Configurar as definições do cluster

Element Software

NetApp
November 12, 2025

Índice

Configurar as definições do cluster

Ativar e desativar a criptografia em repouso para um cluster

Com os clusters SolidFire , você pode criptografar todos os dados em repouso armazenados nas unidades do cluster. Você pode habilitar a proteção de unidades de criptografia automática (SED) em todo o cluster usando um dos seguintes métodos:"Criptografia em repouso baseada em hardware ou software" .

Você pode habilitar a criptografia de hardware em repouso usando a interface do usuário ou a API do Element. Habilitar a criptografia de hardware em repouso não afeta o desempenho ou a eficiência do cluster. Você pode habilitar a criptografia de software em repouso usando apenas a API Element.

A criptografia em repouso baseada em hardware não está habilitada por padrão durante a criação do cluster, mas pode ser ativada e desativada na interface do usuário do Element.

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

O que você vai precisar

- Você possui privilégios de administrador de cluster para habilitar ou alterar as configurações de criptografia.
- Para criptografia em repouso baseada em hardware, você garantiu que o cluster esteja em bom estado antes de alterar as configurações de criptografia.
- Se você estiver desativando a criptografia, dois nós devem participar de um cluster para acessar a chave que desativa a criptografia em uma unidade.

Verificar o estado da criptografia em repouso

Para visualizar o estado atual da criptografia em repouso e/ou da criptografia de software em repouso no cluster, utilize o"Obter informações do cluster" método. Você pode usar o"GetSoftwareEncryptionAtRestInfo" Método para obter informações sobre o que o cluster usa para criptografar dados em repouso.

> O painel de controle da interface do usuário do software Element em `https://<MVIP>/` Atualmente, só é exibido o status de criptografia em repouso para criptografia baseada em hardware.

Opções

- Habilitar criptografia baseada em hardware em repouso
- Habilitar criptografia baseada em software em repouso
- Desative a criptografia baseada em hardware em repouso.

Habilitar criptografia baseada em hardware em repouso

> Para habilitar a criptografia em repouso usando uma configuração de gerenciamento de chaves externa, você deve habilitar a criptografia em repouso por meio do"API" . Habilitar o uso do botão existente da interface do usuário do Element fará com que o sistema volte a usar chaves geradas internamente.

1. Na interface do Element, selecione **Cluster** > **Configurações**.
2. Selecione **Ativar criptografia em repouso**.

Habilitar criptografia baseada em software em repouso

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

1. Durante a criação do cluster, execute o"método de criação de cluster" com `enableSoftwareEncryptionAtRest` definido para `true` .

Desative a criptografia baseada em hardware em repouso.

1. Na interface do Element, selecione **Cluster** > **Configurações**.
2. Selecione **Desativar criptografia em repouso**.

Encontre mais informações

- "Documentação do SolidFire e do Element Software"
- "Documentação para versões anteriores dos produtos NetApp SolidFire e Element."

Defina o limite máximo de clusters cheios.

Você pode alterar o nível em que o sistema gera um aviso de preenchimento do cluster de blocos seguindo os passos abaixo. Além disso, você pode usar o método de API ModifyClusterFullThreshold para alterar o nível em que o sistema gera um aviso de bloqueio ou de metadados.

O que você vai precisar

Você precisa ter privilégios de administrador de cluster.

Passos

1. Clique em **Cluster** > **Configurações**.
2. Na seção Configurações Completas do Cluster, insira uma porcentagem em **Exibir um alerta de aviso quando _% da capacidade permanecer antes que o Helix não consiga se recuperar de uma falha de nó**.
3. Clique em **Salvar alterações**.

Encontre mais informações

"Como são calculados os limites do blockSpace para o Elemento?"

Ativar e desativar o balanceamento de carga por volume

A partir do Element 12.8, você pode usar o Balanceamento de Carga de Volume para distribuir os volumes entre os nós com base no IOPS real de cada volume, em vez do IOPS mínimo configurado na política de QoS. Você pode ativar e desativar o balanceamento de carga por volume, que está desativado por padrão, usando a interface

do usuário do Element ou a API.

