Configurar o gerenciamento de chaves externas

ONTAP 9

NetApp
January 17, 2025

Índice

Configurar o gerenciamento de chaves externas

Configurar uma visão geral do gerenciamento de chaves externas

Você pode usar um ou mais servidores de gerenciamento de chaves externos para proteger as chaves que o cluster usa para acessar dados criptografados. Um servidor de gerenciamento de chaves externo é um sistema de terceiros em seu ambiente de storage que serve chaves para nós que usam o Key Management Interoperability Protocol (KMIP).

Para o ONTAP 9.1 e versões anteriores, as LIFs de gerenciamento de nós devem ser atribuídas a portas configuradas com a função de gerenciamento de nó antes de usar o gerenciador de chaves externo.

O NetApp volume Encryption (NVE) pode ser implementado com o Gerenciador de chaves integrado no ONTAP 9.1 e posterior. No ONTAP 9.3 e posterior, o NVE pode ser implementado com gerenciamento de chaves externas (KMIP) e Gerenciador de chaves integrado. A partir do ONTAP 9.11,1, você pode configurar vários gerenciadores de chaves externos em um cluster. Consulte Configurar servidores de chaves em cluster.

Colete informações de rede no ONTAP 9.2 e anteriores

Se você estiver usando o ONTAP 9.2 ou anterior, você deve preencher a Planilha de configuração de rede antes de ativar o gerenciamento de chaves externas.

A partir do ONTAP 9.3, o sistema deteta automaticamente todas as informações de rede necessárias.

Item	Notas	Valor
Nome da interface de rede de gerenciamento de chaves		
Endereço IP da interface de rede de gerenciamento de chaves	Endereço IP do LIF de gerenciamento de nós, no formato IPv4 ou IPv6	
Comprimento do prefixo da rede IPv6 da interface de rede de gerenciamento de chaves	Se você estiver usando IPv6, o comprimento do prefixo de rede IPv6	
Máscara de sub-rede da interface de rede de gerenciamento de chaves		
Endereço IP do gateway de interface de rede de gerenciamento de chaves		

Endereço IPv6 para a interface de rede do cluster	Necessário somente se você estiver usando IPv6 para a interface de rede de gerenciamento de chaves	
Número da porta para cada servidor KMIP	Opcional. O número da porta deve ser o mesmo para todos os servidores KMIP. Se você não fornecer um número de porta, o padrão será a porta 5696, que é a porta atribuída pela IANA (Internet Assigned Numbers Authority) para KMIP.	
Nome da etiqueta da chave	Opcional. O nome da tag chave é usado para identificar todas as chaves pertencentes a um nó. O nome da etiqueta de chave padrão é o nome do nó.	

Informações relacionadas

"Relatório técnico da NetApp 3954: Requisitos e procedimentos de pré-instalação de criptografia de armazenamento da NetApp para o Gerenciador de chaves vitalício"

"Relatório técnico da NetApp 4074: Requisitos e procedimentos de pré-instalação da criptografia de armazenamento NetApp para o KeySecure"

Instale certificados SSL no cluster

O cluster e o servidor KMIP usam certificados SSL KMIP para verificar a identidade uns dos outros e estabelecer uma conexão SSL. Antes de configurar a conexão SSL com o servidor KMIP, você deve instalar os certificados SSL do cliente KMIP para o cluster e o certificado público SSL para a autoridade de certificação raiz (CA) do servidor KMIP.

Sobre esta tarefa

Em um par de HA, ambos os nós precisam usar os mesmos certificados KMIP SSL públicos e privados. Se você conectar vários pares de HA ao mesmo servidor KMIP, todos os nós dos pares de HA precisarão usar os mesmos certificados KMIP SSL públicos e privados.

