparelhados deve ser a mesma e ser suportada de ponta a ponta entre clusters.
- Ambos os clusters de armazenamento devem ter nomes de cluster exclusivos, MVIPs, SVIPs. E todos os endereços IP dos nós.
- A diferença entre as versões do software Element nos clusters não é maior que uma versão principal. Se a diferença for maior, um dos clusters deve ser atualizado para executar a replicação de dados.



Os dispositivos do acelerador de WAN não foram qualificados pelo NetApp para uso durante a replicação de dados. Esses dispositivos podem interferir na compactação e na deduplicação, se implantados entre dois clusters que estão replicando dados. Certifique-se de qualificar totalmente os efeitos de qualquer dispositivo do acelerador de WAN antes de implantá-lo em um ambiente de produção.

Encontre mais informações

- [Emparelhe clusters para replicação](#)
- [Emparelhar volumes](#)
- [Atribua uma origem de replicação e um destino a volumes emparelhados](#)

Emparelhe clusters para replicação

É necessário emparelhar dois clusters como primeira etapa para usar a funcionalidade de replicação em tempo real. Depois de emparelhar e conectar dois clusters, é possível configurar volumes ativos em um cluster para serem replicados continuamente para um segundo cluster, fornecendo proteção contínua de dados (CDP).

O que você vai precisar

- Você deve ter o Privileges do administrador de cluster para um ou ambos os clusters sendo emparelhados.
- Todos os mips e SIPs dos nós são roteados entre si.
- Menos de 2000 ms de latência de ida e volta entre clusters.
- Ambos os clusters de armazenamento devem ter nomes de cluster exclusivos, MVIPs, SVIPs e todos os endereços IP dos nós.
- A diferença entre as versões do software Element nos clusters não é maior que uma versão principal. Se a diferença for maior, um dos clusters deve ser atualizado para executar a replicação de dados.



O emparelhamento de cluster requer conectividade total entre nós na rede de gerenciamento. A replicação requer conectividade entre os nós individuais na rede do cluster de storage.

É possível emparelhar um cluster com até quatro outros clusters para replicar volumes. Também é possível emparelhar clusters no grupo de clusters uns com os outros.

Encontre mais informações

[Requisitos de porta de rede](#)

Emparelhe clusters usando MVIP ou uma chave de emparelhamento

Você pode emparelhar um cluster de origem e destino usando o MVIP do cluster de destino se houver acesso de administrador de cluster aos dois clusters. Se o acesso do administrador do cluster estiver disponível apenas num cluster num par de clusters, pode ser utilizada uma chave de emparelhamento no cluster de destino para concluir o emparelhamento do cluster.

1. Selecione um dos seguintes métodos para emparelhar clusters:
 - Emparelhar clusters usando MVIP: Use este método se houver acesso de administrador de cluster a ambos os clusters. Este método usa o MVIP do cluster remoto para emparelhar dois clusters.
 - Emparelhar clusters usando uma chave de emparelhamento: Use este método se houver acesso de administrador de cluster a apenas um dos clusters. Este método gera uma chave de emparelhamento que pode ser utilizada no cluster de destino para concluir o emparelhamento do cluster.

Encontre mais informações

- [Emparelhe clusters usando MVIP](#)
- [Emparelhe clusters usando uma chave de emparelhamento](#)

Emparelhe clusters usando MVIP

É possível emparelhar dois clusters para replicação em tempo real usando o MVIP de um cluster para estabelecer uma conexão com o outro cluster. Para usar esse método, é necessário o acesso de administrador de cluster nos dois clusters. O nome de usuário e a senha do administrador do cluster são usados para autenticar o acesso ao cluster antes que os clusters possam ser emparelhados.

1. No cluster local, selecione **proteção de dados > pares de cluster**.
2. Clique em **Emparelhar Cluster**.
3. Clique em **Start Pairing** (Iniciar emparelhamento) e clique em **Yes** (Sim) para indicar que tem acesso ao cluster remoto.
4. Introduza o endereço MVIP do cluster remoto.
5. Clique em **Complete pareamento no cluster remoto**.

Na janela **Autenticação necessária**, introduza o nome de utilizador e a palavra-passe do administrador do cluster remoto.

6. No cluster remoto, selecione **proteção de dados > pares de cluster**.
7. Clique em **Emparelhar Cluster**.
8. Clique em **Complete Pairing**.
9. Clique no botão **Complete Pairing**.

Encontre mais informações

- [Emparelhe clusters usando uma chave de emparelhamento](#)
- ["Emparelhar clusters com MVIP \(vídeo\)"](#)

Emparelhe clusters usando uma chave de emparelhamento

Se tiver acesso de administrador de cluster a um cluster local, mas não ao cluster remoto, pode emparelhar os clusters utilizando uma chave de emparelhamento. Uma chave de emparelhamento é gerada em um cluster local e, em seguida, enviada com segurança para um administrador de cluster em um local remoto para estabelecer uma conexão e concluir o emparelhamento de cluster para replicação em tempo real.

1. No cluster local, selecione **proteção de dados > pares de cluster**.
2. Clique em **Emparelhar Cluster**.
3. Clique em **Start Pairing** (Iniciar emparelhamento) e clique em **no** para indicar que não tem acesso ao cluster remoto.
4. Clique em **Generate Key**.



Esta ação gera uma chave de texto para emparelhamento e cria um par de cluster não configurado no cluster local. Se não concluir o procedimento, terá de eliminar manualmente o par de clusters.

5. Copie a chave de emparelhamento do cluster para a área de transferência.
6. Torne a chave de emparelhamento acessível ao administrador do cluster no local do cluster remoto.



A chave de emparelhamento do cluster contém uma versão do MVIP, nome de utilizador, palavra-passe e informações da base de dados para permitir ligações de volume para replicação remota. Esta chave deve ser tratada de forma segura e não armazenada de forma a permitir o acesso acidental ou não seguro ao nome de utilizador ou palavra-passe.



Não modifique nenhum dos caracteres da chave de emparelhamento. A chave se torna inválida se for modificada.

7. No cluster remoto, selecione **proteção de dados > pares de cluster**.
8. Clique em **Emparelhar Cluster**.
9. Clique em **Complete Pairing** (concluir emparelhamento) e introduza a chave de emparelhamento no campo **Pairing Key** (colar é o método recomendado).
10. Clique em **Complete Pairing**.

Encontre mais informações

- [Emparelhe clusters usando MVIP](#)
- ["Emparelhar clusters utilizando uma chave de emparelhamento de cluster \(vídeo\)"](#)

Valide a conexão do par de cluster

Depois que o emparelhamento do cluster estiver concluído, você pode querer verificar a conexão do par de cluster para garantir o sucesso da replicação.

1. No cluster local, selecione **proteção de dados > pares de cluster**.
2. Na janela **pares de cluster**, verifique se o par de cluster está conectado.
3. **Opcional:** navegue de volta para o cluster local e para a janela **pares de cluster** e verifique se o par de cluster está conectado.

Emparelhar volumes

Depois de estabelecer uma conexão entre clusters em um par de cluster, é possível emparelhar um volume em um cluster com um volume no outro cluster do par. Quando é estabelecida uma relação de emparelhamento de volume, tem de identificar qual o volume que é o destino de replicação.

É possível emparelhar dois volumes para replicação em tempo real armazenados em diferentes clusters de storage em um par de cluster conectado. Depois de emparelhar dois clusters, é possível configurar volumes ativos em um cluster para serem replicados continuamente para um segundo cluster, fornecendo proteção contínua de dados (CDP). Você também pode atribuir um volume para ser a origem ou destino da replicação.

Os emparelhamentos de volume são sempre um-para-um. Depois de um volume fazer parte de um emparelhamento com um volume noutro cluster, não é possível emparelhá-lo novamente com qualquer outro volume.

O que você vai precisar

- Você estabeleceu uma conexão entre clusters em um par de cluster.
- Você tem Privileges de administrador de cluster para um ou ambos os clusters sendo emparelhados.

Passos

1. [Crie um volume de destino com acesso de leitura ou gravação](#)
2. [Emparelhe volumes utilizando uma ID de volume ou uma tecla de emparelhamento](#)
3. [Atribua uma origem de replicação e um destino a volumes emparelhados](#)

Crie um volume de destino com acesso de leitura ou gravação

O processo de replicação envolve dois endpoints: A origem e o volume de destino. Quando você cria o volume de destino, o volume é automaticamente definido para o modo de leitura/gravação para aceitar os dados durante a replicação.

1. Selecione **Management > volumes**.
2. Clique em **criar volume**.
3. Na caixa de diálogo criar um novo volume, insira o Nome do volume.
4. Insira o tamanho total do volume, selecione um tamanho de bloco para o volume e selecione a conta que deve ter acesso ao volume.
5. Clique em **criar volume**.
6. Na janela ativa, clique no ícone ações do volume.

7. Clique em **Editar**.
8. Altere o nível de acesso à conta para destino de replicação.
9. Clique em **Salvar alterações**.

Emparelhe volumes utilizando uma ID de volume ou uma tecla de emparelhamento

O processo de emparelhamento envolve o emparelhamento de dois volumes utilizando uma ID de volume ou uma tecla de emparelhamento.

1. Emparelhe volumes selecionando um dos seguintes métodos:
 - Usando um ID de volume: Use este método se você tiver acesso de administrador de cluster a ambos os clusters nos quais os volumes devem ser emparelhados. Este método usa a ID do volume do volume no cluster remoto para iniciar uma conexão.
 - Usando uma chave de emparelhamento: Use este método se você tiver acesso de administrador de cluster apenas ao cluster de origem. Este método gera uma chave de emparelhamento que pode ser utilizada no cluster remoto para concluir o par de volumes.



A chave de emparelhamento de volume contém uma versão encriptada das informações de volume e pode conter informações confidenciais. Compartilhe esta chave apenas de forma segura.

Encontre mais informações

- [Emparelhe volumes usando um ID de volume](#)
- [Emparelhe volumes utilizando uma tecla de emparelhamento](#)

Emparelhe volumes usando um ID de volume

Você pode emparelhar um volume com outro volume em um cluster remoto se tiver credenciais de administrador de cluster para o cluster remoto.

O que você vai precisar

- Certifique-se de que os clusters que contêm os volumes estão emparelhados.
- Crie um novo volume no cluster remoto.



Pode atribuir uma origem e um destino de replicação após o processo de emparelhamento. Uma origem ou destino de replicação pode ser um volume em um par de volumes. Você deve criar um volume de destino que não contenha dados e tenha as características exatas do volume de origem, como tamanho, configuração de tamanho de bloco para os volumes (512e ou 4K) e configuração de QoS. Se você atribuir um volume existente como destino de replicação, os dados nesse volume serão sobrescritos. O volume de destino pode ser maior ou igual em tamanho ao volume de origem, mas não pode ser menor.

- Conheça o ID de volume alvo.

Passos

1. Selecione **Management > volumes**.
2. Clique no ícone **ações** para o volume que deseja emparelhar.

3. Clique em **Emparelhar**.
4. Na caixa de diálogo **Emparelhar volume**, selecione **Iniciar emparelhamento**.
5. Selecione **I do** para indicar que você tem acesso ao cluster remoto.
6. Selecione um **Replication Mode** na lista:
 - **Tempo real (assíncrono)**: As gravações são confirmadas para o cliente depois que são confirmadas no cluster de origem.
 - **Tempo real (Synchronous)**: As gravações são confirmadas para o cliente depois que são confirmadas nos clusters de origem e de destino.
 - **Somente snapshots**: Somente snapshots criados no cluster de origem são replicados. As gravações ativas do volume de origem não são replicadas.
7. Selecione um cluster remoto na lista.
8. Escolha um ID de volume remoto.
9. Clique em **Start Pairing** (Iniciar emparelhamento).

O sistema abre uma guia do navegador da Web que se conecta à IU do elemento do cluster remoto. Talvez seja necessário fazer logon no cluster remoto com credenciais de administrador de cluster.

10. Na IU do elemento do cluster remoto, selecione **Complete Pairing**.
11. Confirme os detalhes em **Confirm volume Pairing**.
12. Clique em **Complete Pairing**.

Depois de confirmar o emparelhamento, os dois clusters iniciam o processo de ligação dos volumes para emparelhamento. Durante o processo de emparelhamento, você pode ver mensagens na coluna **Status do volume** da janela **pares de volume**. O par de volumes é exibido `PausedMisconfigured` até que a origem e o destino do par de volumes sejam atribuídos.

Depois de concluir o emparelhamento com êxito, deve atualizar a tabela volumes para remover a opção **Emparelhar** da lista **ações** para o volume emparelhado. Se você não atualizar a tabela, a opção **Pair** permanecerá disponível para seleção. Se você selecionar a opção **Emparelhar** novamente, uma nova guia será aberta e, como o volume já está emparelhado, o sistema informará uma `StartVolumePairing Failed: xVolumeAlreadyPaired` mensagem de erro na janela **Emparelhar volume** da página IU do elemento.

Encontre mais informações

- [Mensagens de emparelhamento de volume](#)
- [Avisos de emparelhamento de volume](#)
- [Atribua uma origem de replicação e um destino a volumes emparelhados](#)

Emparelhe volumes utilizando uma tecla de emparelhamento

Se não tiver credenciais de administrador de cluster para um cluster remoto, pode emparelhar um volume com outro volume num cluster remoto utilizando uma chave de emparelhamento.

O que você vai precisar

- Certifique-se de que os clusters que contêm os volumes estão emparelhados.

- Certifique-se de que existe um volume no painel remoto a utilizar para o emparelhamento.



Pode atribuir uma origem e um destino de replicação após o processo de emparelhamento. Uma origem ou destino de replicação pode ser um volume em um par de volumes. Você deve criar um volume de destino que não contenha dados e tenha as características exatas do volume de origem, como tamanho, configuração de tamanho de bloco para os volumes (512e ou 4K) e configuração de QoS. Se você atribuir um volume existente como destino de replicação, os dados nesse volume serão sobrescritos. O volume de destino pode ser maior ou igual em tamanho ao volume de origem, mas não pode ser menor.

Passos

1. Selecione **Management > volumes**.
2. Clique no ícone **ações** para o volume que deseja emparelhar.
3. Clique em **Emparelhar**.
4. Na caixa de diálogo **Emparelhar volume**, selecione **Iniciar emparelhamento**.
5. Selecione **não** para indicar que não tem acesso ao cluster remoto.
6. Selecione um **Replication Mode** na lista:
 - **Tempo real (assíncrono)**: As gravações são confirmadas para o cliente depois que são confirmadas no cluster de origem.
 - **Tempo real (Synchronous)**: As gravações são confirmadas para o cliente depois que são confirmadas nos clusters de origem e de destino.
 - **Somente snapshots**: Somente snapshots criados no cluster de origem são replicados. As gravações ativas do volume de origem não são replicadas.
7. Clique em **Generate Key**.



Esta ação gera uma chave de texto para emparelhamento e cria um par de volume não configurado no cluster local. Se não concluir o procedimento, terá de eliminar manualmente o par de volumes.

8. Copie a chave de emparelhamento para a área de transferência do computador.
9. Torne a tecla de emparelhamento acessível ao administrador do cluster no local do cluster remoto.



A tecla de emparelhamento de volume deve ser tratada de forma segura e não utilizada de forma a permitir o acesso acidental ou não seguro.



Não modifique nenhum dos caracteres da chave de emparelhamento. A chave se torna inválida se for modificada.

10. Na IU do elemento de cluster remoto, selecione **Management > volumes**.
11. Clique no ícone **ações** do volume que deseja emparelhar.
12. Clique em **Emparelhar**.
13. Na caixa de diálogo **Emparelhar volume**, selecione **Complete Pairing**.
14. Cole a chave de emparelhamento do outro cluster na caixa **chave de emparelhamento**.
15. Clique em **Complete Pairing**.

Depois de confirmar o emparelhamento, os dois clusters iniciam o processo de ligação dos volumes para emparelhamento. Durante o processo de emparelhamento, você pode ver mensagens na coluna **Status do volume** da janela **pares de volume**. O par de volumes é exibido `PausedMisconfigured` até que a origem e o destino do par de volumes sejam atribuídos.

Depois de concluir o emparelhamento com êxito, deve atualizar a tabela volumes para remover a opção **Emparelhar** da lista **ações** para o volume emparelhado. Se você não atualizar a tabela, a opção **Pair** permanecerá disponível para seleção. Se você selecionar a opção **Emparelhar** novamente, uma nova guia será aberta e, como o volume já está emparelhado, o sistema informará uma `StartVolumePairing Failed: xVolumeAlreadyPaired` mensagem de erro na janela **Emparelhar volume** da página IU do elemento.

Encontre mais informações

- [Mensagens de emparelhamento de volume](#)
- [Avisos de emparelhamento de volume](#)
- [Atribua uma origem de replicação e um destino a volumes emparelhados](#)

Atribua uma origem de replicação e um destino a volumes emparelhados

Depois que os volumes estiverem emparelhados, você deverá atribuir um volume de origem e seu volume de destino de replicação. Uma origem ou destino de replicação pode ser um volume em um par de volumes. Você também pode usar este procedimento para redirecionar os dados enviados para um volume de origem para um volume de destino remoto, caso o volume de origem fique indisponível.

O que você vai precisar

Você tem acesso aos clusters que contêm os volumes de origem e destino.

