Gerencie a criptografia com a CLI

ONTAP 9

NetApp
January 17, 2025

Índice

Gerencie a criptografia com a CLI

Visão geral da criptografia NetApp

A NetApp oferece tecnologias de criptografia baseadas em software e hardware para garantir que os dados em repouso não possam ser lidos se o meio de storage for reutilizado, devolvido, extraviado ou roubado.

- A criptografia baseada em software usando o NetApp volume Encryption (NVE) é compatível com a criptografia de dados, um volume de cada vez
- A criptografia baseada em hardware usando o NetApp Storage Encryption (NSE) oferece suporte à criptografia de disco total (FDE) dos dados conforme são gravados.

Configurar a encriptação de volume NetApp

Configurar a visão geral da encriptação de volume do NetApp

O NetApp volume Encryption (NVE) é uma tecnologia baseada em software para criptografar dados em repouso, um volume de cada vez. Uma chave de criptografia acessível somente ao sistema de storage garante que os dados de volume não possam ser lidos se o dispositivo subjacente for reutilizado, retornado, extraviado ou roubado.

Compreender o NVE

Com o NVE, os metadados e os dados (incluindo cópias Snapshot) são criptografados. O acesso aos dados é dado por uma chave exclusiva XTS-AES-256, uma por volume. Um servidor de gerenciamento de chaves externo ou OKM (Onboard Key Manager) serve chaves para nós:

- O 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). É uma prática recomendada configurar servidores de gerenciamento de chaves externos em um sistema de armazenamento diferente dos seus dados.
- O Gerenciador de chaves integrado é uma ferramenta integrada que serve chaves para nós do mesmo sistema de storage que seus dados.

A partir do ONTAP 9.7, a criptografia de volume e agregado é ativada por padrão se você tiver uma licença de criptografia de volume (VE) e usar um gerenciador de chaves integrado ou externo. A licença VE está incluída no "ONTAP One". Sempre que um gerenciador de chaves externo ou integrado é configurado, há uma alteração na forma como a criptografia de dados em repouso é configurada para agregados novos e volumes novos. Agregados novos terão a encriptação agregada NetApp (NAE) ativada por predefinição. Volumes novos que não fazem parte de um agregado NAE terão a criptografia de volume NetApp (NVE) ativada por padrão. Se uma máquina virtual de storage de dados (SVM) for configurada com seu próprio gerenciador de chaves usando o gerenciamento de chaves multilocatário, o volume criado para esse SVM será configurado automaticamente com NVE.

Pode ativar a encriptação num volume novo ou existente. O NVE dá suporte a uma variedade completa de recursos de eficiência de storage, incluindo deduplicação e compactação. Começando com ONTAP 9.14,1, você pode Habilite o NVE em volumes raiz do SVM atual.

Se estiver usando o SnapLock, você poderá habilitar a criptografia somente em volumes SnapLock novos e vazios. Não é possível ativar a encriptação num volume SnapLock existente.

Você pode usar o NVE em qualquer tipo de agregado (HDD, SSD, híbrido, LUN de array), com qualquer tipo de RAID e em qualquer implementação de ONTAP com suporte, incluindo ONTAP Select. Você também pode usar o NVE com criptografia baseada em hardware para "criptografar dados" em unidades com autocriptografia.

Quando o NVE está ativado, o despejo de memória também é criptografado.

Criptografia em nível de agregado

Normalmente, cada volume criptografado recebe uma chave exclusiva. Quando o volume é excluído, a chave é excluída com ele.

A partir do ONTAP 9.6, você pode usar *NetApp Aggregate Encryption (NAE)* para atribuir chaves ao agregado que contém para que os volumes sejam criptografados. Quando um volume criptografado é excluído, as chaves do agregado são preservadas. As chaves são excluídas se todo o agregado for excluído.

Você deve usar criptografia em nível de agregado se planeja executar deduplicação in-line ou em segundo plano. De outra forma, a deduplicação em nível de agregado não é compatível com NVE.

A partir do ONTAP 9.7, a criptografia de volume e agregado é ativada por padrão se você tiver uma licença de criptografia de volume (VE) e usar um gerenciador de chaves integrado ou externo.

Os volumes NVE e NAE podem coexistir no mesmo agregado. Os volumes encriptados em encriptação de nível agregado são volumes NAE por predefinição. Você pode substituir o padrão quando criptografar o volume.

Você pode usar o `volume move` comando para converter um volume NVE em um volume NAE e vice-versa. É possível replicar um volume NAE para um volume NVE.

Você não pode usar `secure purge` comandos em um volume NAE.

Quando usar servidores de gerenciamento de chaves externos

Embora seja menos caro e normalmente mais conveniente usar o gerenciador de chaves integrado, você deve configurar servidores KMIP se alguma das seguintes situações for verdadeira:

- Sua solução de gerenciamento de chaves de criptografia precisa estar em conformidade com Federal Information Processing Standards (FIPS) 140-2 ou com o padrão OASIS KMIP.
- Você precisa de uma solução de vários clusters, com gerenciamento centralizado de chaves de criptografia.
- Sua empresa requer a segurança adicional de armazenar chaves de autenticação em um sistema ou em um local diferente dos dados.