Passos

1. Selecione **Cluster** > **Configurações**.
2. Na seção Específica do Cluster, altere o status do Balanceamento de Carga de Volume:

   Ativar balanceamento de carga por volume

   Selecione **Ativar balanceamento de carga com base em IOPS reais** e confirme sua seleção.

   Desativar o balanceamento de carga por volume:

   Selecione **Desativar balanceamento de carga com base em IOPS reais** e confirme sua seleção.

3. Opcionalmente, selecione **Relatórios** > **Visão geral** para confirmar a alteração de status do Saldo em IOPS reais. Você pode precisar rolar a página para baixo nas informações de integridade do cluster para visualizar o status.

Encontre mais informações

- "Ative o balanceamento de carga por volume usando a API."
- "Desative o balanceamento de carga de volume usando a API."
- "Criar e gerenciar políticas de QoS de volume"

Ativar e desativar o acesso ao suporte

Você pode habilitar o acesso de suporte para permitir temporariamente que a equipe de suporte da NetApp acesse os nós de armazenamento via SSH para fins de solução de problemas.

Você precisa ter privilégios de administrador de cluster para alterar o acesso de suporte.

1. Clique em **Cluster** > **Configurações**.
2. Na seção Ativar/Desativar Acesso de Suporte, insira a duração (em horas) durante a qual deseja permitir que a equipe de 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 o banner dos Termos de Uso

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

Opções

Ative o banner dos Termos de Uso Editar o banner dos Termos de Uso Desative o banner dos Termos de Uso

Ative o banner dos Termos de Uso

Você pode ativar um banner com os Termos de Uso que aparece quando um usuário faz login na interface do Element. Quando o usuário clica no banner, uma caixa de diálogo de texto aparece contendo a mensagem que você configurou para o cluster. O banner pode ser fechado a qualquer momento.

Você precisa ter privilégios de administrador de cluster para habilitar a funcionalidade de Termos de Uso.

1. Clique em **Usuários** > **Termos de Uso**.
2. No formulário **Termos de Uso**, insira o texto que será exibido na caixa de diálogo Termos de Uso.

   Não ultrapasse 4096 caracteres.

3. Clique em **Ativar**.

Editar o banner dos Termos de Uso

Você pode editar o texto que o usuário vê ao selecionar o banner de login dos Termos de Uso.

O que você vai precisar

- Você precisa ter privilégios de administrador de cluster para configurar os Termos de Uso.
- Certifique-se de que o recurso Termos de Uso esteja ativado.

Passos

1. Clique em **Usuários** > **Termos de Uso**.
2. Na caixa de diálogo **Termos de Uso**, edite o texto que deseja que apareça.

   Não ultrapasse 4096 caracteres.

3. Clique em **Salvar alterações**.

Desative o banner dos Termos de Uso

Você pode desativar o banner dos Termos de Uso. Com o banner desativado, o usuário não precisa mais aceitar os termos de uso ao utilizar a interface do Element.

O que você vai precisar

- Você precisa ter privilégios de administrador de cluster 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**.

Configure o Protocolo de Tempo de Rede (NTP)

Configure os servidores Network Time Protocol (NTP) para que o cluster possa realizar consultas.

Você pode instruir cada nó em um cluster a consultar um servidor de Protocolo de Tempo de Rede (NTP) em busca de atualizações. O cluster contata apenas os servidores configurados e solicita informações NTP deles.

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

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

A utilização do FQDN depende de as configurações de DNS de cada nó de armazenamento estarem implementadas e operacionais. Para isso, configure os servidores DNS em cada nó de armazenamento e certifique-se de que as portas estejam abertas, consultando a página de Requisitos de Porta de Rede.

Você pode inserir até cinco servidores NTP diferentes.

Você pode usar endereços IPv4 e IPv6.

O que você vai precisar

Você precisa ter privilégios de administrador de cluster para configurar essa opção.