Antes de começar

- O tempo deve ser sincronizado no servidor criando os certificados, o servidor KMIP e o cluster.
- Você deve ter obtido o certificado de cliente KMIP SSL público para o cluster.
- Você deve ter obtido a chave privada associada ao certificado de cliente SSL KMIP para o cluster.
- O certificado de cliente SSL KMIP não deve ser protegido por senha.
- Você deve ter obtido o certificado público SSL para a autoridade de certificação raiz (CA) do servidor KMIP.
- Em um ambiente MetroCluster, é necessário instalar os mesmos certificados SSL KMIP em ambos os clusters.

Você pode instalar os certificados de cliente e servidor no servidor KMIP antes ou depois de instalar os certificados no cluster.

Passos

1. Instale os certificados de cliente SSL KMIP para o cluster:

   ```
   security certificate install -vserver admin_svm_name -type client
   ```

   Você será solicitado a inserir os certificados SSL KMIP público e privado.

   ```
   cluster1::> security certificate install -vserver cluster1 -type client
   ```

2. Instale o certificado público SSL para a autoridade de certificação raiz (CA) do servidor KMIP:

   ```
   security certificate install -vserver admin_svm_name -type server-ca
   ```

   ```
   cluster1::> security certificate install -vserver cluster1 -type server-ca
   ```

Habilite o gerenciamento de chaves externas no ONTAP 9.6 e posterior (baseado em hardware)

Você pode usar um ou mais servidores KMIP para proteger as chaves que o cluster usa para acessar dados criptografados. É possível conectar até quatro servidores KMIP a um nó. Recomenda-se um mínimo de dois servidores para redundância e recuperação de desastres.

A partir do ONTAP 9.11,1, você pode adicionar até 3 servidores de chaves secundárias por servidor de chaves primárias para criar um servidor de chaves em cluster. Para obter mais informações, Configurar servidores de chaves externas em clusterconsulte .

Antes de começar

- Os certificados de cliente e servidor KMIP SSL devem ter sido instalados.
- Você deve ser um administrador de cluster para executar esta tarefa.
- Você deve configurar o ambiente MetroCluster antes de configurar um gerenciador de chaves externo.
- Em um ambiente MetroCluster, é necessário instalar o mesmo certificado KMIP SSL em ambos os clusters.

Passos

1. Configurar a conetividade do gerenciador de chaves para o cluster:

   ```
   security key-manager external enable -vserver admin_SVM -key-servers
   host_name|IP_address:port,... -client-cert client_certificate -server-ca-cert
   server_CA_certificates
   ```

- O `security key-manager external enable` comando substitui o `security key-manager setup` comando. Você pode executar o `security key-manager external modify` comando para alterar a configuração de gerenciamento de chaves externas. Para obter a sintaxe completa do comando, consulte as páginas man.
- Em um ambiente MetroCluster, se você estiver configurando o gerenciamento de chaves externas para o SVM de administrador, repita o `security key-manager external enable` comando no cluster de parceiros.

O comando a seguir habilita o gerenciamento de chaves externas para `cluster1` com três servidores de chaves externas. O primeiro servidor de chaves é especificado usando seu nome de host e porta, o segundo é especificado usando um endereço IP e a porta padrão, e o terceiro é especificado usando um endereço IPv6 e porta:

```
cluster1::> security key-manager external enable -key-servers
ks1.local:15696,10.0.0.10,[fd20:8b1e:b255:814e:32bd:f35c:832c:5a09]:1234
-client-cert AdminVserverClientCert -server-ca-certs
AdminVserverServerCaCert
```

2. Verifique se todos os servidores KMIP configurados estão conetados:

`security key-manager external show-status -node node_name -vserver SVM -key -server host_name|IP_address:port -key-server-status available|not-responding|unknown`

O `security key-manager external show-status` comando substitui o `security key-manager show -status` comando. Para obter a sintaxe completa do comando, consulte a página man.

```
cluster1::> security key-manager external show-status

Node  Vserver  Key Server                                       Status
----  -------  ---------------------------------------
-------------
node1
      cluster1
               10.0.0.10:5696                                   available
               fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234   available
               ks1.local:15696                                  available
node2
      cluster1
               10.0.0.10:5696                                   available
               fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234   available
               ks1.local:15696                                  available

6 entries were displayed.
```

Habilite o gerenciamento de chaves externas no ONTAP 9.5 e versões anteriores (baseado em hardware)

Você pode usar um ou mais servidores KMIP para proteger as chaves que o cluster usa para acessar dados criptografados. É possível conectar até quatro servidores KMIP a um nó. Recomenda-se um mínimo de dois servidores para redundância e recuperação de desastres.