Passos

1. Preparar o volume de origem:
 - a. No cluster que contém o volume que você deseja atribuir como origem, selecione **Gerenciamento > volumes**.
 - b. Clique no ícone **ações** para o volume que deseja atribuir como fonte e clique em **Editar**.
 - c. Na lista suspensa **Access**, selecione **Read/Write**.



Se você estiver invertendo a atribuição de origem e destino, essa ação fará com que o par de volume exiba a seguinte mensagem até que um novo destino de replicação seja atribuído: `PausedMisconfigured`

A alteração do acesso interrompe a replicação de volume e faz com que a transmissão de dados cesse. Certifique-se de que você coordenou essas alterações em ambos os sites.

- a. Clique em **Salvar alterações**.
2. Preparar o volume alvo:
 - a. No cluster que contém o volume que você deseja atribuir como destino, selecione **Gerenciamento > volumes**.
 - b. Clique no ícone **ações** do volume que você deseja atribuir como destino e clique em **Editar**.

c. Na lista suspensa **Access**, selecione **Replication Target**.



Se você atribuir um volume existente como destino de replicação, os dados nesse volume serão sobrescritos. Você deve usar um novo volume de destino que não contenha dados e tenha as características exatas do volume de origem, como tamanho, configuração 512e e configuração de QoS. O volume de destino pode ser maior ou igual em tamanho ao volume de origem, mas não pode ser menor.

d. Clique em **Salvar alterações**.

Encontre mais informações

- [Emparelhe volumes usando um ID de volume](#)
- [Emparelhe volumes utilizando uma tecla de emparelhamento](#)

Valide a replicação de volume

Depois que um volume é replicado, você deve garantir que os volumes de origem e destino estejam ativos. Quando em um estado ativo, os volumes são emparelhados, os dados estão sendo enviados da origem para o volume de destino e os dados estão em sincronia.

1. Em ambos os clusters, selecione **proteção de dados > pares de volume**.
2. Verifique se o status do volume está Ativo.

Encontre mais informações

[Avisos de emparelhamento de volume](#)

Excluir uma relação de volume após a replicação

Após a conclusão da replicação e não precisar mais do relacionamento de par de volume, você poderá excluir o relacionamento de volume.

1. Selecione **proteção de dados > pares de volume**.
2. Clique no ícone **ações** para o par de volumes que deseja excluir.
3. Clique em **Excluir**.
4. Confirme a mensagem.

Gerenciar relacionamentos de volume

Você pode gerenciar relacionamentos de volume de várias maneiras, como pausar a replicação, inverter o emparelhamento de volume, alterar o modo de replicação, excluir um par de volume ou excluir um par de cluster.

Encontre mais informações

- [Pausar a replicação](#)
- [Altere o modo de replicação](#)

- [Eliminar pares de volume](#)

Pausar a replicação

Você pode pausar manualmente a replicação se precisar interromper o processamento de e/S por um curto período de tempo. Talvez você queira pausar a replicação se houver um aumento no processamento de e/S e você quiser reduzir a carga de processamento.

1. Selecione **proteção de dados > pares de volume**.
2. Clique no ícone ações do par de volumes.
3. Clique em **Editar**.
4. No painel **Editar par de volume**, pause manualmente o processo de replicação.



Pausar ou retomar a replicação de volume manualmente faz com que a transmissão de dados cesse ou retome. Certifique-se de que você coordenou essas alterações em ambos os sites.

5. Clique em **Salvar alterações**.

Altere o modo de replicação

Você pode editar as propriedades do par de volume para alterar o modo de replicação da relação de par de volume.

1. Selecione **proteção de dados > pares de volume**.
2. Clique no ícone ações do par de volumes.
3. Clique em **Editar**.
4. No painel **Editar par de volume**, selecione um novo modo de replicação:
 - **Tempo real (assíncrono)**: As gravações são confirmadas para o cliente depois que são confirmadas no cluster de origem.
 - **Tempo real (Synchronous)**: As gravações são confirmadas para o cliente depois que são confirmadas nos clusters de origem e de destino.
 - **Somente snapshots**: Somente snapshots criados no cluster de origem são replicados. As gravações ativas do volume de origem não são replicadas. **Atenção**: alterar o modo de replicação altera o modo imediatamente. Certifique-se de que você coordenou essas alterações em ambos os sites.
5. Clique em **Salvar alterações**.

Eliminar pares de volume

Você pode excluir um par de volume se quiser remover uma associação de par entre dois volumes.

1. Selecione **proteção de dados > pares de volume**.
2. Clique no ícone ações do par de volumes que deseja excluir.
3. Clique em **Excluir**.
4. Confirme a mensagem.

Excluir um par de cluster

Você pode excluir um par de cluster da IU do elemento de um dos clusters do par.

1. Clique em **proteção de dados > pares de cluster**.
2. Clique no ícone ações de um par de cluster.
3. No menu resultante, clique em **Excluir**.
4. Confirme a ação.
5. Execute novamente os passos a partir do segundo cluster no emparelhamento do cluster.

Detalhes do par de cluster

A página pares de cluster na guia proteção de dados fornece informações sobre clusters que foram emparelhados ou que estão em processo de emparelhamento. O sistema exibe mensagens de emparelhamento e progresso na coluna Status.

- **ID**

Um ID gerado pelo sistema dado a cada par de cluster.

- **Nome do cluster remoto**

O nome do outro cluster no par.

- **MVIP remoto**

O endereço IP virtual de gerenciamento do outro cluster no par.

- **Status**

Estado da replicação do cluster remoto

- **Replicação de volumes**

O número de volumes contidos pelo cluster que são emparelhados para replicação.

- **UUID**

Um ID exclusivo dado a cada cluster no par.

Detalhes do par de volume

A página pares de volume na guia proteção de dados fornece informações sobre volumes que foram emparelhados ou que estão em processo de emparelhamento. O sistema apresenta mensagens de emparelhamento e progresso na coluna Estado do volume.

- **ID**

ID gerado pelo sistema para o volume.

- **Nome**

O nome dado ao volume quando foi criado. Os nomes de volume podem ter até 223 caracteres e conter a-z, 0-9 e traço (-).

- **Conta**

Nome da conta atribuída ao volume.

- **Status do volume**

Estado da replicação do volume

- **Status do Snapshot**

Estado do volume instantâneo.

- **Modo**

O método de replicação de gravação do cliente. Os valores possíveis são os seguintes:

- Assíncrono
- Apenas Snapshot
- Sincronizar

- **Direção**

A direção dos dados do volume:

- O ícone de volume de origem (➔) indica que os dados estão sendo gravados em um destino fora do cluster.
- O ícone de volume de destino (➔) indica que os dados estão sendo gravados no volume local de uma fonte externa.

- **Atraso de sincronização**

Período de tempo desde que o volume foi sincronizado pela última vez com o cluster remoto. Se o volume não estiver emparelhado, o valor será nulo.

- **Cluster remoto**

Nome do cluster remoto no qual o volume reside.

- **ID de volume remoto**

ID do volume do volume no cluster remoto.

- **Nome do volume remoto**

Nome dado ao volume remoto quando foi criado.

Mensagens de emparelhamento de volume

Pode ver mensagens de emparelhamento de volume durante o processo de emparelhamento inicial a partir da página pares de volume, no separador proteção de dados. Essas mensagens podem ser exibidas nas extremidades de origem e destino do

par na exibição de lista de volumes replicáveis.

- **PausedDisconnected**

Replicação de origem ou sincronização de RPCs excedeu o tempo limite. A ligação ao cluster remoto foi perdida. Verifique as ligações de rede ao cluster.

- **ResumingConnected**

A sincronização de replicação remota está agora ativa. Iniciar o processo de sincronização e aguardar dados.

- **ResumingRRSync**

Uma única cópia em hélice dos metadados de volume está sendo feita para o cluster emparelhado.

- **ResumingLocalSync**

Uma cópia em hélice dupla dos metadados de volume está sendo feita para o cluster emparelhado.

- **ResumingDataTransfer**

A transferência de dados foi retomada.

- **Ativo**

Os volumes são emparelhados e os dados estão sendo enviados da origem para o volume de destino e os dados estão sincronizados.

- **Ocioso**

Nenhuma atividade de replicação está ocorrendo.

Avisos de emparelhamento de volume

A página pares de volume na guia proteção de dados fornece essas mensagens depois de emparelhar volumes. Essas mensagens podem ser exibidas nas extremidades de origem e destino do par (a menos que indicado de outra forma) na exibição de lista de volumes replicáveis.

- **PausedClusterFull**

Como o cluster de destino está cheio, a replicação de origem e a transferência de dados em massa não podem prosseguir. A mensagem é exibida apenas na extremidade de origem do par.

- **PausedExceededMaxSnapshotCount**

O volume de destino já tem o número máximo de instantâneos e não pode replicar instantâneos adicionais.

- **PausedManual**

O volume local foi pausado manualmente. Ele deve ser despausado antes que a replicação seja retomada.

- **PausedManualRemote**

O volume remoto está no modo de pausa manual. É necessária uma intervenção manual para interromper o volume remoto antes de a replicação ser retomada.

- **PausedMisconfigured**

Aguardando uma fonte e destino ativos. Intervenção manual necessária para retomar a replicação.

- **PausedQoS**

A QoS de destino não pôde sustentar a entrada de e/S. A replicação retoma automática. A mensagem é exibida apenas na extremidade de origem do par.

- **PausedSlowLink**

Ligação lenta detetada e interrompida a replicação. A replicação retoma automática. A mensagem é exibida apenas na extremidade de origem do par.

- **PausedVolumeSizeMismatch**

O volume de destino não tem o mesmo tamanho que o volume de origem.

- **PausedXCOPY**

Um comando SCSI XCOPY está sendo emitido para um volume de origem. O comando deve ser concluído antes que a replicação possa ser retomada. A mensagem é exibida apenas na extremidade de origem do par.

- **StoppedMisconfigured**

Foi detetado um erro de configuração permanente. O volume remoto foi purgado ou não emparelhado. Não é possível efetuar qualquer ação corretiva; é necessário estabelecer um novo emparelhamento.

Use a replicação do SnapMirror entre clusters Element e ONTAP

Você pode criar relacionamentos do SnapMirror a partir da guia proteção de dados na IU do NetApp Element. A funcionalidade SnapMirror deve estar ativada para ver isso na interface do usuário.

O IPv6 não é compatível com replicação SnapMirror entre o software NetApp Element e os clusters do ONTAP.

["Vídeo do NetApp: SnapMirror para software NetApp HCI e Element"](#)

Os sistemas que executam o software NetApp Element oferecem suporte ao recurso SnapMirror para copiar e restaurar cópias Snapshot com sistemas NetApp ONTAP. O principal motivo para usar essa tecnologia é a recuperação de desastres do NetApp HCI para o ONTAP. Os pontos de extremidade incluem ONTAP, ONTAP Select e Cloud Volumes ONTAP. Consulte proteção de dados NetApp HCI TR-4641.

["Relatório técnico da NetApp 4641: Proteção de dados da NetApp HCI"](#)

Encontre mais informações

- ["Crie seu Data Fabric com NetApp HCI, ONTAP e infraestrutura convergente"](#)
- ["Replicação entre o software NetApp Element e o ONTAP"](#)

Visão geral do SnapMirror

Os sistemas que executam o software NetApp Element suportam a funcionalidade SnapMirror para copiar e restaurar snapshots com sistemas NetApp ONTAP.

Os sistemas que executam o Element podem se comunicar diretamente com o SnapMirror em sistemas ONTAP 9,3 ou superior. A API do NetApp Element fornece métodos para habilitar a funcionalidade do SnapMirror em clusters, volumes e snapshots. Além disso, a IU do Element inclui todas as funcionalidades necessárias para gerenciar as relações do SnapMirror entre o software Element e os sistemas ONTAP.

Você pode replicar volumes originados do ONTAP para volumes de elementos em casos de uso específicos com funcionalidade limitada. Para obter mais informações, consulte a documentação do ONTAP.

Encontre mais informações

["Replicação entre o software Element e o ONTAP"](#)

Ative o SnapMirror no cluster

Você deve habilitar manualmente a funcionalidade do SnapMirror no nível do cluster por meio da IU do NetApp Element. O sistema vem com a funcionalidade SnapMirror desativada por padrão e não é automaticamente ativada como parte de uma nova instalação ou atualização. Ativar o recurso SnapMirror é uma tarefa de configuração única.

O SnapMirror só pode ser habilitado para clusters que executam o software Element usado em conjunto com volumes em um sistema NetApp ONTAP. Você deve habilitar a funcionalidade SnapMirror somente se o cluster estiver conectado para uso com o NetApp ONTAP volumes.

O que você vai precisar

O cluster de storage deve estar executando o software NetApp Element.

Passos

1. Clique em **clusters > Configurações**.
2. Encontre as configurações específicas do cluster para o SnapMirror.
3. Clique em **Ativar SnapMirror**.



Ativar a funcionalidade SnapMirror altera permanentemente a configuração do software Element. Pode desativar a funcionalidade SnapMirror e restaurar as predefinições apenas devolvendo o cluster à imagem de fábrica.

4. Clique em **Sim** para confirmar a alteração de configuração do SnapMirror.

Ative o SnapMirror no volume

Você deve habilitar o SnapMirror no volume na IU do Element. Isso permite a replicação

de dados para volumes ONTAP especificados. Esta é a permissão do administrador do cluster que executa o software NetApp Element para SnapMirror para controlar um volume.

O que você vai precisar

- Você ativou o SnapMirror na IU do Element para o cluster.
- Um endpoint SnapMirror está disponível.
- O volume tem de ser de 512e blocos.
- O volume não está participando da replicação remota.
- O tipo de acesso de volume não é destino de replicação.



Você também pode definir essa propriedade ao criar ou clonar um volume.

Passos

1. Clique em **Management > volumes**.
2. Clique no ícone **ações** para o volume para o qual deseja ativar o SnapMirror.
3. No menu resultante, selecione **Editar**.
4. Na caixa de diálogo **Editar volume**, marque a caixa de seleção **Ativar SnapMirror**.
5. Clique em **Salvar alterações**.

Crie um endpoint SnapMirror

Você deve criar um ponto de extremidade do SnapMirror na IU do NetApp Element antes de criar um relacionamento.

Um ponto de extremidade do SnapMirror é um cluster do ONTAP que serve como destino de replicação para um cluster que executa o software Element. Antes de criar uma relação do SnapMirror, primeiro você cria um endpoint do SnapMirror.

Você pode criar e gerenciar até quatro pontos de extremidade SnapMirror em um cluster de storage que executa o software Element.



Se um endpoint existente foi originalmente criado usando a API e as credenciais não foram salvas, você pode ver o endpoint na IU do elemento e verificar sua existência, mas ele não pode ser gerenciado usando a IU do elemento. Esse endpoint só pode ser gerenciado usando a API Element.

Para obter detalhes sobre métodos de API, "[Gerencie o storage com a API Element](#)" consulte .

O que você vai precisar

- Você deve ter habilitado o SnapMirror na IU do Element para o cluster de storage.
- Você conhece as credenciais do ONTAP para o endpoint.

Passos

1. Clique em **proteção de dados > SnapMirror Endpoints**.
2. Clique em **Create Endpoint**.

3. Na caixa de diálogo **criar um novo ponto final**, insira o endereço IP de gerenciamento de cluster do sistema ONTAP.
4. Insira as credenciais de administrador do ONTAP associadas ao endpoint.
5. Rever detalhes adicionais:
 - LIFs: Lista as interfaces lógicas ONTAP entre clusters usadas para se comunicar com o elemento.
 - Status: Mostra o status atual do endpoint SnapMirror. Os valores possíveis são: Conetado, desconetado e não gerenciado.
6. Clique em **Create Endpoint**.

Crie uma relação SnapMirror

Você deve criar um relacionamento SnapMirror na IU do NetApp Element.



Quando um volume ainda não está ativado para o SnapMirror e você seleciona criar uma relação a partir da IU do Element, o SnapMirror é ativado automaticamente nesse volume.

O que você vai precisar

O SnapMirror está ativado no volume.

Passos

1. Clique em **Management > volumes**.
2. Clique no ícone **ações** para o volume que deve fazer parte da relação.
3. Clique em **criar uma relação SnapMirror**.
4. Na caixa de diálogo **criar um relacionamento SnapMirror**, selecione um ponto final na lista **ponto final**.
5. Selecione se a relação será criada usando um novo volume ONTAP ou um volume ONTAP existente.
6. Para criar um novo volume ONTAP na IU do Element, clique em **criar novo volume**.
 - a. Selecione **Storage Virtual Machine** para esta relação.
 - b. Selecione **agregar** na lista suspensa.
 - c. No campo **volume Name Suffix**, insira um sufixo.



O sistema detecta o nome do volume de origem e copia-o para o campo **Nome do volume**. O sufixo inserido anexa o nome.

- d. Clique em **criar volume de destino**.
7. Para usar um volume ONTAP existente, clique em **usar volume existente**.
 - a. Selecione **Storage Virtual Machine** para esta relação.
 - b. Selecione o volume que é o destino para esta nova relação.
 8. Na seção **Detalhes do relacionamento**, selecione uma política. Se a política selecionada tiver regras manter, a tabela regras exibirá as regras e os rótulos associados.
 9. **Opcional**: Selecione um horário.

Isso determina com que frequência a relação cria cópias.
 10. **Opcional**: No campo **Limit bandwidth to**, insira a quantidade máxima de largura de banda que pode ser

consumida pelas transferências de dados associadas a essa relação.