Passos

1. Configure uma lista de IPs e/ou FQDNs nas configurações do servidor.
2. Certifique-se de que o DNS esteja configurado corretamente nos nós.
3. Clique em **Cluster** > **Configurações**.
4. Em Configurações do Protocolo de Tempo de Rede, selecione **Não**, que utiliza a configuração NTP padrão.
5. Clique em **Salvar alterações**.

Encontre mais informações

- "Configure o cluster para escutar transmissões NTP."
- "Documentação do SolidFire e do Element Software"
- "Plug-in NetApp Element para vCenter Server"

Configure o cluster para escutar transmissões NTP.

Ao usar o modo de transmissão, você pode instruir cada nó em um cluster a escutar na rede as mensagens de transmissão do Protocolo de Tempo de Rede (NTP) provenientes de um servidor específico.

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

O que você vai precisar

- Você precisa ter privilégios de administrador de cluster para configurar essa opção.
- Você precisa configurar um servidor NTP em sua rede como um servidor de transmissão (broadcast).

Passos

1. Clique em **Cluster** > **Configurações**.
2. Insira na lista de servidores o(s) servidor(es) NTP que estão usando o modo de transmissão.
3. Em Configurações do Protocolo de Tempo de Rede, selecione **Sim** para usar um cliente de transmissão.
4. Para configurar o cliente de transmissão, no campo **Servidor**, insira o servidor NTP que você configurou no modo de transmissão.
5. Clique em **Salvar alterações**.

Encontre mais informações

- "Configure os servidores Network Time Protocol (NTP) para que o cluster possa realizar consultas."
- "Documentação do SolidFire e do Element Software"
- "Plug-in NetApp Element para vCenter Server"

Gerenciar SNMP

Saiba mais sobre o SNMP

Você pode configurar o Protocolo Simples de Gerenciamento de Rede (SNMP) em seu cluster.

Você pode selecionar um solicitante SNMP, escolher qual versão do SNMP usar, identificar o usuário do Modelo de Segurança Baseado em Usuário (USM) do SNMP 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 da guia Cluster, você pode visualizar as seguintes informações.

- **MIBs SNMP**

  Os arquivos MIB que você pode visualizar ou baixar.

- **Configurações gerais de SNMP**

  Você pode ativar ou desativar o SNMP. Após ativar o SNMP, você poderá escolher qual versão usar. Se estiver usando a versão 2, você pode adicionar solicitantes e, se estiver usando a versão 3, pode configurar usuários do USM.

- **Configurações de SNMP Trap**

  Você pode identificar quais armadilhas deseja capturar. Você pode definir o host, a porta e a string da comunidade para cada destinatário do trap.

Configure um solicitante SNMP.

Quando o SNMP versão 2 está habilitado, você pode ativar ou desativar um solicitante e configurar os solicitantes para receber solicitações SNMP autorizadas.

1. Clique no menu: Cluster [SNMP].
2. Em **Configurações gerais de SNMP**, clique em **Sim** para ativar o SNMP.
3. Na lista **Versão**, selecione **Versão 2**.
4. Na seção **Solicitantes**, insira as informações de **Comunidade** e **Rede**.

> Por padrão, a string da comunidade é pública e a rede é localhost. Você pode alterar essas configurações padrão.

5. **Opcional:** Para adicionar outro solicitante, clique em **Adicionar um Solicitante** e insira as informações de **Nome da Comunidade** e **Rede**.
6. Clique em **Salvar alterações**.

Encontre mais informações

- Configurar traps SNMP
- Visualize os dados do objeto gerenciado usando arquivos de base de informações de gerenciamento.

Configurar um usuário SNMP USM

Ao ativar o SNMP versão 3, você precisa configurar um usuário USM para receber solicitações SNMP autorizadas.

1. Clique em **Cluster** > **SNMP**.
2. Em **Configurações gerais de SNMP**, clique em **Sim** para ativar o SNMP.
3. Na lista **Versão**, selecione **Versão 3**.
4. Na seção **Usuários da USM**, insira o nome, a senha e a frase secreta.
5. **Opcional:** Para adicionar outro usuário do USM, clique em **Adicionar um usuário do USM** e insira o nome, a senha e a frase secreta.
6. Clique em **Salvar alterações**.