Sobre esta tarefa

O ONTAP configura a conectividade do servidor KMIP para todos os nós no cluster.

Antes de começar

- Os certificados de cliente e servidor KMIP SSL devem ter sido instalados.
- Você deve ser um administrador de cluster para executar esta tarefa.
- Você deve configurar o ambiente MetroCluster antes de configurar um gerenciador de chaves externo.
- Em um ambiente MetroCluster, é necessário instalar o mesmo certificado KMIP SSL em ambos os clusters.

Passos

1. Configurar a conectividade do gerenciador de chaves para nós de cluster:

   `security key-manager setup`

   A configuração do gerenciador de chaves é iniciada.

   Em um ambiente MetroCluster, você deve executar esse comando nos dois clusters.

2. Insira a resposta apropriada em cada prompt.
3. Adicionar um servidor KMIP:

   `security key-manager add -address key_management_server_ipaddress`

   ```
   clusterl::> security key-manager add -address 20.1.1.1
   ```

   Em um ambiente MetroCluster, você deve executar esse comando nos dois clusters.

4. Adicione um servidor KMIP adicional para redundância:

   `security key-manager add -address key_management_server_ipaddress`

   ```
   clusterl::> security key-manager add -address 20.1.1.2
   ```

   Em um ambiente MetroCluster, você deve executar esse comando nos dois clusters.

5. Verifique se todos os servidores KMIP configurados estão conetados:

```
security key-manager show -status
```

Para obter a sintaxe completa do comando, consulte a página man.

```
cluster1::> security key-manager show -status

Node            Port      Registered Key Manager  Status
--------------  ----      ----------------------  ---------------
cluster1-01     5696      20.1.1.1                available
cluster1-01     5696      20.1.1.2                available
cluster1-02     5696      20.1.1.1                available
cluster1-02     5696      20.1.1.2                available
```

6. Opcionalmente, converta volumes de texto simples em volumes criptografados.

```
volume encryption conversion start
```

Um gerenciador de chaves externo deve estar totalmente configurado antes de converter os volumes. Em um ambiente MetroCluster, um gerenciador de chaves externo deve ser configurado em ambos os locais.

Configurar servidores de chaves externas em cluster no ONTAP

A partir do ONTAP 9.11,1, é possível configurar a conetividade com servidores de gerenciamento de chaves externos em cluster em um SVM. Com servidores de chaves em cluster, você pode designar servidores de chaves primárias e secundárias em um SVM. Ao Registrar chaves, o ONTAP tentará primeiro acessar um servidor de chaves primárias antes de tentar acessar sequencialmente servidores secundários até que a operação seja concluída com êxito, evitando a duplicação de chaves.

Os servidores de chaves externas podem ser usados para chaves NSE, NVE, NAE e SED. Um SVM pode dar suporte a até quatro servidores KMIP primários externos. Cada servidor principal pode suportar até três servidores de chaves secundárias.

Antes de começar

- "O gerenciamento de chaves KMIP deve estar habilitado para SVM".
- Esse processo só suporta servidores-chave que usam KMIP. Para obter uma lista de servidores de chaves suportados, verifique o "Ferramenta de Matriz de interoperabilidade do NetApp".
- Todos os nós no cluster devem estar executando o ONTAP 9.11,1 ou posterior.
- A ordem dos argumentos da lista de servidores no `-secondary-key-servers` parâmetro reflete a ordem de acesso dos servidores de gerenciamento de chaves externas (KMIP).
- Saiba mais sobre os comandos descritos neste procedimento no "Referência do comando ONTAP".