11. Rever detalhes adicionais:

- **Estado:** Estado da relação atual do volume de destino. Os valores possíveis são:
 - não inicializado: O volume de destino não foi inicializado.
 - Snapmirror: O volume de destino foi inicializado e está pronto para receber atualizações do SnapMirror.
 - Desagregação: O volume de destino é leitura/gravação e instantâneos estão presentes.
- **Status:** Status atual do relacionamento. Os valores possíveis são ociosos, transferindo, verificando, quiescente, quiesced, enfileirado, preparando, finalizando, abortando e quebrando.
- **Tempo de atraso:** A quantidade de tempo em segundos que o sistema de destino fica atrás do sistema de origem. O tempo de atraso não deve ser superior ao intervalo de programação de transferência.
- **Limite de largura de banda:** A quantidade máxima de largura de banda que pode ser consumida pelas transferências de dados associadas a essa relação.
- **Último transferido:** Carimbo de data/hora do último instantâneo transferido. Clique para obter mais informações.
- **Nome da política:** O nome da política ONTAP SnapMirror para o relacionamento.
- **Tipo de política:** Tipo de política ONTAP SnapMirror selecionada para o relacionamento. Os valores possíveis são:
 - async_mirror
 - mirror_vault
- **Nome da programação:** Nome da programação pré-existente no sistema ONTAP selecionado para esta relação.

12. Para não inicializar neste momento, certifique-se de que a caixa de verificação **Inicializar** não está selecionada.



A inicialização pode ser demorada. Você pode querer executar isso durante horas fora de pico. A inicialização executa uma transferência de linha de base; ela faz uma cópia instantânea do volume de origem, depois transfere essa cópia e todos os dados bloqueiam que ela faz referência ao volume de destino. Você pode inicializar manualmente ou usar uma programação para iniciar o processo de inicialização (e atualizações subsequentes) de acordo com a programação.

13. Clique em **criar relacionamento**.

14. Clique em **proteção de dados > relacionamentos SnapMirror** para visualizar esta nova relação SnapMirror.

Ações de relacionamento do SnapMirror

Você pode configurar um relacionamento na página relacionamentos do SnapMirror da guia proteção de dados. As opções do ícone ações são descritas aqui.

- **Editar:** Edita a política usada ou o cronograma para o relacionamento.
- **Excluir:** Exclui a relação do SnapMirror. Esta função não elimina o volume de destino.
- **Inicializar:** Realiza a primeira transferência inicial de dados para estabelecer uma nova relação.

- **Update:** Executa uma atualização sob demanda do relacionamento, replicando quaisquer novos dados e cópias Snapshot incluídas desde a última atualização para o destino.
- **Quiesce:** Impede quaisquer atualizações adicionais para um relacionamento.
- **Resume:** Retoma um relacionamento que é quiesced.
- **Break:** Faz o volume de destino ler-escrever e pára todas as transferências atuais e futuras. Determine se os clientes não estão usando o volume de origem original, porque a operação de ressincronização reversa faz o volume de origem original somente leitura.
- **Resync:** Restabelece um relacionamento quebrado na mesma direção antes da quebra ocorrer.
- **Reverse Resync:** Automatiza as etapas necessárias para criar e inicializar uma nova relação na direção oposta. Isso só pode ser feito se o relacionamento existente estiver em um estado quebrado. Esta operação não eliminará a relação atual. O volume de origem original reverte para a cópia Snapshot comum mais recente e ressincroniza com o destino. Todas as alterações feitas no volume de origem original desde a última atualização bem-sucedida do SnapMirror são perdidas. Quaisquer alterações feitas ou novos dados gravados no volume de destino atual são enviadas de volta ao volume de origem original.
- **Abort:** Cancela uma transferência atual em andamento. Se uma atualização do SnapMirror for emitida para uma relação abortada, a relação continuará com a última transferência do último ponto de verificação de reinício que foi criado antes da ocorrência do cancelamento.

Etiquetas SnapMirror

Um rótulo SnapMirror serve como um marcador para transferir um instantâneo especificado de acordo com as regras de retenção do relacionamento.

A aplicação de um rótulo a um instantâneo marca-o como um destino para a replicação do SnapMirror. A função da relação é impor as regras sobre a transferência de dados selecionando o instantâneo rotulado correspondente, copiando-o para o volume de destino e garantindo que o número correto de cópias seja mantido. Refere-se à política para determinar a contagem de manutenção e o período de retenção. A política pode ter qualquer número de regras e cada regra tem um rótulo exclusivo. Esse rótulo serve como o link entre o instantâneo e a regra de retenção.

É o rótulo SnapMirror que indica qual regra é aplicada para o instantâneo selecionado, instantâneo de grupo ou agendamento.

Adicione etiquetas SnapMirror a instantâneos

Os rótulos do SnapMirror especificam a política de retenção de snapshot no endpoint do SnapMirror. Você pode adicionar rótulos a snapshots e snapshots de grupo.

Você pode exibir rótulos disponíveis a partir de uma caixa de diálogo relacionamento SnapMirror existente ou do Gerenciador do sistema NetApp ONTAP.



Quando você adiciona um rótulo a um instantâneo de grupo, todos os rótulos existentes a snapshots individuais são substituídos.

O que você vai precisar

- O SnapMirror está ativado no cluster.
- O rótulo que você deseja adicionar já existe no ONTAP.

Passos

1. Clique na página **proteção de dados > instantâneos** ou **instantâneos de grupo**.
2. Clique no ícone **ações** para o instantâneo ou instantâneo de grupo ao qual deseja adicionar um rótulo SnapMirror.
3. Na caixa de diálogo **Editar captura Instantânea**, insira o texto no campo **Etiqueta SnapMirror**. O rótulo deve corresponder a um rótulo de regra na política aplicada à relação SnapMirror.
4. Clique em **Salvar alterações**.

Adicionar etiquetas SnapMirror a agendas de instantâneos

Você pode adicionar rótulos SnapMirror a agendas de instantâneos para garantir que uma política SnapMirror seja aplicada. É possível exibir rótulos disponíveis em uma caixa de diálogo de relacionamento do SnapMirror existente ou no Gerenciador de sistemas do NetAppONTAP.

O que você vai precisar

- O SnapMirror deve estar ativado no nível do cluster.
- O rótulo que você deseja adicionar já existe no ONTAP.

Passos

1. Clique em **proteção de dados > horários**.
2. Adicione um rótulo SnapMirror a um agendamento de uma das seguintes maneiras:

| Opção | Passos |
|--------------------------------------|---|
| Criando uma nova agenda | <ol style="list-style-type: none"> a. Selecione criar horário. b. Introduza todos os outros detalhes relevantes. c. Selecione criar horário. |
| Modificação do agendamento existente | <ol style="list-style-type: none"> a. Clique no ícone ações para a programação à qual deseja adicionar um rótulo e selecione Editar. b. Na caixa de diálogo resultante, insira o texto no campo Etiqueta SnapMirror. c. Selecione Salvar alterações. |

Encontre mais informações

[Criar uma agenda de instantâneos](#)

Recuperação de desastres usando o SnapMirror

No caso de um problema com um volume ou cluster que executa o software NetApp Element, use a funcionalidade SnapMirror para quebrar a relação e o failover para o volume de destino.



Se o cluster original tiver falhado completamente ou não existir, contacte o suporte da NetApp para obter mais assistência.

Executar um failover a partir de um cluster de Element

Você pode executar um failover do cluster Element para tornar o volume de destino leitura/gravação acessível a hosts no lado do destino. Antes de executar um failover a partir do cluster Element, é necessário interromper a relação do SnapMirror.

Use a IU do NetApp Element para executar o failover. Se a IU do Element não estiver disponível, você também poderá usar o Gerenciador de sistema do ONTAP ou a CLI do ONTAP para emitir o comando Break Relationship.

O que você vai precisar

- Existe uma relação SnapMirror e tem pelo menos um instantâneo válido no volume de destino.
- É necessário fazer failover para o volume de destino devido a uma interrupção não planejada ou evento planejado no local principal.

Passos

1. Na IU do Element, clique em **proteção de dados > relacionamentos SnapMirror**.
2. Encontre a relação com o volume de origem que você deseja fazer failover.
3. Clique no ícone **ações**.
4. Clique em **Break**.
5. Confirme a ação.

O volume no cluster de destino agora tem acesso de leitura e gravação e pode ser montado nos hosts de aplicações para retomar as cargas de trabalho de produção. Toda a replicação do SnapMirror é interrompida como resultado dessa ação. A relação mostra um estado de rutura.

Execute um failback para o elemento

Quando o problema no lado principal tiver sido atenuado, você deve ressincronizar o volume de origem original e fazer o failover de volta para o software NetApp Element. As etapas que você executa variam dependendo se o volume de origem original ainda existe ou se você precisa fazer o failback para um volume recém-criado.

Encontre mais informações

- [Execute um failback quando o volume de origem ainda existir](#)
- [Execute um failback quando o volume de origem não existir mais](#)
- [Cenários de failback do SnapMirror](#)

Cenários de failback do SnapMirror

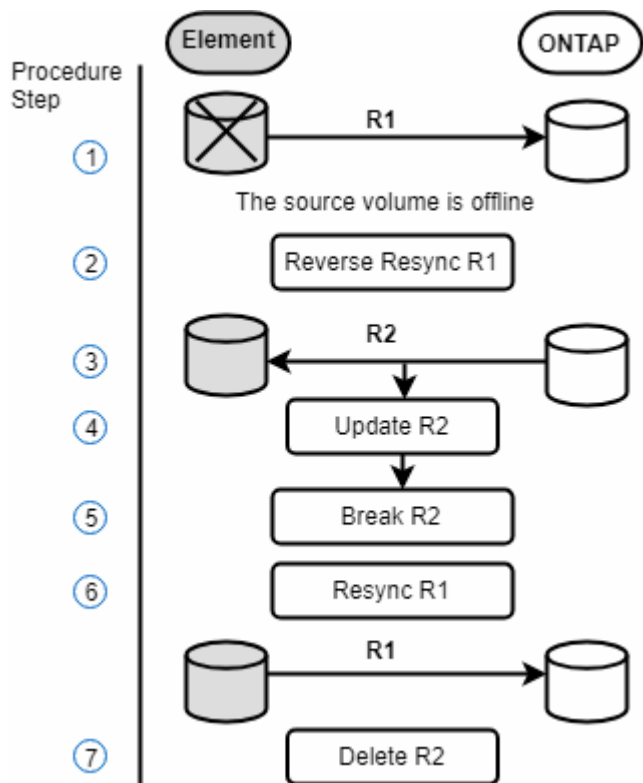
A funcionalidade de recuperação de desastres do SnapMirror é ilustrada em dois cenários de failback. Estes assumem que o relacionamento original foi falhado sobre (quebrado).

Os passos dos procedimentos correspondentes são adicionados para referência.

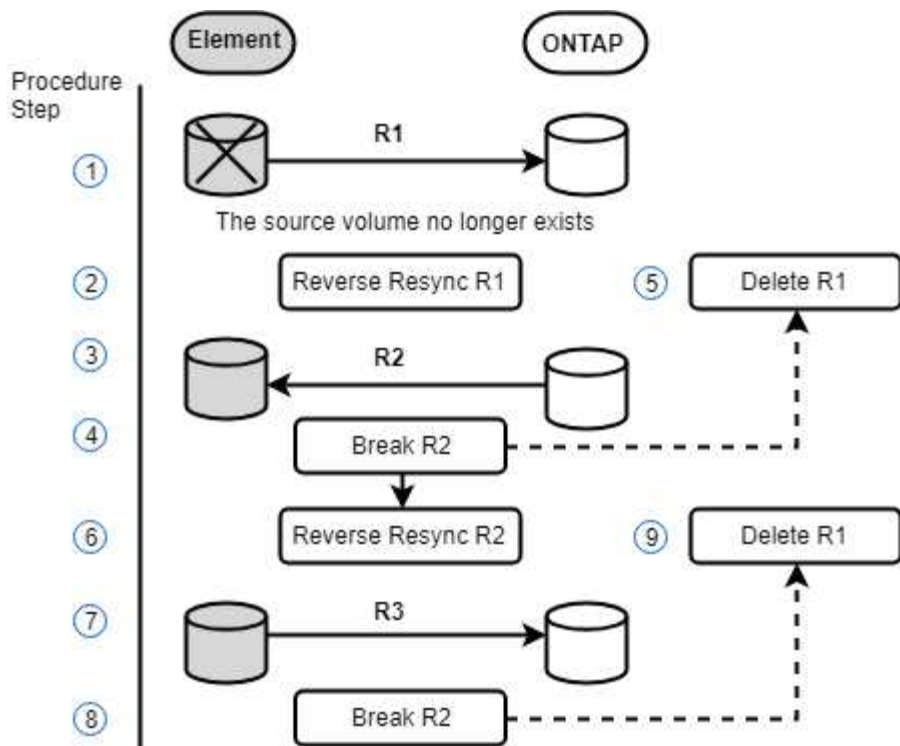


Nos exemplos aqui, R1 é a relação original em que o cluster que executa o software NetApp Element é o volume de origem original (elemento) e ONTAP é o volume de destino original (ONTAP). R2 e R3 representam as relações inversas criadas através da operação resincronizada reversa.

A imagem a seguir mostra o cenário de failback quando o volume de origem ainda existe:



A imagem a seguir mostra o cenário de failback quando o volume de origem não existe mais:



Encontre mais informações

- [Execute um failback quando o volume de origem ainda existir](#)
- [Execute um failback quando o volume de origem não existir mais](#)

Execute um failback quando o volume de origem ainda existir

Você pode ressincronizar o volume de origem original e fazer o failover usando a IU do NetApp Element. Este procedimento aplica-se a cenários em que o volume de origem original ainda existe.

1. Na IU do elemento, encontre a relação que você quebrou para executar o failover.
2. Clique no ícone ações e clique em **Reverse Resync**.
3. Confirme a ação.



A operação Reverse Resync cria uma nova relação na qual as funções dos volumes de origem e destino originais são revertidas (isso resulta em duas relações à medida que a relação original persiste). Todos os novos dados do volume de destino original são transferidos para o volume de origem original como parte da operação de ressincronização reversa. Você pode continuar acessando e gravando dados no volume ativo no lado do destino, mas precisará desconectar todos os hosts do volume de origem e executar uma atualização do SnapMirror antes de redirecionar para o primário original.

4. Clique no ícone ações do relacionamento inverso que você acabou de criar e clique em **Atualizar**.

Agora que você concluiu a ressincronização reversa e garantiu que não há sessões ativas conectadas ao volume no lado do destino e que os dados mais recentes estejam no volume principal original, você pode executar as seguintes etapas para concluir o failback e reativar o volume primário original:

5. Clique no ícone ações da relação inversa e clique em **Break**.
6. Clique no ícone ações do relacionamento original e clique em **Resync**.



O volume primário original agora pode ser montado para retomar as cargas de trabalho de produção no volume primário original. A replicação original do SnapMirror é retomada com base na política e na programação configurada para a relação.

7. Depois de confirmar que o status do relacionamento original é "snapmirror", clique no ícone ações do relacionamento inverso e clique em **Delete**.

Encontre mais informações

[Cenários de failback do SnapMirror](#)

Execute um failback quando o volume de origem não existir mais

Você pode ressincronizar o volume de origem original e fazer o failover usando a IU do NetApp Element. Esta seção se aplica a cenários em que o volume de origem original foi perdido, mas o cluster original ainda está intacto. Para obter instruções sobre como restaurar um novo cluster, consulte a documentação no site de suporte da NetApp.

O que você vai precisar

- Você tem uma relação de replicação descontínua entre os volumes Element e ONTAP.
- O volume do elemento é irremediavelmente perdido.
- O nome do volume original é apresentado como NÃO ENCONTRADO.

Passos

1. Na IU do elemento, encontre a relação que você quebrou para executar o failover.

*Prática recomendada: * Anote a política do SnapMirror e os detalhes do cronograma do relacionamento original com desagregação. Esta informação será necessária ao recriar a relação.

2. Clique no ícone **ações** e clique em **Reverse Resync**.
3. Confirme a ação.



A operação Reverse Resync cria uma nova relação na qual as funções do volume de origem original e do volume de destino são revertidas (isso resulta em duas relações à medida que a relação original persiste). Como o volume original não existe mais, o sistema cria um novo volume de elemento com o mesmo nome de volume e tamanho de volume que o volume de origem original. Ao novo volume é atribuída uma política de QoS padrão chamada sm-recovery e está associada a uma conta padrão chamada sm-recovery. Você vai querer editar manualmente a conta e a política de QoS para todos os volumes criados pelo SnapMirror para substituir os volumes de origem originais que foram destruídos.

Os dados do snapshot mais recente são transferidos para o novo volume como parte da operação de ressincronização reversa. Você pode continuar acessando e gravando dados no volume ativo no lado do destino, mas precisará desconectar todos os hosts do volume ativo e executar uma atualização do SnapMirror antes de restaurar o relacionamento principal original em uma etapa posterior. Depois de concluir a ressincronização inversa e garantir que não há sessões ativas conetadas ao volume no lado do destino e que os dados mais recentes estejam no volume principal original, continue com as etapas a

seguir para concluir o failback e reativar o volume primário original:

4. Clique no ícone **ações** da relação inversa que foi criada durante a operação Reverse Resync e clique em **Break**.
5. Clique no ícone **ações** da relação original, na qual o volume de origem não existe e clique em **Excluir**.
6. Clique no ícone **ações** da relação inversa, que você quebrou na etapa 4, e clique em **Reverse Resync**.
7. Isso inverte a origem e o destino e resulta em uma relação com a mesma fonte de volume e destino de volume que a relação original.
8. Clique no ícone **ações** e em **Editar** para atualizar esse relacionamento com as configurações originais de política de QoS e agendamento que você anotou.
9. Agora é seguro excluir a relação inversa que você reverte ressynced no passo 6.