Configurar traps SNMP

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

Quando os traps SNMP estão habilitados, o cluster SolidFire gera traps associados a entradas de log de eventos e alertas do sistema. Para receber notificações SNMP, você precisa escolher os traps que devem ser gerados e identificar os destinatários das informações do trap. Por padrão, nenhuma armadilha é gerada.

1. Clique em **Cluster** > **SNMP**.
2. Selecione um ou mais tipos de traps na seção **Configurações de SNMP Trap** que o sistema deve gerar:

- Armadilhas de falha de cluster
- Armadilhas de falhas resolvidas em cluster
- Armadilhas de Eventos em Cluster

3. Na seção **Destinatários da Trap**, insira as informações de host, porta e string da comunidade para um destinatário.
4. **Opcional**: Para adicionar outro destinatário de trap, clique em **Adicionar um destinatário de trap** e insira as informações de host, porta e string da comunidade.
5. Clique em **Salvar alterações**.

Visualize os dados do objeto gerenciado usando arquivos de base de informações de gerenciamento.

Você pode visualizar e baixar os arquivos MIB (Management Information Base) 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
- Estatísticas de volume por conta
- Estatísticas do nó
- Outros dados, como relatórios, erros e eventos do sistema.

O sistema também oferece suporte ao acesso ao arquivo MIB que contém os pontos de acesso de nível superior (OIDs) para produtos da série SF.

Passos

1. Clique em **Cluster** > **SNMP**.
2. Em **SNMP MIBs**, clique no arquivo MIB que deseja baixar.
3. Na janela de download que se abrir, 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 depois que esta for adicionada com sucesso ao cluster. Você pode usar a interface do usuário do Element para gerenciar unidades.

Detalhes das unidades

A página Unidades na guia Cluster fornece uma lista das unidades ativas no cluster. Você pode filtrar a página selecionando entre as abas Ativos, Disponíveis, Removendo, Excluindo e Com Falha.

Ao inicializar um cluster pela primeira vez, a lista de unidades ativas estará vazia. Você pode adicionar unidades que não estejam atribuídas a um cluster e que sejam listadas na guia Disponível após a criação de

um novo cluster 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 é atribuído quando o nó é adicionado ao cluster.

- **Nome do nó**

  O nome do nó que abriga a unidade.

- **Vaga**

  O número do slot onde a unidade está fisicamente localizada.

- **Capacidade**

  O tamanho do disco rígido, em GB.

- **Serial**

  O número de série da unidade.

- **Desperdício restante**

  Indicador de nível de desgaste.

  O sistema de armazenamento informa a quantidade aproximada de desgaste disponível em cada unidade de estado sólido (SSD) para gravação e apagamento de dados. Um disco rígido que consumiu 5% de seus ciclos de gravação e apagamento para os quais foi projetado apresenta 95% de desgaste restante. O sistema não atualiza automaticamente as informações sobre o desgaste do disco; você pode atualizar a página ou fechá-la e recarregá-la para atualizar as informações.

- **Tipo**

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

Para maiores informações

- "Documentação do SolidFire e do Element Software"
- "Plug-in NetApp Element para vCenter Server"

Gerenciar nós

Gerenciar nós

Você pode gerenciar o armazenamento 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 tornada inutilizável ("isolada"), para que ele esteja em conformidade com a regra de capacidade. Essa situação permanece inalterada até que mais espaço de armazenamento seja adicionado. Se um nó muito grande for adicionado e também desobedecer à regra de capacidade, o nó anteriormente isolado deixará de estar isolado, enquanto o nó recém-adicionado ficará isolado. A capacidade deve sempre ser adicionada em pares para evitar que isso aconteça. Quando um nó fica inativo, uma falha de cluster apropriada é lançada.