Crie um servidor de chaves em cluster

O procedimento de configuração depende se você configurou ou não um servidor de chave primária.

Adicionar servidores de chaves primárias e secundárias a uma SVM

1. Confirme se nenhum gerenciamento de chaves foi habilitado para o cluster:
   `security key-manager external show -vserver` *`svm_name`* Se o SVM já tiver o máximo de quatro servidores de chaves primárias ativados, você deverá remover um dos servidores de chaves primárias existentes antes de adicionar um novo.
2. Ative o gerenciador de chaves principal:
   `security key-manager external enable -vserver` *`svm_name`* `-key-servers` *`server_ip`* `-client-cert` *`client_cert_name`* `-server-ca-certs` *`server_ca_cert_names`*
3. Modifique o servidor de chaves primárias para adicionar servidores de chaves secundárias. O `-secondary-key-servers` parâmetro aceita uma lista separada por vírgulas de até três servidores-chave.
   `security key-manager external modify-server -vserver` *`svm_name`* `-key-servers` *`primary_key_server`* `-secondary-key-servers` *`list_of_key_servers`*

Adicione servidores de chave secundária a um servidor de chave primária existente

1. Modifique o servidor de chaves primárias para adicionar servidores de chaves secundárias. O `-secondary-key-servers` parâmetro aceita uma lista separada por vírgulas de até três servidores-chave.
   `security key-manager external modify-server -vserver` *`svm_name`* `-key-servers` *`primary_key_server`* `-secondary-key-servers` *`list_of_key_servers`* Para obter mais informações sobre servidores de chaves secundárias, [mod-secondary]consulte .

Modificar servidores de chaves em cluster

Você pode modificar clusters de servidores de chave externos alterando o status (primário ou secundário) de servidores de chave específicos, adicionando e removendo servidores de chave secundária ou alterando a ordem de acesso de servidores de chave secundária.

Converta servidores de chaves primárias e secundárias

Para converter um servidor de chave primária em um servidor de chave secundário, primeiro remova-o do SVM com o `security key-manager external remove-servers` comando.

Para converter um servidor de chave secundária em um servidor de chave primária, primeiro você deve remover o servidor de chave secundária de seu servidor de chave primária existente. [mod-secondary]Consulte . Se você converter um servidor de chaves secundário para um servidor primário ao remover uma chave existente, tentar adicionar um novo servidor antes de concluir a remoção e conversão pode resultar na duplicação de chaves.

Modificar servidores de chaves secundárias

Os servidores de chaves secundárias são gerenciados com o `-secondary-key-servers` parâmetro `security key-manager external modify-server` do comando. O `-secondary-key-servers` parâmetro aceita uma lista separada por vírgulas. A ordem especificada dos servidores de chaves secundárias na lista determina a sequência de acesso para os servidores de chaves secundárias. A ordem de

acesso pode ser modificada executando o comando `security key-manager external modify-server` com os servidores de chaves secundárias inseridos em uma sequência diferente.

Para remover um servidor de chave secundário, os `-secondary-key-servers` argumentos devem incluir os servidores de chave que você deseja manter ao omitir o que deve ser removido. Para remover todos os servidores de chaves secundárias, use o argumento `-`, significando nenhum.

Saiba mais sobre o comando link:https://docs.NetApp.com/US-en/ONTAP-cli/[`security key-manager external` ONTAP

Crie chaves de autenticação no ONTAP 9.6 e posterior

Você pode usar o `security key-manager key create` comando para criar as chaves de autenticação para um nó e armazená-las nos servidores KMIP configurados.

Sobre esta tarefa

Se a configuração de segurança exigir que você use chaves diferentes para autenticação de dados e autenticação FIPS 140-2-2, você deve criar uma chave separada para cada uma. Se esse não for o caso, você poderá usar a mesma chave de autenticação para conformidade com FIPS usada para acesso aos dados.

O ONTAP cria chaves de autenticação para todos os nós no cluster.