Encontre mais informações

[Cenários de failback do SnapMirror](#)

Faça uma transferência ou migração única do ONTAP para o Element

Em geral, quando você usa o SnapMirror para recuperação de desastres de um cluster de storage SolidFire que executa o software NetApp Element para o software ONTAP, o Element é a origem e o ONTAP o destino. No entanto, em alguns casos, o sistema de storage ONTAP pode servir como origem e elemento como destino.

- Existem dois cenários:
 - Não existe nenhuma relação de recuperação de desastres anterior. Siga todas as etapas deste procedimento.
 - Existe uma relação anterior de recuperação de desastres, mas não entre os volumes que estão sendo usados para essa mitigação. Neste caso, siga apenas os passos 3 e 4 abaixo.

O que você vai precisar

- O nó de destino do elemento deve ter sido tornado acessível ao ONTAP.
- O volume do elemento deve ter sido habilitado para replicação do SnapMirror.

Você deve especificar o caminho de destino do elemento no formulário `hostip:/LUN/<id_number>`, onde `lun` é a cadeia real `"lun"` e `id_number` é a ID do volume do elemento.

Passos

1. Usando o ONTAP, crie a relação com o cluster Element:

```
snapmirror create -source-path SVM:volume|cluster://SVM/volume
-destination-path hostip:/lun/name -type XDP -schedule schedule -policy
policy
```

```
cluster_dst::> snapmirror create -source-path svm_1:volA_dst
-destination-path 10.0.0.11:/lun/0005 -type XDP -schedule my_daily
-policy MirrorLatest
```

2. Verifique se a relação SnapMirror foi criada usando o comando ONTAP `snapmirror show`.

Consulte as informações sobre como criar uma relação de replicação na documentação do ONTAP e para obter a sintaxe de comando completa, consulte a página de manual do ONTAP.

3. Usando a `ElementCreateVolume` API, crie o volume de destino e defina o modo de acesso ao volume de destino como `SnapMirror`:

Crie um volume de elemento usando a API `Element`

```
{
  "method": "CreateVolume",
  "params": {
    "name": "SMTargetVolumeTest2",
    "accountID": 1,
    "totalSize": 100000000000,
    "enable512e": true,
    "attributes": {},
    "qosPolicyID": 1,
    "enableSnapMirrorReplication": true,
    "access": "snapMirrorTarget"
  },
  "id": 1
}
```

4. Inicialize a relação de replicação usando o comando ONTAP `snapmirror initialize`:

```
snapmirror initialize -source-path hostip:/lun/name
-destination-path SVM:volume|cluster://SVM/volume
```

Faça backup e restaure volumes

Você pode fazer backup e restaurar volumes para outro storage SolidFire, bem como armazenamentos de objetos secundários que são compatíveis com Amazon S3 ou OpenStack Swift.

Ao restaurar volumes do OpenStack Swift ou Amazon S3, você precisa de informações de manifesto do processo de backup original. Se você estiver restaurando um volume que foi feito backup em um sistema de storage SolidFire, nenhuma informação de manifesto será necessária.

Encontre mais informações

- [Faça backup de um volume em um armazenamento de objetos do Amazon S3](#)
- [Faça backup de um volume para um armazenamento de objetos OpenStack Swift](#)
- [Fazer backup de um volume em um cluster de storage SolidFire](#)
- [Restaure um volume do backup em um armazenamento de objetos do Amazon S3](#)
- [Restaurar um volume do backup em um armazenamento de objetos OpenStack Swift](#)
- [Restaurar um volume do backup em um cluster de storage SolidFire](#)

Faça backup de um volume em um armazenamento de objetos do Amazon S3

Você pode fazer backup de volumes em armazenamentos de objetos externos compatíveis com o Amazon S3.

1. Clique em **Management > volumes**.
2. Clique no ícone ações do volume que você deseja fazer backup.
3. No menu resultante, clique em **Backup to**.
4. Na caixa de diálogo **Backup integrado** em **Backup to**, selecione **S3**.
5. Selecione uma opção em **Data Format**:
 - *** Nativo***: Um formato compactado legível apenas pelos sistemas de armazenamento SolidFire.
 - **Uncompressed**: Um formato não comprimido compatível com outros sistemas.
6. Insira um nome de host para usar para acessar o armazenamento de objetos no campo **Nome de host**.
7. Insira um ID de chave de acesso para a conta no campo **ID de chave de acesso**.
8. Digite a chave de acesso secreta para a conta no campo **chave de acesso secreta**.
9. Introduza o bucket S3 no qual pretende guardar a cópia de segurança no campo **S3 Bucket**.
10. Digite um nametag para anexar ao prefixo no campo **nametag**.
11. Clique em **Iniciar leitura**.

Faça backup de um volume para um armazenamento de objetos OpenStack Swift

Você pode fazer backup de volumes para armazenamentos de objetos externos compatíveis com o OpenStack Swift.

1. Clique em **Management > volumes**.
2. Clique no ícone ações do volume a ser feito backup.
3. No menu resultante, clique em **Backup to**.
4. Na caixa de diálogo **Backup integrado** em **Backup to**, selecione **Swift**.
5. Selecione um formato de dados em **Data Format**:
 - *** Nativo***: Um formato compactado legível apenas pelos sistemas de armazenamento SolidFire.
 - **Uncompressed**: Um formato não comprimido compatível com outros sistemas.
6. Insira um URL a ser usado para acessar o armazenamento de objetos no campo **URL**.
7. Introduza um nome de utilizador para a conta no campo **Nome de utilizador**.

8. Introduza a chave de autenticação da conta no campo **Authentication Key** (chave de autenticação).
9. Insira o recipiente no qual deseja armazenar o backup no campo **container**.
10. **Opcional:** Insira uma tag de nome para anexar ao prefixo no campo **nametag**.
11. Clique em **Iniciar leitura**.

Fazer backup de um volume em um cluster de storage SolidFire

É possível fazer backup de volumes que residem em um cluster remoto para clusters de storage que executam o software Element.

Certifique-se de que os clusters de origem e destino estejam emparelhados.

["Emparelhe clusters para replicação"](#) Consulte .

Ao fazer backup ou restaurar de um cluster para outro, o sistema gera uma chave para ser usada como autenticação entre os clusters. Essa chave de gravação de volume em massa permite que o cluster de origem se autentique com o cluster de destino, fornecendo um nível de segurança ao gravar no volume de destino. Como parte do processo de backup ou restauração, você precisa gerar uma chave de gravação de volume em massa a partir do volume de destino antes de iniciar a operação.

1. No cluster de destino, **Management > volumes**.
2. Clique no ícone ações do volume de destino.
3. No menu resultante, clique em **Restaurar de**.
4. Na caixa de diálogo **Restauração integrada**, em **Restaurar de**, selecione **SolidFire**.
5. Selecione uma opção em **Data Format**:
 - *** Nativo***: Um formato compactado legível apenas pelos sistemas de armazenamento SolidFire.
 - **Uncompressed**: Um formato não comprimido compatível com outros sistemas.
6. Clique em **Generate Key**.
7. Copie a chave da caixa **Bulk volume Write Key** para a área de transferência.
8. No cluster de origem, vá para **Management > volumes**.
9. Clique no ícone ações do volume a ser feito backup.
10. No menu resultante, clique em **Backup to**.
11. Na caixa de diálogo **Backup integrado** em **Backup to**, selecione **SolidFire**.
12. Selecione a mesma opção selecionada anteriormente no campo **Data Format**.
13. Introduza o endereço IP virtual de gestão do cluster do volume de destino no campo **Remote Cluster MVIP**.
14. Introduza o nome de utilizador do cluster remoto no campo **Nome de utilizador do cluster remoto**.
15. Introduza a palavra-passe do cluster remoto no campo **Palavra-passe do cluster remoto**.
16. No campo **Bulk volume Write Key** (chave de gravação de volume em massa), cole a chave que você gerou no cluster de destino anteriormente.
17. Clique em **Iniciar leitura**.

Restaure um volume do backup em um armazenamento de objetos do Amazon S3

Você pode restaurar um volume de um backup em um armazenamento de objetos do Amazon S3.

1. Clique em **Reporting > Event Log**.
2. Localize o evento de backup que criou o backup que você precisa restaurar.
3. Na coluna **Detalhes** do evento, clique em **Mostrar Detalhes**.
4. Copie as informações do manifesto para a área de transferência.
5. Clique em **Management > volumes**.
6. Clique no ícone ações do volume que deseja restaurar.
7. No menu resultante, clique em **Restaurar de**.
8. Na caixa de diálogo **Restauração integrada** em **Restaurar de**, selecione **S3**.
9. Selecione a opção que corresponde ao backup em **Data Format**:
 - *** Nativo***: Um formato compactado legível apenas pelos sistemas de armazenamento SolidFire.
 - **Uncompressed**: Um formato não comprimido compatível com outros sistemas.
10. Insira um nome de host para usar para acessar o armazenamento de objetos no campo **Nome de host**.
11. Insira um ID de chave de acesso para a conta no campo **ID de chave de acesso**.
12. Digite a chave de acesso secreta para a conta no campo **chave de acesso secreta**.
13. Introduza o bucket S3 no qual pretende guardar a cópia de segurança no campo **S3 Bucket**.
14. Cole as informações do manifesto no campo **MANIFEST**.
15. Clique em **Start Write** (Iniciar gravação).

Restaurar um volume do backup em um armazenamento de objetos OpenStack Swift

Você pode restaurar um volume de um backup em um armazenamento de objetos OpenStack Swift.

1. Clique em **Reporting > Event Log**.
2. Localize o evento de backup que criou o backup que você precisa restaurar.
3. Na coluna **Detalhes** do evento, clique em **Mostrar Detalhes**.
4. Copie as informações do manifesto para a área de transferência.
5. Clique em **Management > volumes**.
6. Clique no ícone ações do volume que deseja restaurar.
7. No menu resultante, clique em **Restaurar de**.
8. Na caixa de diálogo **Restauração integrada** em **Restaurar de**, selecione **Swift**.
9. Selecione a opção que corresponde ao backup em **Data Format**:
 - *** Nativo***: Um formato compactado legível apenas pelos sistemas de armazenamento SolidFire.
 - **Uncompressed**: Um formato não comprimido compatível com outros sistemas.
10. Insira um URL a ser usado para acessar o armazenamento de objetos no campo **URL**.
11. Introduza um nome de utilizador para a conta no campo **Nome de utilizador**.

12. Introduza a chave de autenticação da conta no campo **Authentication Key** (chave de autenticação).
13. Digite o nome do contentor no qual o backup é armazenado no campo **container**.
14. Cole as informações do manifesto no campo **MANIFEST**.
15. Clique em **Start Write** (Iniciar gravação).

Restaurar um volume do backup em um cluster de storage SolidFire

É possível restaurar um volume a partir de um backup em um cluster de storage do SolidFire.

Ao fazer backup ou restaurar de um cluster para outro, o sistema gera uma chave para ser usada como autenticação entre os clusters. Essa chave de gravação de volume em massa permite que o cluster de origem se autentique com o cluster de destino, fornecendo um nível de segurança ao gravar no volume de destino. Como parte do processo de backup ou restauração, você precisa gerar uma chave de gravação de volume em massa a partir do volume de destino antes de iniciar a operação.

1. No cluster de destino, clique em **Management > volumes**.
2. Clique no ícone ações do volume que deseja restaurar.
3. No menu resultante, clique em **Restaurar de**.
4. Na caixa de diálogo **Restauração integrada**, em **Restaurar de**, selecione **SolidFire**.
5. Selecione a opção que corresponde ao backup em **Data Format**:
 - *** Nativo***: Um formato compactado legível apenas pelos sistemas de armazenamento SolidFire.
 - **Uncompressed**: Um formato não comprimido compatível com outros sistemas.
6. Clique em **Generate Key**.
7. Copie a informação **Bulk volume Write Key** para a área de transferência.
8. No cluster de origem, clique em **Management > volumes**.
9. Clique no ícone ações do volume que você deseja usar para a restauração.
10. No menu resultante, clique em **Backup to**.
11. Na caixa de diálogo **Backup integrado**, selecione **SolidFire** em **Backup para**.
12. Selecione a opção que corresponde ao backup em **Data Format**.
13. Introduza o endereço IP virtual de gestão do cluster do volume de destino no campo **Remote Cluster MVIP**.
14. Introduza o nome de utilizador do cluster remoto no campo **Nome de utilizador do cluster remoto**.
15. Introduza a palavra-passe do cluster remoto no campo **Palavra-passe do cluster remoto**.
16. Cole a chave da área de transferência no campo **Bulk volume Write Key**.
17. Clique em **Iniciar leitura**.

Solucionar problemas do sistema

Deve monitorizar o sistema para fins de diagnóstico e obter informações sobre as tendências de desempenho e os Estados de várias operações do sistema. Talvez seja necessário substituir nós ou SSDs para fins de manutenção.

- ["Ver informações sobre eventos do sistema"](#)
- ["Exibir o status das tarefas em execução"](#)
- ["Ver alertas do sistema"](#)
- ["Visualizar a atividade de performance do nó"](#)
- ["Ver o desempenho do volume"](#)
- ["Ver sessões iSCSI"](#)
- ["Ver sessões Fibre Channel"](#)
- ["Solucionar problemas de unidades"](#)
- ["Solucionar problemas de nós"](#)
- ["Trabalhar com utilitários por nó para nós de storage"](#)
- ["Trabalhe com o nó de gerenciamento"](#)
- ["Entenda os níveis de plenitude do cluster"](#)

Para mais informações

- ["Documentação do software SolidFire e Element"](#)
- ["Plug-in do NetApp Element para vCenter Server"](#)

Ver informações sobre eventos do sistema

Pode visualizar informações sobre vários eventos detetados no sistema. O sistema atualiza as mensagens de eventos a cada 30 segundos. O log de eventos exibe os principais eventos do cluster.

1. Na IU do elemento, selecione **Reporting > Event Log**.

Para cada evento, você verá as seguintes informações:

| Item | Descrição |
|----------------|---|
| ID | ID exclusivo associado a cada evento. |
| Tipo de evento | O tipo de evento sendo registrado, por exemplo, eventos de API ou eventos de clone. |
| Mensagem | Mensagem associada ao evento. |
| Detalhes | Informações que ajudam a identificar por que o evento ocorreu. |
| ID de serviço | O serviço que relatou o evento (se aplicável). |
| Nó | O nó que relatou o evento (se aplicável). |

| | |
|----------------|--|
| ID da unidade | A unidade que relatou o evento (se aplicável). |
| Hora do evento | A hora em que o evento ocorreu. |

Encontre mais informações

[Tipos de eventos](#)

Tipos de eventos

O sistema relata vários tipos de eventos; cada evento é uma operação concluída pelo sistema. Os eventos podem ser de rotina, eventos normais ou eventos que exigem atenção do administrador. A coluna tipos de eventos na página Registro de eventos indica em qual parte do sistema o evento ocorreu.



O sistema não Registra comandos de API somente leitura no log de eventos.

A lista a seguir descreve os tipos de eventos que aparecem no log de eventos:

- **ApiEvent**

Eventos iniciados por um usuário por meio de uma API ou IU da Web que modificam as configurações.

- **BinAssignmentsEvent**

Eventos relacionados à atribuição de compartimentos de dados. Os compartimentos são essencialmente contentores que armazenam dados e são mapeados no cluster.

- **BinSyncEvent**

Eventos do sistema relacionados a uma reatribuição de dados entre serviços de bloco.

- **BsCheckEvent**

Eventos do sistema relacionados a verificações de serviço de bloqueio.

- **BsKillEvent**

Eventos do sistema relacionados às terminações de serviço de bloqueio.

- **BulkOpEvent**

Eventos relacionados a operações realizadas em um volume inteiro, como backup, restauração, snapshot ou clone.

- **CloneEvent**

Eventos relacionados à clonagem de volumes.

- **ClusterMasterEvent**

Eventos que aparecem após a inicialização do cluster ou após alterações de configuração no cluster,

como adicionar ou remover nós.

- **CsumEvent**

Eventos relacionados a somas de verificação de dados inválidas no disco.

- **DataEvent**

Eventos relacionados à leitura e escrita de dados.

- **DbEvent**

Eventos relacionados ao banco de dados global mantido por nós de ensemble no cluster.

- **DriveEvent**

Eventos relacionados às operações de acionamento.

- **CriptoporAtRestEvent**

Eventos relacionados ao processo de criptografia em um cluster.

- **EnsembleEvent**

Eventos relacionados ao aumento ou diminuição do número de nós em um ensemble.

- **FibreChannelEvent**

Eventos relacionados com a configuração e as conexões com os nós.

- **GcEvent**

Eventos relacionados a processos são executados a cada 60 minutos para recuperar o storage em unidades de bloco. Esse processo também é conhecido como coleta de lixo.

- **leEvent**

Erro interno do sistema.

- **InstallEvent**

Eventos de instalação automática de software. O software está sendo instalado automaticamente em um nó pendente.

- **ISCSIEvent**

Eventos relacionados com problemas iSCSI no sistema.

