Gerencie seu sistema

Element Software

NetApp
November 19, 2025

This PDF was generated from https://docs.netapp.com/pt-br/element-software-123/storage/task_system_manage_mfa_set_up_multi_factor_authentication.html on November 19, 2025. Always check docs.netapp.com for the latest.

Índice

Gerencie seu sistema . . . 1
- Para mais informações . . . 1
- Ativar a autenticação multifator . . . 1
  - Configurar a autenticação multifator . . . 1
  - Informações adicionais para autenticação multifator . . . 2
- Configure as definições do cluster . . . 2
  - Encontre mais informações . . . 3
  - Ative e desative a criptografia em repouso para um cluster . . . 3
  - Defina o limite máximo do cluster . . . 4
  - Ativar e desativar o acesso ao suporte . . . 5
  - Gerenciar os termos de uso banner . . . 5
  - Defina o Network Time Protocol (Protocolo de hora de rede) . . . 6
  - Gerenciar SNMP . . . 8
  - Gerenciar unidades . . . 10
  - Gerenciar nós . . . 11
  - Veja os detalhes das portas Fibre Channel . . . 14
  - Gerenciar redes virtuais . . . 15
- Criar um cluster compatível com unidades FIPS . . . 18
  - Evite misturar nós para unidades FIPS . . . 18
  - Ative a criptografia em repouso . . . 19
  - Identificar se os nós estão prontos para o recurso unidades FIPS . . . 19
  - Ative o recurso unidades FIPS . . . 20
  - Verifique o status da unidade FIPS . . . 20
  - Solucionar problemas do recurso da unidade FIPS . . . 21
- Ative o FIPS 140-2 para HTTPS no cluster . . . 21
  - Encontre mais informações . . . 22
  - Cifras SSL . . . 22
- Comece a usar o gerenciamento de chaves externas . . . 24
  - Configurar o gerenciamento de chaves externas . . . 24
  - Rechavear criptografia de software na chave mestra em repouso . . . 25
  - Recuperar chaves de autenticação inacessíveis ou inválidas . . . 28
  - Comandos externos da API de gerenciamento de chaves . . . 28

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 autocriptografia (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 carateres.

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 carateres.

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 carateres 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 carateres 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 secção **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 carateres 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 carateres 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 conetado 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: "CreateKeyProviderKmip"

   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: "CreateKeyServerKmip" "TestKeyServerKmip"

      Se o teste falhar, verifique a conetividade 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: "AddKeyServerToProviderKmip" "TestKeyProviderKmip"

      Se o teste falhar, verifique a conetividade 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:

- CreateKeyServerKmip
- ModifyKeyServerKmip
- DeleteKeyServerKmip
- GetKeyServerKmip
- ListKeyServersKmip
- TestKeyServerKmip

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

- CreateKeyProviderKmip

- DeleteKeyProviderKmip
- AddKeyServerToProviderKmip
- RemoveKeyServerFromProviderKmip
- GetKeyProviderKmip
- ListKeyProvidersKmip
- RekeySoftwareEncryptionAtRestMasterKey
- TestKeyProviderKmip

Para obter informações sobre os métodos de API, "Informações de referência da API"consulte .

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 DESTE DOCUMENTO. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTE SOFTWARE, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

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

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

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

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

Informações sobre marcas comerciais

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