- Este comando não é suportado quando o Onboard Key Manager está ativado. No entanto, duas chaves de autenticação são criadas automaticamente quando o Onboard Key Manager está ativado. As teclas podem ser visualizadas com o seguinte comando:

  ```
  security key-manager key query -key-type NSE-AK
  ```

- Você receberá um aviso se os servidores de gerenciamento de chaves configurados já estiverem armazenando mais de 128 chaves de autenticação.
- Você pode usar o `security key-manager key delete` comando para excluir quaisquer chaves não utilizadas. O `security key-manager key delete` comando falha se a chave dada estiver atualmente em uso pelo ONTAP. (Você deve ter Privileges maior que "'admin'" para usar este comando.)

  Em um ambiente MetroCluster, antes de excluir uma chave, certifique-se de que a chave não está em uso no cluster de parceiros. Você pode usar os seguintes comandos no cluster de parceiros para verificar se a chave não está em uso:

  - `storage encryption disk show -data-key-id key-id`
  - `storage encryption disk show -fips-key-id key-id`

Antes de começar

Você deve ser um administrador de cluster para executar esta tarefa.

Passos

1. Crie as chaves de autenticação para nós de cluster:

   ```
   security key-manager key create -key-tag passphrase_label -prompt-for-key
   true|false
   ```

A configuração `prompt-for-key=true` faz com que o sistema solicite ao administrador do cluster a senha a ser usada ao autenticar unidades criptografadas. Caso contrário, o sistema gera automaticamente uma frase-passe de 32 bytes. O `security key-manager key create` comando substitui o `security key-manager create-key` comando. Para obter a sintaxe completa do comando, consulte a página man.

O exemplo a seguir cria as chaves de autenticação para `cluster1`o , gerando automaticamente uma senha de 32 bytes:

```
cluster1::> security key-manager key create
Key ID:
000000000000000002000000000001006268333f870860128fbe17d393e5083b0000000000000000
```

2. Verifique se as chaves de autenticação foram criadas:

   `security key-manager key query -node node`

   O `security key-manager key query` comando substitui o `security key-manager query key` comando. Para obter a sintaxe completa do comando, consulte a página man. O ID da chave exibido na saída é um identificador usado para se referir à chave de autenticação. Não é a chave de autenticação real ou a chave de criptografia de dados.

   O exemplo a seguir verifica se as chaves de autenticação foram criadas para `cluster1`:

```
cluster1::> security key-manager key query
       Vserver: cluster1
   Key Manager: external
          Node: node1

Key Tag                                  Key Type  Restored
---------------------------------------  --------  --------
node1                                    NSE-AK    yes
    Key ID:
000000000000000002000000000001000c11b3863f78c2273343d7ec5a67762e00000000
00000000
node1                                    NSE-AK    yes
    Key ID:
000000000000000002000000000001006f4e2513353a674305872a4c9f3bf79700000000
00000000

       Vserver: cluster1
   Key Manager: external
          Node: node2

Key Tag                                  Key Type  Restored
---------------------------------------  --------  --------
node2                                    NSE-AK    yes
    Key ID:
000000000000000002000000000001000c11b3863f78c2273343d7ec5a67762e00000000
00000000
node2                                    NSE-AK    yes
    Key ID:
000000000000000002000000000001006f4e2513353a674305872a4c9f3bf79700000000
00000000
```

Crie chaves de autenticação no ONTAP 9.5 e anteriores

Você pode usar o `security key-manager create-key` comando para criar as chaves de autenticação para um nó e armazená-las nos servidores KMIP configurados.

Sobre esta tarefa

Se a configuração de segurança exigir que você use chaves diferentes para autenticação de dados e autenticação FIPS 140-2-2, você deve criar uma chave separada para cada uma. Se esse não for o caso, você poderá usar a mesma chave de autenticação para conformidade com o FIPS usada para acesso aos dados.

O ONTAP cria chaves de autenticação para todos os nós no cluster.