- **LimitEvent**

Eventos relacionados ao número de volumes ou volumes virtuais em uma conta ou no cluster que se aproxima do máximo permitido.

- **ManutençãoModeEvent**

Eventos relacionados ao modo de manutenção do nó, como desabilitar o nó.

- **NetworkEvent**

Eventos relacionados ao status da rede virtual.

- **PlatformHardwareEvent**

Eventos relacionados a problemas detetados em dispositivos de hardware.

- **RemoteClusterEvent**

Eventos relacionados com o emparelhamento remoto do cluster.

- **AgendadorEvent**

Eventos relacionados a instantâneos programados.

- **ServiceEvent**

Eventos relacionados com o estado do serviço do sistema.

- **SliceEvent**

Eventos relacionados ao Slice Server, como a remoção de uma unidade ou volume de metadados.

Existem três tipos de eventos de reatribuição de cortes, que incluem informações sobre o serviço em que um volume é atribuído:

- inversão: alterando o serviço primário para um novo serviço primário

```
sliceID oldPrimaryServiceID->newPrimaryServiceID
```

- movendo: mudando o serviço secundário para um novo serviço secundário

```
sliceID {oldSecondaryServiceID(s)}->{newSecondaryServiceID(s)}
```

- eliminação: removendo um volume de um conjunto de serviços

```
sliceID {oldSecondaryServiceID(s)}
```

- **SnmptTrapEvent**

Eventos relacionados a traps SNMP.

- **StatEvent**

Eventos relacionados com estatísticas do sistema.

- **TsEvent**

Eventos relacionados com o serviço de transporte do sistema.

- **UnexpectedException**

Eventos relacionados a exceções inesperadas do sistema.

- **UreEvent**

Eventos relacionados a erros de leitura irrecuperáveis que ocorrem durante a leitura a partir do dispositivo de armazenamento.

- **VasaProviderEvent**

Eventos relacionados a um provedor VASA (vSphere APIs for Storage Awareness).

Exibir o status das tarefas em execução

Você pode ver o status de progresso e conclusão das tarefas em execução na IU da Web que estão sendo relatadas pelos métodos de API ListSyncJobs e ListBulkVolumeJobs. Você pode acessar a página tarefas em execução na guia relatórios da IU do elemento.

Se houver um grande número de tarefas, o sistema pode colocá-las em fila e executá-las em lotes. A página tarefas em execução exibe os serviços que estão sendo sincronizados no momento. Quando uma tarefa é concluída, ela é substituída pela próxima tarefa de sincronização na fila. A sincronização de tarefas pode continuar a aparecer na página tarefas em execução até que não haja mais tarefas a serem concluídas.



Você pode ver os dados de sincronizações de replicação para volumes em replicação na página tarefas em execução do cluster que contém o volume de destino.

Ver alertas do sistema

Pode visualizar alertas para obter informações sobre avarias ou erros do cluster no sistema. Os alertas podem ser informações, avisos ou erros e são um bom indicador de quão bem o cluster está funcionando. A maioria dos erros resolve-se automaticamente.

Você pode usar o método ListClusterFaults API para automatizar o monitoramento de alertas. Isso permite que você seja notificado sobre todos os alertas que ocorrem.

1. Na IU do elemento, selecione **Reporting > Alerts**.

O sistema atualiza os alertas na página a cada 30 segundos.

Para cada evento, você verá as seguintes informações:

| Item | Descrição |
|------|--|
| ID | ID exclusiva associada a um alerta de cluster. |

| | |
|----------------|---|
| Gravidade | O grau de importância do alerta. Valores possíveis: <ul style="list-style-type: none"> • Aviso: Um problema menor que em breve pode exigir atenção. Atualizações do sistema ainda são permitidas. • Erro: Uma falha que pode causar degradação no desempenho ou perda de alta disponibilidade (HA). Erros geralmente não devem afetar o serviço de outra forma. • Crítico: Uma falha grave que afeta o serviço. O sistema não consegue atender a solicitações de e/S de API ou cliente. Operar neste estado pode levar a uma perda potencial de dados. • BestPractice: Uma prática recomendada de configuração do sistema não está sendo usada. |
| Tipo | O elemento que afeta a avaria. Pode ser nó, unidade, cluster, serviço ou volume. |
| Nó | ID do nó para o nó a que esta avaria se refere. Incluído para falhas de nó e unidade, caso contrário definido como - (traço). |
| ID da unidade | ID da unidade para a unidade à qual esta avaria se refere. Incluído para falhas de condução, caso contrário definido para - (tablier). |
| Código de erro | Um código descritivo que indica o que causou a falha. |
| Detalhes | Uma descrição da avaria com detalhes adicionais. |
| Data | A data e a hora em que a avaria foi registada. |

2. Clique em **Mostrar Detalhes** para obter um alerta individual para visualizar informações sobre o alerta.
3. Para ver os detalhes de todos os alertas na página, clique na coluna Detalhes.

Depois que o sistema resolver um alerta, todas as informações sobre o alerta, incluindo a data em que foi resolvido, são movidas para a área resolvida.

Encontre mais informações

- [Códigos de falha do cluster](#)
- ["Gerencie o storage com a API Element"](#)

Códigos de falha do cluster

O sistema relata um erro ou um estado que pode ser de interesse gerando um código de

falha, que está listado na página Alertas. Esses códigos ajudam a determinar qual componente do sistema experimentou o alerta e por que o alerta foi gerado.

A lista a seguir descreve os diferentes tipos de códigos:

- **AuthenticationServiceFault**

O Serviço de autenticação em um ou mais nós de cluster não está funcionando como esperado.

Entre em Contato com o suporte da NetApp para obter assistência.

- **DisponívelVirtualNetworkIPAddressLow**

O número de endereços de rede virtual no bloco de endereços IP é baixo.

Para resolver essa falha, adicione mais endereços IP ao bloco de endereços de rede virtual.

- **BlockClusterFull**

Não há espaço de armazenamento em bloco suficiente para suportar uma perda de nó único. Consulte o método da API GetClusterFullThreshold para obter detalhes sobre os níveis de plenitude do cluster. Esta avaria no grupo de instrumentos indica uma das seguintes condições:

- stage3Low (Aviso): O limite definido pelo usuário foi cruzado. Ajuste as configurações de Cluster Full ou adicione mais nós.
- stage4Critical (erro): Não há espaço suficiente para recuperar de uma falha de 1 nós. A criação de volumes, snapshots e clones não é permitida.
- stage5CompletelyConsumed (crítico)¹; não são permitidas gravações ou novas ligações iSCSI. As conexões iSCSI atuais serão mantidas. As gravações falharão até que mais capacidade seja adicionada ao cluster. Para resolver essa falha, limpe ou exclua volumes ou adicione outro nó de armazenamento ao cluster de armazenamento.

- **BlocksDegraded**

Os dados de bloco não são mais totalmente replicados devido a uma falha.

| Gravidade | Descrição |
|-----------|---|
| Aviso | Apenas duas cópias completas dos dados de bloco são acessíveis. |
| Erro | Apenas uma única cópia completa dos dados do bloco é acessível. |
| Crítico | Não há cópias completas dos dados de bloco acessíveis. |

Nota: o estado de aviso só pode ocorrer num sistema Triple Helix.

Para resolver essa falha, restaure quaisquer nós off-line ou bloqueie serviços ou entre em Contato com o suporte da NetApp para obter assistência.

- **BlockServiceTooFull**

Um serviço de bloco está usando muito espaço.

Para resolver essa falha, adicione mais capacidade provisionada.

• **BlockServiceUnHealthy**

Um serviço de bloco foi detetado como não saudável:

- Aviso: Nenhuma ação é tomada. Este período de aviso expirará em `cTimeUntilBSIsKilledMSec`: 330000 milissegundos.
- Gravidade: O sistema está desativando automaticamente os dados e replicando novamente seus dados para outras unidades íntegras.
- Gravidade Crítica: Há serviços de bloco com falha em vários nós maiores ou iguais à contagem de replicação (2 para hélice dupla). Os dados não estão disponíveis e a sincronização do bin não será concluída. Verifique se há problemas de conectividade de rede e erros de hardware. Haverá outras falhas se os componentes de hardware específicos tiverem falhado. A falha será apagada quando o serviço de bloco estiver acessível ou quando o serviço tiver sido desativado.

• **ClockSkewExceedsFaultThreshold**

O desvio de tempo entre o mestre de cluster e o nó que está apresentando um token excede o limite recomendado. O cluster de storage não pode corrigir o desvio de tempo entre os nós automaticamente.

Para resolver essa falha, use servidores NTP internos à sua rede, em vez dos padrões de instalação. Se estiver a utilizar um servidor NTP interno, contacte o suporte da NetApp para obter assistência.

• **ClusterCannotSync**

Há uma condição de espaço fora e os dados nas unidades de armazenamento de bloco off-line não podem ser sincronizados com unidades que ainda estão ativas.

Para resolver essa falha, adicione mais armazenamento.

• **Incluído**

Não há mais espaço de armazenamento livre no cluster de armazenamento.

Para resolver essa falha, adicione mais armazenamento.

• **ClusterIOPSAreOverProvisioned**

As IOPS do cluster estão provisionadas em excesso. A soma de todas as IOPS mínimas de QoS é maior do que as IOPS esperadas do cluster. A QoS mínima não pode ser mantida para todos os volumes simultaneamente.

Para resolver esse problema, reduza as configurações mínimas de IOPS de QoS para volumes.

• **DisableDriveSecurityFailed**

O cluster não está configurado para ativar a segurança da unidade (criptografia em repouso), mas pelo menos uma unidade tem a segurança da unidade ativada, o que significa que a desativação da segurança da unidade nessas unidades falhou. Esta avaria é registada com a gravidade ""Aviso"".

Para resolver esta avaria, verifique os detalhes da avaria para o motivo pelo qual a segurança da unidade não pode ser desativada. Possíveis razões são:

- Não foi possível adquirir a chave de encriptação, investigue o problema com o acesso à chave ou ao servidor de chaves externo.
- A operação de desativação falhou na unidade, determine se a chave errada poderia ter sido adquirida. Se nenhum destes for o motivo da falha, a unidade pode precisar ser substituída.

Você pode tentar recuperar uma unidade que não desabilite a segurança com êxito mesmo quando a chave de autenticação correta é fornecida. Para executar esta operação, remova a(s) unidade(s) do sistema movendo-a para disponível, execute uma eliminação segura na unidade e mova-a de volta para Ativo.

• **DisconnectedClusterPair**

Um par de cluster está desconetado ou configurado incorretamente. Verifique a conectividade de rede entre os clusters.

• **DisconnectedRemoteNode**

Um nó remoto está desconetado ou configurado incorretamente. Verifique a conectividade de rede entre os nós.

• **DisconnectedSnapMirrorEndpoint**

Um endpoint SnapMirror remoto está desconetado ou configurado incorretamente. Verifique a conectividade de rede entre o cluster e o SnapMirrorEndpoint remoto.

• **DriveAvailable**

Uma ou mais unidades estão disponíveis no cluster. Em geral, todos os clusters devem ter todas as unidades adicionadas e nenhuma no estado disponível. Se esta avaria aparecer inesperadamente, contacte o suporte da NetApp.

Para resolver essa falha, adicione todas as unidades disponíveis ao cluster de armazenamento.

• **DriveFailed**

O cluster retorna essa falha quando uma ou mais unidades falharam, indicando uma das seguintes condições:

- O gestor de unidades não consegue aceder à unidade.
- O serviço de corte ou bloco falhou muitas vezes, presumivelmente por causa de falhas de leitura ou gravação da unidade e não pode ser reiniciado.
- A unidade está ausente.
- O serviço mestre para o nó está inacessível (todas as unidades no nó são consideradas ausentes/com falha).
- A unidade está bloqueada e a chave de autenticação da unidade não pode ser adquirida.
- A unidade está bloqueada e a operação de desbloqueio falha. Para resolver este problema:
- Verifique a conectividade de rede para o nó.
- Substitua a unidade.
- Certifique-se de que a chave de autenticação está disponível.

• **DriveHealthFault**

Uma unidade falhou na verificação INTELIGENTE de integridade e, como resultado, as funções da unidade são diminuídas. Existe um nível crítico de gravidade para esta avaria:

- Unidade com série: <serial number> in slot: <node slot> <drive slot> falhou a verificação geral INTELIGENTE de integridade. Para resolver esta avaria, substitua a unidade.

• **DriveWearFault**

A vida útil restante de uma unidade caiu abaixo dos limites, mas ainda está funcionando. Existem dois níveis de gravidade possíveis para esta falha: Crítico e Aviso:

- Unidade com série: <serial number> in slot: <node slot> <drive slot> tem níveis críticos de desgaste.
- Unidade com série: <serial number> in slot: <node slot> <drive slot> tem baixas reservas de desgaste. Para resolver esta avaria, substitua a unidade em breve.

• **DuplicateClusterMasterCandidates**

Mais de um candidato mestre do cluster de armazenamento foi detetado. Entre em Contato com o suporte da NetApp para obter assistência.

• **EnableDriveSecurityFailed**

O cluster está configurado para exigir segurança da unidade (criptografia em repouso), mas a segurança da unidade não pôde ser ativada em pelo menos uma unidade. Esta avaria é registada com a gravidade ""Aviso"".

Para resolver esta avaria, verifique os detalhes da avaria para o motivo pelo qual a segurança da unidade não pôde ser ativada. Possíveis razões são:

- Não foi possível adquirir a chave de encriptação, investigue o problema com o acesso à chave ou ao servidor de chaves externo.
- A operação de ativação falhou na unidade, determine se a chave errada poderia ter sido adquirida. Se nenhum destes for o motivo da falha, a unidade pode precisar ser substituída.

Você pode tentar recuperar uma unidade que não habilite a segurança com êxito mesmo quando a chave de autenticação correta é fornecida. Para executar esta operação, remova a(s) unidade(s) do sistema movendo-a para disponível, execute uma eliminação segura na unidade e mova-a de volta para Ativo.

• **EnsembleDegraded**

A conectividade ou a energia da rede foi perdida para um ou mais nós do ensemble.

Para resolver esta avaria, restaure a conectividade ou a alimentação da rede.

• **exceção**

Uma avaria comunicada que não é uma avaria de rotina. Estas avarias não são eliminadas automaticamente da fila de avarias. Entre em Contato com o suporte da NetApp para obter assistência.

• **FailedSpaceToFull**

Um serviço de bloco não está respondendo às solicitações de gravação de dados. Isto faz com que o serviço de corte fique sem espaço para armazenar gravações com falha.

Para resolver esta avaria, restaure a funcionalidade de serviços de bloco para permitir que as gravações continuem normalmente e que o espaço com falha seja eliminado do serviço de corte.

- **FanSensor**

Um sensor da ventoinha falhou ou está em falta.

Para resolver essa falha, substitua qualquer hardware com falha.

- **FibreChannelAccessDegraded**

Um nó Fibre Channel não responde a outros nós no cluster de storage durante seu IP de storage por um período de tempo. Nesse estado, o nó será considerado não responsivo e gerará uma falha de cluster. Verifique a conectividade da rede.

- **FibreChannelAccessUnavailable**

Todos os nós do Fibre Channel não respondem. As IDs de nó são exibidas. Verifique a conectividade da rede.

- **FibreChannelActiveIxl**

A contagem IXL Nexus está se aproximando do limite suportado de 8000 sessões ativas por nó Fibre Channel.

- O limite de melhores práticas é 5500.
- O limite de aviso é 7500.
- O limite máximo (não aplicado) é 8192. Para resolver essa falha, reduza a contagem IXL Nexus abaixo do limite de melhores práticas de 5500.

- **FibreChannelConfig**

Esta avaria no grupo de instrumentos indica uma das seguintes condições:

- Há uma porta Fibre Channel inesperada em um slot PCI.
- Existe um modelo HBA Fibre Channel inesperado.
- Existe um problema com o firmware de um HBA Fibre Channel.
- Uma porta Fibre Channel não está online.
- Há um problema persistente na configuração de passagem Fibre Channel. Entre em Contato com o suporte da NetApp para obter assistência.

- **FibreChannelIOPS**

A contagem total de IOPS está se aproximando do limite de IOPS para nós Fibre Channel no cluster. Os limites são:

- FC0025: Limite de 450K IOPS a um tamanho de bloco de 4K PB por nó Fibre Channel.
- FCN001: Limite de 625K OPS a 4K tamanho de bloco por nó Fibre Channel. Para resolver essa falha, equilibre a carga em todos os nós Fibre Channel disponíveis.

- **FibreChannelStaticIxl**

A contagem IXL Nexus está se aproximando do limite suportado de 16000 sessões estáticas por nó Fibre Channel.

- O limite de melhores práticas é 11000.

- O limite de aviso é 15000.
- O limite máximo (imposto) é 16384. Para resolver essa falha, reduza a contagem IXL Nexus abaixo do limite de melhores práticas de 11000.

• **FileSystemCapacityLow**

Há espaço insuficiente em um dos sistemas de arquivos.

Para resolver essa falha, adicione mais capacidade ao sistema de arquivos.

• **FipsDrivesMismatch**

Uma unidade não FIPS foi fisicamente inserida em um nó de storage com capacidade FIPS ou uma unidade FIPS foi fisicamente inserida em um nó de storage não FIPS. Uma única falha é gerada por nó e lista todas as unidades afetadas.

Para resolver esta avaria, remova ou substitua a unidade ou unidades incompatíveis em questão.