Encontre mais informações

Adicionar um nó a um cluster

Adicionar um nó a um cluster

Você pode adicionar nós a um cluster quando precisar de mais espaço de armazenamento ou após a criação do cluster. Os nós requerem configuração inicial quando são ligados pela primeira vez. Após a configuração do nó, ele aparece na lista de nós pendentes e você pode adicioná-lo a um cluster.

A versão do software em cada nó de um cluster deve ser compatível. Ao adicionar um nó a um cluster, o cluster instala a versão de cluster do software NetApp Element no novo nó, conforme necessário.

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

> Se um nó recém-adicionado representar mais de 50% da capacidade total do cluster, parte da capacidade desse nó será tornada inutilizável ("isolada"), para que ele esteja em conformidade com a regra de capacidade. Essa situação permanece inalterada até que mais espaço de armazenamento seja adicionado. Se um nó muito grande for adicionado e também desobedecer à regra de capacidade, o nó anteriormente isolado deixará de estar isolado, enquanto o nó recém-adicionado ficará isolado. A capacidade deve sempre ser adicionada em pares para evitar que isso aconteça. Quando um nó fica inativo, é lançada uma falha de cluster strandedCapacity.

"Vídeo da NetApp : Dimensionamento sob seu controle: Expandindo um cluster SolidFire"

Você pode adicionar nós aos dispositivos NetApp HCI .

Passos

1. Selecione **Cluster** > **Nós**.
2. Clique em **Pendente** para visualizar a lista de nós pendentes.

   Quando o processo de adição de nós estiver concluído, eles aparecerão na lista de nós ativos. Até então, os nós pendentes aparecem na lista de Pendentes Ativos.

   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. Faça um dos seguintes:

- Para adicionar nós individuais, clique no ícone **Ações** do nó que deseja adicionar.
- Para adicionar vários nós, selecione a caixa de seleção dos nós que deseja adicionar e, em seguida, **Ações em massa**. **Nota:** Se o nó que você está adicionando tiver uma versão do software Element diferente da versão em execução no cluster, o cluster atualizará o nó de forma assíncrona para a versão do software Element em execução no nó mestre do cluster. Após a atualização do nó, ele se adiciona automaticamente ao cluster. Durante esse processo assíncrono, o nó ficará em um estado pendingActive.

4. Clique em **Adicionar**.

   O nó aparece na lista de nós ativos.

Encontre mais informações

Versionamento e compatibilidade do Node.js

Versionamento e compatibilidade do Node.js

A compatibilidade do nó é baseada na versão do software Element instalada no nó. Os clusters de armazenamento baseados no software Element criam automaticamente uma imagem de um nó para a versão do software Element presente no cluster, caso o nó e o cluster não estejam em versões compatíveis.

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

- **Principal**

  O primeiro número indica a versão do software. Um nó com um número de componente principal específico não pode ser adicionado a um cluster que contenha nós com números de patch principal diferentes, nem é possível criar um cluster com nós de versões principais mistas.

- **Menor**

  O segundo número designa funcionalidades de software menores ou melhorias em funcionalidades de software existentes que foram adicionadas 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 nenhuma outra versão incremental do software Element que possua um componente secundário diferente. Por exemplo, a versão 11.0 não é compatível com a 11.1, e a versão 11.1 não é compatível com a 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, a versão 11.0.1 é compatível com a 11.0.2, e a versão 11.0.2 é compatível com a 11.0.3.

Os números de versão principal e secundária devem corresponder para garantir a compatibilidade. Os números dos microamplificadores não precisam ser idênticos para serem compatíveis.

Capacidade do cluster em um ambiente de nós mistos

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

A Série H é composta pelos nós H610S-1, H610S-2, H610S-4 e H410S. Esses nós são compatíveis com 10GbE e 25GbE.

É melhor não misturar nós criptografados com nós não 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 da série SF 4805, o maior nó que pode ser adicionado individualmente é um SF 9605. O limite de capacidade do cluster é calculado com base na perda potencial do maior nó nessa situação.