- Este comando não é suportado quando o gerenciamento de chaves integradas está habilitado.

- Você receberá um aviso se os servidores de gerenciamento de chaves configurados já estiverem armazenando mais de 128 chaves de autenticação.

  Você pode usar o software do servidor de gerenciamento de chaves para excluir quaisquer chaves não utilizadas e, em seguida, executar o comando novamente.

Antes de começar

Você deve ser um administrador de cluster para executar esta tarefa.

Passos

1. Crie as chaves de autenticação para nós de cluster:

   `security key-manager create-key`

   Para obter a sintaxe de comando completa, consulte a página man para o comando.

   > O ID da chave exibido na saída é um identificador usado para se referir à chave de autenticação. Não é a chave de autenticação real ou a chave de criptografia de dados.

   O exemplo a seguir cria as chaves de autenticação para `cluster1`:

   ```
   cluster1::> security key-manager create-key
      (security key-manager create-key)
   Verifying requirements...

   Node: cluster1-01
   Creating authentication key...
   Authentication key creation successful.
   Key ID: F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C

   Node: cluster1-01
   Key manager restore operation initialized.
   Successfully restored key information.

   Node: cluster1-02
   Key manager restore operation initialized.
   Successfully restored key information.
   ```

2. Verifique se as chaves de autenticação foram criadas:

   `security key-manager query`

   Para obter a sintaxe completa do comando, consulte a página man.

   O exemplo a seguir verifica se as chaves de autenticação foram criadas para `cluster1`:

```
cluster1::> security key-manager query

  (security key-manager query)

          Node: cluster1-01
   Key Manager: 20.1.1.1
 Server Status: available

Key Tag        Key Type  Restored
-------------  --------  --------
cluster1-01    NSE-AK    yes
       Key ID:
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C


          Node: cluster1-02
   Key Manager: 20.1.1.1
 Server Status: available

Key Tag        Key Type  Restored
-------------  --------  --------
cluster1-02    NSE-AK    yes
       Key ID:
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
```

Atribuir uma chave de autenticação de dados a uma unidade FIPS ou SED (gerenciamento de chaves externas)

Você pode usar o `storage encryption disk modify` comando para atribuir uma chave de autenticação de dados a uma unidade FIPS ou SED. Os nós de cluster usam essa chave para bloquear ou desbloquear dados criptografados na unidade.

Sobre esta tarefa

Uma unidade com autocriptografia é protegida contra acesso não autorizado somente se o ID da chave de autenticação estiver definido como um valor não padrão. O ID seguro do fabricante (MSID), que tem ID de chave 0x0, é o valor padrão para unidades SAS. Para unidades NVMe, o valor padrão é uma chave nula, representada como um ID de chave em branco. Quando você atribui o ID da chave a uma unidade de autocriptografia, o sistema altera o ID da chave de autenticação para um valor não padrão.

Este procedimento não causa interrupções.

Antes de começar

Você deve ser um administrador de cluster para executar esta tarefa.

Passos

1. Atribuir uma chave de autenticação de dados a uma unidade FIPS ou SED:

   `storage encryption disk modify -disk *disk_ID* -data-key-id *key_ID*`

   Para obter a sintaxe de comando completa, consulte a página man para o comando.

   > Você pode usar o `security key-manager query -key-type NSE-AK` comando para exibir IDs de chave.

   ```
   cluster1::> storage encryption disk modify -disk 0.10.* -data-key-id
   F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C

   Info: Starting modify on 14 disks.
         View the status of the operation by using the
         storage encryption disk show-status command.
   ```

2. Verifique se as chaves de autenticação foram atribuídas:

   `storage encryption disk show`

   Para obter a sintaxe completa do comando, consulte a página man.

   ```
   cluster1::> storage encryption disk show
   Disk    Mode Data Key ID
   -----   ----
   ------------------------------------------------------------------
   0.0.0   data
   F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
   0.0.1   data
   F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
   [...]
   ```

Informações sobre direitos autorais

Informações sobre marcas comerciais