• **FipsDrivesOutOfCompliance**

O sistema detetou que a encriptação em repouso foi desativada após a funcionalidade de unidades FIPS estar ativada. Essa falha também é gerada quando o recurso unidades FIPS está ativado e uma unidade ou nó não FIPS está presente no cluster de storage.

Para resolver esta avaria, ative a encriptação em repouso ou remova o hardware não FIPS do cluster de armazenamento.

• **FipsSelfTestFailure**

O subsistema FIPS detetou uma falha durante o autoteste.

Entre em Contato com o suporte da NetApp para obter assistência.

• **HardwareConfigMismatch**

Esta avaria no grupo de instrumentos indica uma das seguintes condições:

- A configuração não corresponde à definição do nó.
- Existe um tamanho de unidade incorreto para este tipo de nó.
- Foi detetada uma unidade não suportada. Uma possível razão é que a versão do elemento instalado não reconhece esta unidade. Recomendamos a atualização do software Element neste nó.
- Há uma incompatibilidade de firmware da unidade.
- O estado capaz de encriptação da unidade não corresponde ao nó. Entre em Contato com o suporte da NetApp para obter assistência.

• **IdPCertificateExpiration**

O certificado SSL do provedor de serviços do cluster para uso com um provedor de identidade de terceiros (IDP) está prestes a expirar ou já expirou. Esta avaria utiliza as seguintes gravidades com base na urgência:

| Gravidade | Descrição |
|-----------|-----------|
|-----------|-----------|

| | |
|---------|--|
| Aviso | O certificado expira dentro de 30 dias. |
| Erro | O certificado expira dentro de 7 dias. |
| Crítico | O certificado expira dentro de 3 dias ou já expirou. |

Para resolver esta avaria, atualize o certificado SSL antes de expirar. Use o método `UpdateIpdConfiguration API` com `refreshCertificateExpirationTime=true` para fornecer o certificado SSL atualizado.

- **InconsistentBondModes**

Os modos de ligação no dispositivo VLAN estão em falta. Esta avaria apresenta o modo de ligação esperado e o modo de ligação atualmente em utilização.

- **InconsistentInterfaceConfiguration**

A configuração da interface é incoerente.

Para resolver essa falha, verifique se as interfaces de nós no cluster de storage estão configuradas de forma consistente.

- **InconsistentMtus**

Esta avaria no grupo de instrumentos indica uma das seguintes condições:

- Bond1G incompatibilidade: MTUs inconsistentes foram detetadas em interfaces Bond1G.
- Bond10G incompatibilidade: MTUs inconsistentes foram detetadas em interfaces Bond10G. Esta falha exhibe o nó ou nós em questão junto com o valor MTU associado.

- **InconsistentRoutingRules**

As regras de roteamento para essa interface são inconsistentes.

- **InconsistentSubnetMasks**

A máscara de rede no dispositivo VLAN não corresponde à máscara de rede gravada internamente para a VLAN. Esta avaria apresenta a máscara de rede esperada e a máscara de rede atualmente em utilização.

- **IncorretBondPortCount**

O número de portas de ligação está incorreto.

- **InvalidConfiguredFibredChannelNodeCount**

Uma das duas conexões de nó Fibre Channel esperadas está degradada. Esta avaria aparece quando apenas um nó de canal de fibra está ligado.

Para resolver essa falha, verifique a conectividade de rede do cluster e o cabeamento de rede e verifique se há serviços com falha. Se não houver problemas de rede ou de serviço, entre em Contato com o suporte da NetApp para uma substituição de nó Fibre Channel.

- **IrqBalanceFailed**

Ocorreu uma exceção ao tentar equilibrar interrupções.

Entre em Contato com o suporte da NetApp para obter assistência.

• **KmipCertificateFault**

- O certificado da Autoridade de Certificação raiz (CA) está próximo da expiração.

Para resolver essa falha, adquira um novo certificado da CA raiz com data de expiração de pelo menos 30 dias e use `ModifyKeyServerKmip` para fornecer o certificado de CA raiz atualizado.

- O certificado do cliente está próximo da expiração.

Para resolver essa falha, crie uma nova CSR usando `GetClientCertificateSigningRequest`, peça que ela assine garantindo que a nova data de expiração esteja de pelo menos 30 dias e use `ModifyKeyServerKmip` para substituir o certificado de cliente KMIP que expira pelo novo certificado.

- O certificado de autoridade de certificação raiz (CA) expirou.

Para resolver essa falha, adquira um novo certificado da CA raiz com data de expiração de pelo menos 30 dias e use `ModifyKeyServerKmip` para fornecer o certificado de CA raiz atualizado.

- O certificado de cliente expirou.

Para resolver essa falha, crie uma nova CSR usando `GetClientCertificateSigningRequest`, faça com que ela assine garantindo que a nova data de expiração esteja de pelo menos 30 dias e use `ModifyKeyServerKmip` para substituir o certificado de cliente KMIP expirado pelo novo certificado.

- Erro de certificado da Autoridade de Certificação raiz (CA).

Para resolver essa falha, verifique se o certificado correto foi fornecido e, se necessário, readquira o certificado da CA raiz. Use `ModifyKeyServerKmip` para instalar o certificado de cliente KMIP correto.

- Erro de certificado do cliente.

Para resolver essa falha, verifique se o certificado de cliente KMIP correto está instalado. A CA raiz do certificado de cliente deve ser instalada no EKS. Use `ModifyKeyServerKmip` para instalar o certificado de cliente KMIP correto.

• **KmipServerFault**

- Falha de ligação

Para resolver esta avaria, verifique se o servidor de chaves externas está ativo e acessível através da rede. Use `TestKeyServerKimp` e `TestKeyProviderKmip` para testar sua conexão.

- Falha de autenticação

Para resolver essa falha, verifique se os certificados de cliente KMIP e CA raiz corretos estão sendo usados e se a chave privada e o certificado de cliente KMIP correspondem.

- Erro de servidor

Para resolver esta avaria, verifique os detalhes do erro. A solução de problemas no servidor de chaves externas pode ser necessária com base no erro retornado.

• **MemórioEccThreshold**

Foi detetado um grande número de erros ECC corrigíveis ou incorrigíveis. Esta avaria utiliza as seguintes gravidades com base na urgência:

| Evento | Gravidade | Descrição |
|--|-----------|---|
| Um único DIMM cErrorCount atinge cDimmCorrectableErrWarnThreshold. | Aviso | Erros de memória ECC corrigíveis acima do limite no DIMM: <Processor> <DIMM Slot> |
| Um único DIMM cErrorCount permanece acima de cDimmCorrectableErrWarnThreshold até que cErrorFaultTimer expire para o DIMM. | Erro | Erros de memória ECC corrigíveis acima do limite no DIMM: <Processor> <DIMM> |
| Um controlador de memória relata cErrorCount acima de cMemCtrlrCorrectableErrWarnThreshold, e cMemCtrlrCorrectableErrWarnDuration é especificado. | Aviso | Erros de memória ECC corrigíveis acima do limite no controlador de memória: <Processor> <Memory Controller> |
| Um controlador de memória relata cErrorCount acima cMemCtrlrCorrectableErrWarnThreshold até que cErrorFaultTimer expire para o controlador de memória. | Erro | Erros de memória ECC corrigíveis acima do limite no DIMM: <Processor> <DIMM> |
| Um único DIMM relata um uErrorCount acima de zero, mas menor que cDimmUncorrectableErrFaultThreshold. | Aviso | Erro(s) de memória ECC incorrigível(s) detetado(s) no DIMM: <Processor> <DIMM Slot> |
| Um único DIMM relata um uErrorCount de pelo menos cDimmUncorrectableErrFaultThreshold. | Erro | Erro(s) de memória ECC incorrigível(s) detetado(s) no DIMM: <Processor> <DIMM Slot> |
| Um controlador de memória relata um uErrorCount acima de zero, mas menor que cMemCtrlrUncorrectableErrFaultThreshold. | Aviso | Erro(s) de memória ECC incorrigível(s) detetado(s) no controlador de memória: <Processor> <Memory Controller> |

| | | |
|--|------|---|
| Um controlador de memória relata um uErrorCount de pelo menos cMemCtrlUncorretableErrFaultThreshold. | Erro | Erro(s) de memória ECC incorrigível(s) detetado(s) no controlador de memória: <Processor> <Memory Controller> |
|--|------|---|

Para resolver esta avaria, contacte o suporte da NetApp para obter assistência.

• **MemoryUsageThreshold**

O uso da memória está acima do normal. Esta avaria utiliza as seguintes gravidades com base na urgência:



Consulte o cabeçalho **Detalhes** na falha de erro para obter informações mais detalhadas sobre o tipo de falha.

| Gravidade | Descrição |
|-----------|---|
| Aviso | A memória do sistema está baixa. |
| Erro | A memória do sistema é muito baixa. |
| Crítico | A memória do sistema é completamente consumida. |

Para resolver esta avaria, contacte o suporte da NetApp para obter assistência.

• **MetadataClusterFull**

Não há espaço de armazenamento de metadados livre suficiente para dar suporte a uma perda de nó único. Consulte o método da API GetClusterFullThreshold para obter detalhes sobre os níveis de plenitude do cluster. Esta avaria no grupo de instrumentos indica uma das seguintes condições:

- stage3Low (Aviso): O limite definido pelo usuário foi cruzado. Ajuste as configurações de Cluster Full ou adicione mais nós.
- stage4Critical (erro): Não há espaço suficiente para recuperar de uma falha de 1 nós. A criação de volumes, snapshots e clones não é permitida.
- stage5CompletelyConsumed (crítico)¹; não são permitidas gravações ou novas ligações iSCSI. As conexões iSCSI atuais serão mantidas. As gravações falharão até que mais capacidade seja adicionada ao cluster. Limpe ou exclua dados ou adicione mais nós. Para resolver essa falha, limpe ou exclua volumes ou adicione outro nó de armazenamento ao cluster de armazenamento.

• **MtuCheckFailure**

Um dispositivo de rede não está configurado para o tamanho adequado da MTU.

Para resolver essa falha, verifique se todas as interfaces de rede e portas de switch estão configuradas para quadros jumbo (MTUs de até 9000 bytes de tamanho).

• **NetworkConfig**

Esta avaria no grupo de instrumentos indica uma das seguintes condições:

- Uma interface esperada não está presente.
- Uma interface duplicada está presente.
- Uma interface configurada está inativa.
- É necessário reiniciar a rede. Entre em Contato com o suporte da NetApp para obter assistência.

• **NoAvailableVirtualNetworkIPAddresses**

Não há endereços de rede virtual disponíveis no bloco de endereços IP.

- A TAG(no no no) não tem endereços IP de armazenamento disponíveis. Nós adicionais não podem ser adicionados ao cluster. Para resolver essa falha, adicione mais endereços IP ao bloco de endereços de rede virtual.

• **NodeHardwareFault (a interface de rede <name> está inativa ou o cabo está desligado)**

Uma interface de rede está inativa ou o cabo está desconetado.

Para resolver essa falha, verifique a conectividade de rede para o nó ou nós.

• **NodeHardwareFault (o estado capaz de encriptação da unidade não corresponde ao estado capaz de encriptação do nó para a unidade no slot <node slot> <drive slot>)**

Uma unidade não corresponde aos recursos de criptografia com o nó de armazenamento em que está instalada.

• **NodeHardwareFault (<actual size> incorreto do tamanho da unidade <drive type> para a unidade no slot <node slot> <drive slot> para este tipo de nó - esperado <expected size>)**

Um nó de armazenamento contém uma unidade com o tamanho incorreto para este nó.

• **NodeHardwareFault (unidade não suportada detetada no slot <node slot> <drive slot>; estatísticas da unidade e informações de integridade não estarão disponíveis)**

Um nó de armazenamento contém uma unidade que não suporta.

• **NodeHardwareFault (a unidade no slot <node slot> <drive slot> deve estar usando a versão de firmware <expected version>, mas está usando a versão não suportada <actual version>)**

Um nó de armazenamento contém uma unidade que executa uma versão de firmware não suportada.

• **NodeMaintenanceMode**

Um nó foi colocado no modo de manutenção. Esta avaria utiliza as seguintes gravidades com base na urgência:

| Gravidade | Descrição |
|-----------|---|
| Aviso | Indica que o nó ainda está no modo de manutenção. |

| | |
|------|--|
| Erro | Indica que o modo de manutenção não foi desativado, provavelmente devido a falhas ou padrões ativos. |
|------|--|

Para resolver esta avaria, desative o modo de manutenção assim que a manutenção for concluída. Se a avaria no nível de erro persistir, contacte o suporte da NetApp para obter assistência.

- **NodeOffline**

O software Element não pode se comunicar com o nó especificado. Verifique a conectividade da rede.

- **NotUsingLACPBondMode**

O modo de ligação LACP não está configurado.

Para resolver essa falha, use a ligação LACP ao implantar nós de storage; os clientes podem ter problemas de desempenho se o LACP não estiver habilitado e configurado corretamente.

- **NtpServerUnreachable**

O cluster de armazenamento não pode se comunicar com o servidor NTP ou servidores especificados.

Para resolver essa falha, verifique a configuração do servidor NTP, rede e firewall.

- **NtpTimeNotInSync**

A diferença entre o tempo do cluster de armazenamento e o tempo do servidor NTP especificado é muito grande. O cluster de armazenamento não pode corrigir a diferença automaticamente.

Para resolver essa falha, use servidores NTP internos à sua rede, em vez dos padrões de instalação. Se estiver a utilizar servidores NTP internos e o problema persistir, contacte o suporte da NetApp para obter assistência.

- **NvramDeviceStatus**

Um dispositivo NVRAM apresenta um erro, está a falhar ou falhou. Esta avaria tem as seguintes gravidades:

| Gravidade | Descrição |
|-----------|--|
| Aviso | <p>Foi detetado um aviso pelo hardware. Esta condição pode ser transitória, como um aviso de temperatura.</p> <ul style="list-style-type: none"> • NvmLifetimeError • NvmLifetimeStatus • EnergySourceLifetimeStatus • EnergySourceTemperatureStatus • WarningThresholdExceeded |

| | |
|---------|---|
| Erro | <p>Foi detetado um erro ou estado crítico pelo hardware. O master do cluster tenta remover a unidade de corte da operação (isto gera um evento de remoção da unidade). Se os serviços de corte secundário não estiverem disponíveis, a unidade não será removida. Erros retornados além dos erros de nível de aviso:</p> <ul style="list-style-type: none"> • O ponto de montagem do dispositivo NVRAM não existe. • A partição do dispositivo NVRAM não existe. • A partição do dispositivo NVRAM existe, mas não está montada. |
| Crítico | <p>Foi detetado um erro ou estado crítico pelo hardware. O master do cluster tenta remover a unidade de corte da operação (isto gera um evento de remoção da unidade). Se os serviços de corte secundário não estiverem disponíveis, a unidade não será removida.</p> <ul style="list-style-type: none"> • PersistênciaLost • ArmStatusSaveNArmed • Erro csaveStatusError |

Substitua qualquer hardware com falha no nó. Se isso não resolver o problema, entre em Contato com o suporte da NetApp para obter assistência.

- **PowerSupplyError**

Esta avaria no grupo de instrumentos indica uma das seguintes condições:

- Não existe uma fonte de alimentação.
- Uma fonte de alimentação falhou.
- Uma entrada da fonte de alimentação está ausente ou fora da faixa. Para resolver essa falha, verifique se a alimentação redundante é fornecida a todos os nós. Entre em Contato com o suporte da NetApp para obter assistência.

- **ProvisionadoSpaceTooFull**

A capacidade provisionada geral do cluster está muito cheia.

Para resolver essa falha, adicione mais espaço provisionado ou exclua e limpe volumes.

- **RemoteRepAsyncDelayExceeded**

O atraso assíncrono configurado para replicação foi excedido. Verifique a conectividade de rede entre clusters.

- * RemoteRepClusterFull*

Os volumes interromperam a replicação remota porque o cluster de armazenamento de destino está demasiado cheio.

Para resolver esta avaria, liberte algum espaço no cluster de armazenamento de destino.

- **RemoteRepSnapshotClusterFull**

Os volumes interromperam a replicação remota de instantâneos porque o cluster de armazenamento de destino está demasiado cheio.

Para resolver esta avaria, liberte algum espaço no cluster de armazenamento de destino.

- * RemoteRepSnapshotsExceededLimit*

Os volumes interromperam a replicação remota de instantâneos porque o volume do cluster de armazenamento de destino excedeu o limite de instantâneos.

Para resolver esta avaria, aumente o limite de instantâneos no cluster de armazenamento de destino.

- **ScheduleActionError**

Uma ou mais das atividades agendadas foram executadas, mas falharam.

A falha será apagada se a atividade programada for executada novamente e for bem-sucedida, se a atividade programada for excluída ou se a atividade for pausada e retomada.

- **SensorReadingFailed**

O autoteste do controlador de gestão da placa de base (BMC) falhou ou um sensor não conseguiu comunicar com o BMC.

Entre em Contato com o suporte da NetApp para obter assistência.

- **ServiceNotRunning**

Um serviço necessário não está em execução.

Entre em Contato com o suporte da NetApp para obter assistência.

- **SliceServiceTooFull**

Um serviço de fatia tem pouca capacidade provisionada atribuída a ele.

Para resolver essa falha, adicione mais capacidade provisionada.

- **SliceServiceUnHealthy**

O sistema detetou que um serviço de corte não está saudável e está a ser desativado automaticamente.