Dependendo da versão do seu software Element, os seguintes nós de armazenamento da série SF não são suportados:

Começando por…	Nó de armazenamento não suportado…
Elemento 12.8	• SF4805 • SF9605 • SF19210 • SF38410
Elemento 12.7	• SF2405 • SF9608
Elemento 12.0	• SF3010 • SF6010 • SF9010

Se você tentar atualizar um desses nós para uma versão não suportada do Element, verá um erro informando que o nó não é compatível com o Element 12.x.

Ver detalhes do nó

Você pode visualizar detalhes de nós individuais, como etiquetas de serviço, detalhes da unidade e gráficos com estatísticas de utilização e da unidade. A página Nós da aba Cluster fornece a coluna Versão, onde você pode visualizar a versão do software de cada nó.

Passos

1. Clique em **Cluster** > **Nós**.
2. Para visualizar os detalhes de um nó específico, clique no ícone **Ações** correspondente ao nó.
3. Clique em **Ver detalhes**.
4. Analise os detalhes do nó:
    - **ID do nó**: O ID do nó gerado pelo sistema.

- **Nome do nó**: O nome do host do nó.
- **Função do Nó**: A função que o nó desempenha no cluster. Valores possíveis:
  - Mestre do Cluster: O nó que executa tarefas administrativas em todo o cluster e contém o MVIP e o SVIP.
  - Nó de conjunto: Um nó que participa do cluster. Existem 3 ou 5 nós de conjunto, 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.
- **Utilização do nó**: A porcentagem de utilização do nó com base no calor do nó. O valor exibido é o recentPrimaryTotalHeat em porcentagem. Disponível a partir do Elemento 12.8.
- **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 da VLAN de gerenciamento**: O ID virtual para a rede local de gerenciamento.
- **ID da VLAN de armazenamento**: O ID virtual da rede local de armazenamento.
- **Versão**: A versão do software em execução em cada nó.
- **Porta de Replicação**: A porta usada nos nós para replicação remota.
- **Etiqueta de serviço**: O número de etiqueta de serviço exclusivo atribuído ao nó.
- **Domínio de Proteção Personalizado**: O domínio de proteção personalizado atribuído ao nó.

Veja os detalhes das portas Fibre Channel.

Você pode visualizar detalhes das portas Fibre Channel, como status, nome e endereço da porta, na página Portas FC.

Veja informações sobre as portas Fibre Channel conectadas ao cluster.

Passos

1. Clique em **Cluster** > **Portas FC**.
2. Para filtrar as informações desta página, clique em **Filtrar**.
3. Confira os detalhes:
   - **ID do nó**: 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.
   - **Porta HBA**: Porta física no adaptador de barramento de host Fibre Channel (HBA).
   - **WWNN**: O nome do nó mundial.
   - **WWPN**: Nome do porto mundial de destino.

- **WWN do switch**: Nome mundial do switch Fibre Channel.
- **Estado da Porta**: Estado atual da porta.
- **ID da porta nPort**: O ID da porta do nó na estrutura Fibre Channel.
- **Velocidade**: A velocidade negociada do Fibre Channel. Os valores possíveis são os seguintes:
  - 4Gbps
  - 8Gbps
  - 16Gbps

Encontre mais informações

- "Documentação do SolidFire e do Element Software"
- "Plug-in NetApp Element para vCenter Server"

Gerenciar redes virtuais

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 único cluster. As conexões com o cluster são segregadas na pilha de rede por meio do uso de VLAN tagging.

Encontre mais informações

- Adicionar uma rede virtual
- Habilitar roteamento e encaminhamento virtuais
- Editar uma rede virtual
- Editar VLANs VRF
- Excluir uma rede virtual

Adicionar uma rede virtual

Você pode adicionar uma nova rede virtual a uma configuração de cluster para habilitar uma conexão de ambiente multi-inquilino a um cluster que executa o software Element.

O que você vai precisar

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

Para esta configuração, você deve considerar os seguintes critérios:

- As VLANs que não possuem VRF habilitado exigem que os iniciadores estejam na mesma sub-rede que o SVIP.
- As VLANs com suporte a VRF não exigem que os iniciadores estejam na mesma sub-rede que o SVIP, e o roteamento é suportado.