- Aviso: Nenhuma ação é tomada. Este período de aviso expira em 6 minutos.
- Gravidade: O sistema está desativando automaticamente os dados e replicando novamente seus dados para outras unidades íntegras. Verifique se há problemas de conectividade de rede e erros de hardware. Haverá outras falhas se os componentes de hardware específicos tiverem falhado. A avaria será eliminada quando o serviço de corte estiver acessível ou quando o serviço tiver sido desativado.

- **SshEnabled**

O serviço SSH é ativado em um ou mais nós no cluster de armazenamento.

Para resolver essa falha, desative o serviço SSH no nó ou nós apropriados ou entre em Contato com o suporte da NetApp para obter assistência.

- **SslCertificateExpiration**

O certificado SSL associado a este nó está próximo da expiração ou expirou. Esta avaria utiliza as seguintes gravidades com base na urgência:

| Gravidade | Descrição |
|-----------|--|
| Aviso | O certificado expira dentro de 30 dias. |
| Erro | O certificado expira dentro de 7 dias. |
| Crítico | O certificado expira dentro de 3 dias ou já expirou. |

Para resolver esta avaria, renove o certificado SSL. Se necessário, entre em Contato com o suporte da NetApp para obter assistência.

- **StrandedCapacity**

Um único nó representa mais da metade da capacidade do cluster de storage.

Para manter a redundância de dados, o sistema reduz a capacidade do nó maior, de modo que parte de sua capacidade de bloco fique ociosa (não usada).

Para resolver essa falha, adicione mais unidades aos nós de storage existentes ou adicione nós de storage ao cluster.

- **TemSensor**

Um sensor de temperatura indica temperaturas superiores às normais. Esta avaria pode ser acionada em conjunto com avarias powerSupplyError ou fanSensor.

Para resolver esta avaria, verifique se existem obstruções de fluxo de ar perto do grupo de armazenamento. Se necessário, entre em Contato com o suporte da NetApp para obter assistência.

- **upgrade**

Uma atualização está em andamento há mais de 24 horas.

Para resolver esta avaria, retome a atualização ou contacte o suporte da NetApp para obter assistência.

- **UnresponsiveService**

Um serviço ficou sem resposta.

Entre em Contato com o suporte da NetApp para obter assistência.

- **VirtualNetworkConfig**

Esta avaria no grupo de instrumentos indica uma das seguintes condições:

- Uma interface não está presente.
- Há um namespace incorreto em uma interface.
- Existe uma máscara de rede incorreta.
- Existe um endereço IP incorreto.
- Uma interface não está ativa e em execução.
- Há uma interface supérflua em um nó. Entre em Contato com o suporte da NetApp para obter assistência.

• **VolumesDegraded**

Os volumes secundários não terminaram de replicar e sincronizar. A mensagem é apagada quando a sincronização estiver concluída.

• **VolumesOffline**

Um ou mais volumes no cluster de armazenamento estão offline. A avaria **volumeDegraded** também estará presente.

Entre em Contato com o suporte da NetApp para obter assistência.

Visualizar a atividade de performance do nó

Você pode visualizar a atividade de performance de cada nó em um formato gráfico. Essas informações fornecem estatísticas em tempo real para CPU e operações de e/S de leitura/gravação por segundo (IOPS) para cada unidade do nó. O gráfico de utilização é atualizado a cada cinco segundos e o gráfico de estatísticas da unidade é atualizado a cada dez segundos.

1. Clique em **Cluster > nodes**.
2. Clique em **ações** para o nó que deseja exibir.
3. Clique em **Ver detalhes**.



Você pode ver pontos específicos no tempo nos gráficos de linha e barra posicionando o cursor sobre a linha ou barra.

Ver o desempenho do volume

Você pode exibir informações detalhadas de desempenho de todos os volumes no cluster. Você pode classificar as informações por ID de volume ou por qualquer uma das colunas de desempenho. Você também pode usar o filtro de informações por determinados critérios.

Você pode alterar a frequência com que o sistema atualiza as informações de desempenho na página clicando na lista **Atualizar todos** e escolhendo um valor diferente. O intervalo de atualização padrão é de 10 segundos se o cluster tiver menos de 1000 volumes; caso contrário, o padrão é de 60 segundos. Se você escolher um valor de nunca, a atualização automática de página será desativada.

Você pode reativar a atualização automática clicando em **Ativar atualização automática**.

1. Na IU do Element, selecione **Reporting > volume Performance**.
2. Na lista de volumes, clique no ícone ações de um volume.
3. Clique em **Ver detalhes**.

Uma bandeja é exibida na parte inferior da página contendo informações gerais sobre o volume.

4. Para ver informações mais detalhadas sobre o volume, clique em **Ver mais detalhes**.

O sistema apresenta informações detalhadas, bem como gráficos de desempenho para o volume.

Encontre mais informações

[Detalhes do desempenho do volume](#)

Detalhes do desempenho do volume

Você pode exibir estatísticas de desempenho de volumes na página desempenho de volume da guia relatórios na IU do Element.

A lista a seguir descreve os detalhes que estão disponíveis para você:

- **ID**

A ID gerada pelo sistema para o volume.

- **Nome**

O nome dado ao volume quando foi criado.

- **Conta**

O nome da conta atribuída ao volume.

- **Grupos de acesso**

O nome do grupo de acesso ao volume ou grupos aos quais o volume pertence.

- *** Utilização de volume***

Um valor percentual que descreve quanto o cliente está usando o volume.

Valores possíveis:

- 0: O cliente não está usando o volume
- 100: O cliente está usando o máximo
- >100: O cliente está usando o burst

- **Total de IOPS**

O número total de IOPS (leitura e gravação) atualmente sendo executado em relação ao volume.

- **Leia IOPS**

O número total de IOPS de leitura atualmente sendo executado em relação ao volume.

- **Escreva IOPS**

O número total de IOPS de gravação atualmente sendo executado em relação ao volume.

- * Taxa de transferência total*

A quantidade total de throughput (leitura e gravação) que está sendo executada atualmente em relação ao volume.

- **Leia a taxa de transferência**

A quantidade total de taxa de transferência de leitura que está sendo executada atualmente em relação ao volume.

- **Taxa de transferência de gravação**

A quantidade total de taxa de transferência de gravação atualmente sendo executada em relação ao volume.

- **Latência total**

O tempo médio, em microssegundos, para concluir as operações de leitura e gravação em um volume.

- **Latência de leitura**

O tempo médio, em microssegundos, para concluir as operações de leitura para o volume nos últimos 500 milissegundos.

- **Latência de gravação**

O tempo médio, em microssegundos, para concluir as operações de gravação em um volume nos últimos 500 milissegundos.

- **Profundidade da fila**

O número de operações de leitura e gravação pendentes no volume.

- **Tamanho médio de IO**

Tamanho médio em bytes de e/S recentes para o volume nos últimos 500 milissegundos.

Ver sessões iSCSI

Pode visualizar as sessões iSCSI que estão ligadas ao cluster. Você pode filtrar as informações para incluir apenas as sessões desejadas.

1. Na IU do elemento, selecione **Reporting > iSCSI Sessions**.
2. Para ver os campos de critérios de filtro, clique em **filtro**.

Encontre mais informações

[Detalhes da sessão iSCSI](#)

Detalhes da sessão iSCSI

Pode visualizar informações sobre as sessões iSCSI ligadas ao cluster.

A lista a seguir descreve as informações que você pode encontrar sobre as sessões iSCSI:

- **Nó**

O nó que hospeda a partição de metadados primária para o volume.

- **Conta**

O nome da conta que possui o volume. Se o valor estiver em branco, é apresentado um traço (-).

- **Volume**

O nome do volume identificado no nó.

- **ID do volume**

ID do volume associado ao IQN alvo.

- **ID do iniciador**

Um ID gerado pelo sistema para o iniciador.

- **Alias do Iniciador**

Um nome opcional para o iniciador que facilita a localização do iniciador quando estiver em uma lista longa.

- **IP do Iniator**

O endereço IP do endpoint que inicia a sessão.

- **Iniciador IQN**

O IQN do endpoint que inicia a sessão.

- **IP de destino**

O endereço IP do nó que hospeda o volume.

- **Target IQN**

O IQN do volume.

- **Criado em**

Data em que a sessão foi estabelecida.

Ver sessões Fibre Channel

É possível visualizar as sessões Fibre Channel (FC) conetadas ao cluster. Você pode filtrar as informações para incluir apenas as conexões que deseja exibir na janela.

1. Na IU do elemento, selecione **Reporting > FC Sessions**.
2. Para ver os campos de critérios de filtro, clique em **filtro**.

Encontre mais informações

[Detalhes da sessão Fibre Channel](#)

Detalhes da sessão Fibre Channel

Você pode encontrar informações sobre as sessões ativas de Fibre Channel (FC) conetadas ao cluster.

A lista a seguir descreve as informações que você pode encontrar sobre as sessões FC conetadas ao cluster:

- **ID do nó**

O nó que hospeda a sessão para a conexão.

- **Nome do nó**

Nome do nó gerado pelo sistema.

- **ID do iniciador**

Um ID gerado pelo sistema para o iniciador.

- **Iniciador WWPN**

O nome da porta inicial mundial.

- **Alias do Iniciador**

Um nome opcional para o iniciador que facilita a localização do iniciador quando estiver em uma lista longa.

- *** Alvo WWPN***

O nome da porta mundial de destino.

- **Grupo de Acesso por volume**

Nome do grupo de acesso ao volume ao qual a sessão pertence.

- **ID do Grupo de Acesso por volume**

ID gerado pelo sistema para o grupo de acesso.

Solucionar problemas de unidades

Você pode substituir uma unidade de estado sólido (SSD) com falha por uma unidade de substituição. Os SSDs para nós de storage do SolidFire são de substituição a quente. Se você suspeitar que um SSD falhou, entre em Contato com o suporte da NetApp para verificar a falha e orientá-lo sobre o procedimento de resolução adequado. O suporte da

NetApp também trabalha com você para obter uma unidade de substituição de acordo com seu contrato de nível de serviço.

Como trocar, neste caso, significa que você pode remover uma unidade com falha de um nó ativo e substituí-la por uma nova unidade SSD do NetApp. Não é recomendável que você remova unidades que não tenham falha em um cluster ativo.

Você deve manter as peças sobressalentes no local sugeridas pelo suporte da NetApp para permitir a substituição imediata da unidade em caso de falha.



Para fins de teste, se você estiver simulando uma falha de unidade puxando uma unidade de um nó, você deve esperar 30 segundos antes de inserir a unidade novamente no slot da unidade.

Se uma unidade falhar, o Double Helix redistribui os dados na unidade pelos nós restantes no cluster. Várias falhas de unidade no mesmo nó não são um problema, pois o software Element protege contra duas cópias de dados que residem no mesmo nó. Uma unidade com falha resulta nos seguintes eventos:

- Os dados são migrados para fora da unidade.
- A capacidade geral do cluster é reduzida pela capacidade da unidade.
- A proteção de dados da Double Helix garante que haja duas cópias válidas dos dados.



Os sistemas de storage SolidFire não suportam a remoção de uma unidade se isso resultar em uma quantidade insuficiente de storage para migrar dados.

Para mais informações

- [Remover unidades com falha do cluster](#)
- [Resolução de problemas básicos da unidade MDSS](#)
- [Remova as unidades MDSS](#)
- ["Substituição de unidades para nós de storage do SolidFire"](#)
- ["Substituição de unidades para nós de storage da série H600S"](#)
- ["Informações sobre hardware H410S e H610S"](#)
- ["Informações sobre o hardware da série SF"](#)

Remover unidades com falha do cluster

O sistema SolidFire coloca uma unidade em um estado com falha se o autodiagnóstico da unidade disser ao nó que falhou ou se a comunicação com a unidade parar por cinco minutos e meio ou mais. O sistema exibe uma lista das unidades com falha. Você deve remover uma unidade com falha da lista de unidades com falha no software NetApp Element.

As unidades na lista **Alerts** são exibidas como **blockServiceUnHealthy** quando um nó está offline. Ao reiniciar o nó, se o nó e suas unidades voltarem online dentro de cinco minutos e meio, as unidades serão atualizadas automaticamente e continuarão como unidades ativas no cluster.

1. Na IU do elemento, selecione **Cluster > Drives**.

2. Clique em **Failed** para ver a lista de unidades com falha.
3. Observe o número do slot da unidade com falha.

Você precisa dessas informações para localizar a unidade com falha no chassi.

4. Remova as unidades com falha usando um dos seguintes métodos:

| Opção | Passos |
|-----------------------------------|--|
| Para remover unidades individuais | <ol style="list-style-type: none"> a. Clique em ações para a unidade que deseja remover. b. Clique em Remover. |
| Para remover várias unidades | <ol style="list-style-type: none"> a. Selecione todas as unidades que deseja remover e clique em ações em massa. b. Clique em Remover. |

Resolução de problemas básicos da unidade MDSS

É possível recuperar unidades de metadados (ou slice) adicionando-as de volta ao cluster no caso de uma ou ambas as unidades de metadados falharem. Você pode executar a operação de recuperação na IU do NetApp Element se o recurso MDSS já estiver ativado no nó.

Se uma ou ambas as unidades de metadados em um nó sofrer uma falha, o serviço de fatia será encerrado e os dados de ambas as unidades serão copiados para diferentes unidades no nó.

Os cenários a seguir descrevem possíveis cenários de falha e fornecem recomendações básicas para corrigir o problema:

Falha na unidade de corte do sistema

- Neste cenário, o slot 2 é verificado e retornado a um estado disponível.
- A unidade de corte do sistema tem de ser preenchida novamente antes de o serviço de corte poder ser colocado novamente online.
- Deve substituir a unidade de corte do sistema, quando a unidade de corte do sistema ficar disponível, adicione a unidade e a unidade de ranhura 2 ao mesmo tempo.



Você não pode adicionar a unidade no slot 2 por si só como uma unidade de metadados. Você deve adicionar ambas as unidades de volta ao nó ao mesmo tempo.

Falha no slot 2

- Neste cenário, a unidade de corte do sistema é verificada e devolvida a um estado disponível.
- Deve substituir o slot 2 por um sobressalente, quando o slot 2 estiver disponível, adicione a unidade de corte do sistema e a unidade de slot 2 ao mesmo tempo.

Falha na unidade de corte do sistema e na ranhura 2

- Deve substituir a unidade de corte do sistema e a ranhura 2 por uma unidade sobressalente. Quando ambas as unidades estiverem disponíveis, adicione a unidade de corte do sistema e a unidade de slot 2 ao mesmo tempo.

Ordem de operações

- Substitua a unidade de hardware com falha por uma unidade sobressalente (substitua ambas as unidades se ambas tiverem falhado).
- Adicione unidades de volta ao cluster quando elas tiverem sido preenchidas novamente e estiverem em um estado disponível.

Verifique as operações

- Verifique se as unidades no slot 0 (ou interno) e no slot 2 estão identificadas como unidades de metadados na lista unidades ativas.
- Verifique se todo o equilíbrio de cortes foi concluído (não existem mais mensagens de cortes em movimento no registo de eventos durante, pelo menos, 30 minutos).

Para mais informações

[Adicione unidades MDSS](#)

Adicione unidades MDSS

Você pode adicionar uma segunda unidade de metadados em um nó SolidFire convertendo a unidade de bloco no slot 2 em uma unidade de fatia. Isto é conseguido ativando a funcionalidade de serviço de corte multi-unidades (MDSS). Para ativar esse recurso, entre em Contato com o suporte da NetApp.

Obter uma unidade de corte em um estado disponível pode exigir a substituição de uma unidade com falha por uma unidade nova ou sobressalente. Tem de adicionar a unidade de corte do sistema ao mesmo tempo que adiciona a unidade para o slot 2. Se tentar adicionar a unidade de corte slot 2 sozinha ou antes de adicionar a unidade de corte do sistema, o sistema irá gerar um erro.

1. Clique em **Cluster > Drives**.
2. Clique em **Available** para ver a lista de unidades disponíveis.
3. Selecione as unidades de corte a adicionar.
4. Clique em **ações em massa**.
5. Clique em **Add**.
6. Confirme na guia **unidades ativas** que as unidades foram adicionadas.

Remova as unidades MDSS

Pode remover as unidades de serviço de corte multi-unidades (MDSS). Este procedimento aplica-se apenas se o nó tiver várias unidades de corte.



Se a unidade de corte do sistema e a unidade de ranhura 2 falharem, o sistema irá desligar os serviços de corte e remover as unidades. Se não houver falha e você remover as unidades, ambas devem ser removidas ao mesmo tempo.

1. Clique em **Cluster > Drives**.
2. Na guia unidades **disponíveis**, clique na caixa de seleção das unidades de corte que estão sendo removidas.
3. Clique em **ações em massa**.
4. Clique em **Remover**.
5. Confirme a ação.

Solucionar problemas de nós

Você pode remover nós de um cluster para manutenção ou substituição. Você deve usar a IU ou API do NetApp Element para remover nós antes de colocá-los offline.

Uma visão geral do procedimento para remover nós de storage é a seguinte:

- Verifique se há capacidade suficiente no cluster para criar uma cópia dos dados no nó.
- Remova unidades do cluster usando a IU ou o método da API RemoveDrives.

Isso resulta na migração de dados do sistema das unidades do nó para outras unidades do cluster. O tempo que esse processo demora depende da quantidade de dados que precisam ser migrados.

- Remova o nó do cluster.

Tenha em mente as seguintes considerações antes de desligar ou ligar um nó:

- Desativar nós e clusters envolve riscos se não for executado corretamente.

Desligar um nó deve ser feito sob a direção do suporte NetApp.

- Se um nó estiver inativo por mais de 5,5 minutos em qualquer tipo de condição de desligamento, a proteção de dados Double Helix inicia a tarefa de gravar blocos replicados únicos em outro nó para replicar os dados. Nesse caso, entre em Contato com o suporte da NetApp para obter ajuda sobre a análise do nó com falha.
- Para reinicializar ou desligar um nó com segurança, você pode usar o comando Shutdown API.
- Se um nó estiver em estado inativo ou desligado, entre em Contato com o suporte da NetApp antes de colocá-lo novamente on-line.
- Depois que um nó é colocado novamente on-line, você deve adicionar as unidades de volta ao cluster, dependendo de quanto tempo ele ficou fora de serviço.

Para mais informações

["Substituição de um chassi SolidFire com falha"](#)

["Substituição de um nó da série H600S com falha"](#)

Desligue um cluster

Execute o procedimento a seguir para desligar todo um cluster.

Passos

1. (Opcional) entre em Contato com o suporte da NetApp para obter assistência para concluir as etapas preliminares.
2. Verifique se todas as e/S pararam.
3. Desligar todas as sessões iSCSI:
 - a. Navegue até o endereço de IP virtual de gerenciamento (MVIP) no cluster para abrir a IU do Element.
 - b. Observe os nós listados na lista de nós.
 - c. Execute o método Shutdown API com a opção Halt especificada em cada ID do nó no cluster.

Ao reiniciar o cluster, você deve seguir determinadas etapas para verificar se todos os nós estão online:



1. Verifique se todas as falhas críticas de gravidade e `volumesOffline` cluster foram resolvidas.
2. Aguarde 10 a 15 minutos para que o cluster se assente.
3. Comece a trazer os hosts para acessar os dados.

Se você quiser permitir mais tempo ao ligar os nós e verificar se eles estão em boas condições após a manutenção, entre em Contato com o suporte técnico para obter assistência com o atraso da sincronização de dados para evitar a sincronização desnecessária de bin.

Encontre mais informações

["Como desligar e ligar graciosamente um cluster de storage NetApp SolidFire/HCI"](#)

Trabalhar com utilitários por nó para nós de storage

Você pode usar os utilitários por nó para solucionar problemas de rede se as ferramentas de monitoramento padrão na IU do software NetApp Element não lhe fornecerem informações suficientes para solucionar problemas. Os utilitários por nó fornecem informações e ferramentas específicas que podem ajudá-lo a solucionar problemas de rede entre nós ou com o nó de gerenciamento.

Encontre mais informações

- [Acesse as configurações por nó usando a IU por nó](#)
- [Detalhes das definições de rede a partir da IU por nó](#)
- [Detalhes das configurações do cluster a partir da IU por nó](#)
- [Execute testes do sistema usando a IU por nó](#)
- [Execute utilitários do sistema usando a IU por nó](#)

Acesse as configurações por nó usando a IU por nó

Você pode acessar as configurações de rede, configurações de cluster e testes e utilitários do sistema na interface de usuário por nó depois de inserir o IP do nó de gerenciamento e autenticar.

Se você quiser modificar as configurações de um nó em um estado Ativo que faz parte de um cluster, você deve fazer login como um usuário administrador de cluster.



Você deve configurar ou modificar um nó de cada vez. Você deve garantir que as configurações de rede especificadas estejam tendo o efeito esperado e que a rede esteja estável e com bom desempenho antes de fazer modificações em outro nó.

1. Abra a IU por nó usando um dos seguintes métodos:

- Introduza o endereço IP de gestão seguido de :442 numa janela do navegador e inicie sessão utilizando um nome de utilizador e uma palavra-passe de administrador.
- Na IU do elemento, selecione **Cluster > nodes** e clique no link de endereço IP de gerenciamento do nó que deseja configurar ou modificar. Na janela do navegador que se abre, você pode editar as configurações do nó.



Detalhes das definições de rede a partir da IU por nó

Você pode alterar as configurações de rede do nó de armazenamento para dar ao nó um novo conjunto de atributos de rede.

Pode ver as definições de rede para um nó de armazenamento na página **Definições de rede** quando iniciar sessão no (<https://<nó IP>:442/hcc/nó/definições de rede>). Pode seleccionar as definições **Bond1G** (gestão) ou **Bond10G** (armazenamento). A lista a seguir descreve as configurações que você pode modificar quando um nó de armazenamento está no estado disponível, pendente ou Ativo:

- **Método**

O método utilizado para configurar a interface. Métodos possíveis:

- Loopback: Usado para definir a interface de loopback IPv4.
- Manual: Usado para definir interfaces para as quais nenhuma configuração é feita por padrão.
- dhcp: Usado para obter um endereço IP via DHCP.
- Estático: Usado para definir interfaces Ethernet com endereços IPv4 alocados estaticamente.

- **Velocidade de ligação**

A velocidade negociada pela NIC virtual.

- **Endereço IPv4**

O endereço IPv4 para a rede eth0.

- **IPv4 Máscara de sub-rede**

Subdivisões de endereços da rede IPv4.

- **Endereço do gateway IPv4**

Endereço de rede do roteador para enviar pacotes para fora da rede local.

- **Endereço IPv6**

O endereço IPv6 para a rede eth0.

- **Endereço do gateway IPv6**

Endereço de rede do roteador para enviar pacotes para fora da rede local.

- **MTU**

Maior tamanho de pacote que um protocolo de rede pode transmitir. Deve ser maior ou igual a 1500. Se você adicionar uma segunda NIC de armazenamento, o valor deve ser 9000.

- **Servidores DNS**

Interface de rede usada para comunicação de cluster.

- **Domínios de pesquisa**

Procure endereços MAC adicionais disponíveis para o sistema.

- **Modo Bond**

Pode ser um dos seguintes modos:

- ActivePassive (padrão)
- ALB
- LACP

- **Status**

Valores possíveis:

- UpAndRunning
- Para baixo
- Para cima

- **Etiqueta de rede virtual**

Tag atribuída quando a rede virtual foi criada.

- **Rotas**

Rotas estáticas para hosts ou redes específicas através da interface associada as rotas são configuradas para usar.

Detalhes das configurações do cluster a partir da IU por nó

Você pode verificar as configurações do cluster para um nó de armazenamento após a configuração do cluster e modificar o nome do host do nó.

A lista a seguir descreve as configurações de cluster para um nó de armazenamento indicado na página **Configurações de cluster** da interface IP por nó (<https://<node>:442/hcc/nó/configurações de cluster>).

- **Função**

Função que o nó tem no cluster. Valores possíveis:

- Storage: Nó de storage ou Fibre Channel.
- Gerenciamento: O nó é um nó de gerenciamento.

- **Nome do anfitrião**

Nome do nó.

- **Cluster**

Nome do cluster.

- **Cluster Membership**

Estado do nó. Valores possíveis:

- Disponível: O nó não tem nome de cluster associado e ainda não faz parte de um cluster.
- Pendente: O nó está configurado e pode ser adicionado a um cluster designado. A autenticação não é necessária para acessar o nó.
- PendingActive: O sistema está em processo de instalação de software compatível no nó. Quando concluído, o nó se moverá para o estado Ativo.
- Ativo: O nó está participando de um cluster. A autenticação é necessária para modificar o nó.

- **Versão**

Versão do software Element em execução no nó.

- **Conjunto**

Nós que fazem parte do conjunto de banco de dados.

- **ID do nó**

ID atribuída quando um nó é adicionado ao cluster.

- **Interface de cluster**

Interface de rede usada para comunicação de cluster.

- **Interface de Gestão**

Interface de rede de gerenciamento. Este padrão é Bond1G, mas também pode usar Bond10G.

- **Interface de armazenamento**

Interface de rede de storage usando Bond10G.

- **Capacidade de encriptação**

Indica se o nó suporta ou não criptografia de unidade.

Execute testes do sistema usando a IU por nó

Você pode testar as alterações nas configurações de rede depois de comê-las na configuração de rede. Você pode executar os testes para garantir que o nó de storage seja estável e possa ser colocado on-line sem problemas.

Você fez login na IU por nó do nó de armazenamento.

1. Clique em **testes do sistema**.
2. Clique em **Run Test** ao lado do teste que deseja executar ou selecione **Run All Tests** (Executar todos os testes).



Executar todas as operações de teste pode ser demorado e deve ser feito apenas na direção do suporte NetApp.

- **Teste do conjunto conetado**

Testa e verifica a conetividade a um conjunto de banco de dados. Por padrão, o teste usa o conjunto para o cluster ao qual o nó está associado. Alternativamente, você pode fornecer um conjunto diferente para testar a conetividade.

- **Teste conetar Mvip**

Faz o ping do endereço IP virtual de gerenciamento (MVIP) especificado e, em seguida, executa uma chamada de API simples para o MVIP para verificar a conetividade. Por padrão, o teste usa o MVIP para o cluster ao qual o nó está associado.

- **Teste conetar Svip**

Faz o ping do endereço IP virtual de armazenamento (SVIP) especificado usando pacotes ICMP (Internet Control Message Protocol) que correspondem ao tamanho máximo da unidade de transmissão (MTU) definido no adaptador de rede. Em seguida, liga-se ao SVIP como um iniciador

iSCSI. Por padrão, o teste usa o SVIP para o cluster ao qual o nó está associado.

- **Configuração do hardware de teste**

Testa se todas as configurações de hardware estão corretas, valida as versões de firmware estão corretas e confirma que todas as unidades estão instaladas e funcionando corretamente. Isto é o mesmo que o teste de fábrica.



Esse teste tem uso intensivo de recursos e só deve ser executado se solicitado pelo suporte da NetApp.

- **Teste de conectividade local**

Testa a conectividade com todos os outros nós no cluster fazendo ping no IP do cluster (CIP) em cada nó. Este teste só será exibido em um nó se o nó fizer parte de um cluster ativo.

- **Teste localizar Cluster**

Valida que o nó pode localizar o cluster especificado na configuração do cluster.

- **Configuração da rede de teste**

Verifica se as definições de rede configuradas correspondem às definições de rede que estão a ser utilizadas no sistema. Esse teste não se destina a detetar falhas de hardware quando um nó participa ativamente de um cluster.

- **Teste ping**

Pings uma lista especificada de hosts ou, se nenhum for especificado, cria dinamicamente uma lista de todos os nós registrados no cluster e pings cada um para conectividade simples.

- **Teste de conectividade remota**

Testa a conectividade com todos os nós em clusters emparelhados remotamente fazendo o ping do IP do cluster (CIP) em cada nó. Este teste só será exibido em um nó se o nó fizer parte de um cluster ativo.

Execute utilitários do sistema usando a IU por nó

Você pode usar a IU por nó para o nó de armazenamento para criar ou excluir pacotes de suporte, redefinir configurações para unidades e reiniciar serviços de rede ou cluster.

Você fez login na IU por nó do nó de armazenamento.

1. Clique em **Utilitários do sistema**.
2. Clique no botão do utilitário de sistema que você deseja executar.

- **Potência de controle**

Reinicializa, liga ou desliga o nó.



Esta operação causa perda temporária de conectividade de rede.

Especifique os seguintes parâmetros:

- Ação: As opções incluem reiniciar e parar (desligar).
- Atraso de ativação: Qualquer tempo adicional antes do nó voltar online.

- **Coletar Logs de nó**

Cria um pacote de suporte no diretório /tmp/bundles do nó.

Especifique os seguintes parâmetros:

- Nome do pacote: Nome exclusivo para cada pacote de suporte criado. Se nenhum nome for fornecido, então "supportbundle" e o nome do nó serão usados como o nome do arquivo.
- Args extra: Este parâmetro é alimentado para o script sf_make_support_bundle. Este parâmetro deve ser utilizado apenas a pedido do suporte NetApp.
- Segundos de tempo limite: Especifique o número de segundos a aguardar por cada resposta de ping individual.

- **Excluir Logs de nó**

Exclui todos os pacotes de suporte atuais no nó que foram criados usando **Create Cluster Support Bundle** ou o método da API CreateSupportBundle.

- **Repor drives**

Inicializa unidades e remove todos os dados atualmente residentes na unidade. Você pode reutilizar a unidade em um nó existente ou em um nó atualizado.

Especifique o seguinte parâmetro:

- Unidades: Lista de nomes de dispositivos (não drives) a repor.

- **Redefinir configuração de rede**

Ajuda a resolver problemas de configuração de rede para um nó individual e redefine a configuração de rede de um nó individual para as configurações padrão de fábrica.

- **Repor nó**

Repõe um nó nas definições de fábrica. Todos os dados são removidos, mas as configurações de rede para o nó são preservadas durante esta operação. Os nós só podem ser redefinidos se não forem atribuídos a um cluster e no estado disponível.



Todos os dados, pacotes (atualizações de software), configurações e arquivos de log são excluídos do nó quando você usa essa opção.

- * Reinicie a rede*

Reinicia todos os serviços de rede em um nó.



Esta operação pode causar perda temporária de conectividade de rede.

- **Restart Services**

Reinicia os serviços de software Element em um nó.



Esta operação pode causar interrupção temporária do serviço do nó. Você deve executar esta operação apenas na direção do suporte NetApp.

Especifique os seguintes parâmetros:

- Serviço: Nome do serviço a ser reiniciado.
- Ação: Ação a executar no serviço. As opções incluem iniciar, parar e reiniciar.

Trabalhe com o nó de gerenciamento

Você pode usar o nó de gerenciamento (mNode) para atualizar serviços do sistema, gerenciar ativos e configurações do cluster, executar testes e utilitários do sistema, configurar o Active IQ para monitoramento do sistema e ativar o acesso ao suporte NetApp para solução de problemas.



Como prática recomendada, associe apenas um nó de gerenciamento a uma instância do VMware vCenter e evite definir os mesmos recursos de storage e computação ou instâncias do vCenter em vários nós de gerenciamento.

Consulte "[documentação do nó de gerenciamento](#)" para obter mais informações.

Entenda os níveis de plenitude do cluster

O cluster que executa o software Element gera falhas de cluster para avisar o administrador de storage quando o cluster está sem capacidade. Existem três níveis de preenchimento do cluster, todos exibidos na IU do NetApp Element: Aviso, erro e crítico.

O sistema usa o código de erro BlockClusterFull para avisar sobre a plenitude do armazenamento do bloco de cluster. Você pode visualizar os níveis de gravidade de preenchimento do cluster na guia Alertas da IU do elemento.

A lista a seguir inclui informações sobre os níveis de gravidade BlockClusterFull:

• Aviso

Este é um aviso configurável pelo cliente que aparece quando a capacidade de bloco do cluster está se aproximando do nível de gravidade do erro. Por padrão, esse nível é definido em três por cento abaixo do nível de erro e pode ser ajustado através da IU e API do elemento. Você precisa adicionar mais capacidade ou liberar capacidade o mais rápido possível.

• Erro

Quando o cluster estiver nesse estado, se um nó for perdido, não haverá capacidade suficiente no cluster para reconstruir a proteção de dados Double Helix. A criação de novos volumes, os clones e os snapshots são bloqueados enquanto o cluster está nesse estado. Este não é um estado seguro ou recomendado para que qualquer cluster esteja dentro. Você deve adicionar mais capacidade ou liberar capacidade imediatamente.

• Crítica

Esse erro crítico ocorreu porque o cluster é 100% consumido. Ele está em um estado somente leitura e nenhuma nova conexão iSCSI pode ser feita ao cluster. Quando esta fase for alcançada, você deve liberar

ou adicionar mais capacidade imediatamente.

O sistema usa o código de erro `MetadataClusterFull` para avisar sobre a plenitude do armazenamento de metadados do cluster. Você pode visualizar a plenitude do armazenamento de metadados do cluster na seção capacidade do cluster na página Visão geral da guia relatórios na IU do elemento.

A lista a seguir inclui informações sobre os níveis de gravidade `MetadataClusterFull`:

- **Aviso**

Este é um aviso configurável pelo cliente que aparece quando a capacidade de metatdata do cluster está se aproximando do nível de gravidade do erro. Por padrão, esse nível é definido em três por cento abaixo do nível de erro e pode ser ajustado através da API Element. Você precisa adicionar mais capacidade ou liberar capacidade o mais rápido possível.

- **Erro**

Quando o cluster estiver nesse estado, se um nó for perdido, não haverá capacidade suficiente no cluster para reconstruir a proteção de dados Double Helix. A criação de novos volumes, os clones e os snapshots são bloqueados enquanto o cluster está nesse estado. Este não é um estado seguro ou recomendado para que qualquer cluster esteja dentro. Você deve adicionar mais capacidade ou liberar capacidade imediatamente.

- **Crítica**

Esse erro crítico ocorreu porque o cluster é 100% consumido. Ele está em um estado somente leitura e nenhuma nova conexão iSCSI pode ser feita ao cluster. Quando esta fase for alcançada, você deve liberar ou adicionar mais capacidade imediatamente.



O seguinte se aplica aos limites de cluster de dois nós:

- O erro de preenchimento de metadados está 20% abaixo do crítico.
- O erro de preenchimento do bloco está na unidade de bloco 1 (incluindo capacidade ociosa) abaixo da crítica; o que significa que há duas unidades de bloco que valem a capacidade abaixo da crítica.

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 SOFTWARES, 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.