- O SVIP padrão não exige que os iniciadores estejam na mesma sub-rede que o SVIP, e o roteamento é suportado.

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

Passos

1. Clique em **Cluster** > **Rede**.
2. Clique em **Criar VLAN**.
3. Na caixa de diálogo **Criar uma nova VLAN**, insira os valores nos seguintes campos:
   - **Nome da VLAN**
   - **Etiqueta VLAN**
   - **SVIP**
   - **Máscara de rede**
   - (Opcional) **Descrição**
4. Insira o endereço **IP inicial** para o intervalo de endereços IP em **Blocos de Endereços IP**.
5. Insira o **Tamanho** do intervalo de IP como o número de endereços IP a serem incluídos no bloco.
6. Clique em **Adicionar um bloco** para adicionar um bloco não contínuo de endereços IP para esta VLAN.
7. Clique em **Criar VLAN**.

Veja os detalhes da rede virtual

Passos

1. Clique em **Cluster** > **Rede**.
2. Revise os detalhes.
   - **ID**: Identificação única da rede VLAN, atribuída pelo sistema.
   - **Nome**: Nome exclusivo atribuído pelo usuário para a rede VLAN.
   - **Etiqueta VLAN**: Etiqueta 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. O VRF deve estar ativado.
   - **VRF ativado**: Indica se o roteamento e encaminhamento virtual está ativado ou não.
   - **IPs Utilizados**: O intervalo de endereços IP da rede virtual utilizados para a rede virtual.

Habilitar roteamento e encaminhamento virtuais

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

Você só pode habilitar o VRF no momento da criação de uma VLAN. Se você quiser voltar a usar uma VLAN sem VRF, você deve excluir e recriar a VLAN.

1. Clique em **Cluster** > **Rede**.
2. Para ativar o VRF em uma nova VLAN, selecione **Criar VLAN**.
   a. Insira as informações relevantes para a nova VRF/VLAN. Consulte Adicionando uma rede virtual.
   b. Selecione a caixa de seleção **Ativar VRF**.
   c. **Opcional**: Insira um gateway.
3. Clique em **Criar VLAN**.

Encontre mais informações

Adicionar uma rede virtual

Editar uma rede virtual

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

Caso existam sessões iSCSI, de replicação remota ou outras sessões de rede em andamento, a modificação poderá falhar.

Ao gerenciar o tamanho dos intervalos de endereços IP de VLANs, 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 endereços IP que foi adicionado após o intervalo de endereços IP inicial, mas não pode redimensionar um bloco de IP removendo endereços IP.
- Ao tentar remover endereços IP, seja do intervalo de endereços IP inicial ou de um bloco de IP, que estejam em uso por nós no cluster, a operação pode falhar.
- Não é possível reatribuir endereços IP específicos em uso a outros nós do cluster.

Você pode adicionar um bloco de endereços IP seguindo o procedimento abaixo:

1. Selecione **Cluster** > **Rede**.
2. Selecione o ícone Ações da VLAN que deseja editar.
3. Selecione **Editar**.
4. Na caixa de diálogo **Editar VLAN**, insira os novos atributos para a 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 artigos da base de conhecimento sobre resolução de problemas

Acesse os artigos da Base de Conhecimento para obter ajuda na resolução de problemas relacionados ao gerenciamento de seus intervalos de endereços IP de VLAN.

- "Aviso de IP duplicado após adicionar um nó de armazenamento em uma VLAN no cluster Element."
- "Como determinar quais IPs de VLAN estão em uso e a quais nós esses IPs estão atribuídos no Element?"

Editar VLANs VRF

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

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

Excluir 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** > **Rede**.
2. Clique no ícone Ações da VLAN que deseja excluir.
3. Clique em **Excluir**.
4. Confirme a mensagem.

Encontre mais informações

Editar uma rede virtual

Informações sobre direitos autorais

Informações sobre marcas comerciais