Escopo do gerenciamento de chaves externas

O escopo do gerenciamento de chaves externas determina se os servidores de gerenciamento de chaves protegem todos os SVMs no cluster ou somente SVMs selecionadas:

- Você pode usar um *cluster scope* para configurar o gerenciamento de chaves externas para todos os SVMs no cluster. O administrador do cluster tem acesso a todas as chaves armazenadas nos servidores.

- A partir do ONTAP 9.6, você pode usar um *escopo SVM* para configurar o gerenciamento de chaves externas para um SVM nomeado no cluster. Isso é melhor para ambientes com alocação a vários clientes nos quais cada locatário usa um SVM diferente (ou conjunto de SVMs) para fornecer dados. Somente o administrador do SVM de um determinado locatário tem acesso às chaves desse locatário.
- A partir do ONTAP 9.10,1, você pode usar o Azure Key Vault e Google Cloud KMS para proteger chaves NVE somente para SVMs de dados. Isso está disponível para o KMS da AWS a partir de 9.12.0.

Você pode usar ambos os escopos no mesmo cluster. Se os servidores de gerenciamento de chaves tiverem sido configurados para um SVM, o ONTAP usará apenas esses servidores para proteger chaves. Caso contrário, o ONTAP protege as chaves com os servidores de gerenciamento de chaves configurados para o cluster.

Uma lista de gerenciadores de chaves externos validados está disponível no "Ferramenta de Matriz de interoperabilidade NetApp (IMT)". Você pode encontrar esta lista inserindo o termo "key managers" no recurso de pesquisa do IMT.

Detalhes do suporte

A tabela a seguir mostra os detalhes de suporte do NVE:

Recurso ou recurso	Detalhes do suporte
Plataformas	Capacidade de descarga AES-NI necessária. Consulte o Hardware Universe (HWU) para verificar se o NVE e o NAE são compatíveis com sua plataforma.

Criptografia	A partir do ONTAP 9.7, agregados e volumes recém-criados são criptografados por padrão quando você adiciona uma licença de criptografia de volume (VE) e tem um gerenciador de chaves integrado ou externo configurado. Se você precisar criar um agregado não criptografado, use o seguinte comando:
	
	`storage aggregate create -encrypt-with-aggr-key false`
	
	Se você precisar criar um volume de texto simples, use o seguinte comando:
	
	`volume create -encrypt false`
	
	A encriptação não está ativada por predefinição quando:
	
	• A licença VE não está instalada.
	• O gerenciador de chaves não está configurado.
	• Plataforma ou software não suporta criptografia.
	• A criptografia de hardware está ativada.

ONTAP	Todas as implementações do ONTAP. O suporte para ONTAP Cloud está disponível no ONTAP 9.5 e posterior.
Dispositivos	HDD, SSD, híbrido, array LUN.
RAID	RAID0, RAID4, RAID-DP, RAID-TEC.

Volumes	Volumes de dados e volumes raiz atuais do SVM. Não é possível criptografar dados em volumes de metadados do MetroCluster. Em versões do ONTAP anteriores a 9.14.1, não é possível criptografar dados no volume raiz da SVM com NVE. A partir do ONTAP 9.14,1, o ONTAP suporta NVE em volumes raiz do SVM.
Criptografia em nível de agregado	A partir do ONTAP 9.6, o NVE é compatível com criptografia no nível de agregado (NAE): • Você deve usar criptografia em nível de agregado se planeja executar deduplicação in-line ou em segundo plano. • Você não pode rechavear um volume de criptografia de nível agregado. • A limpeza segura não é suportada em volumes de criptografia no nível de agregado. • Além dos volumes de dados, o NAE é compatível com a criptografia dos volumes raiz da SVM e do volume de metadados do MetroCluster. O NAE não suporta criptografia do volume raiz.
Escopo da SVM	A partir do ONTAP 9.6, o NVE é compatível com o escopo SVM somente para gerenciamento de chaves externas, e não para Gerenciador de chaves integrado. O MetroCluster é suportado a partir do ONTAP 9.8.
Eficiência de storage	Deduplicação, compressão, compactação, FlexClone. Os clones usam a mesma chave que o pai, mesmo depois de dividir o clone do pai. Você deve executar um `volume move` em um clone dividido, após o qual o clone dividido terá uma chave diferente.
Replicação	• Para replicação de volume, os volumes de origem e destino podem ter configurações de criptografia diferentes. A criptografia pode ser configurada para a origem e não configurada para o destino e vice-versa. A encriptação configurada na origem não será replicada para o destino. A criptografia deve ser configurada manualmente na origem e no destino. Configurar o NVEConsulte e Criptografia de dados de volume com NVE. • Para a replicação SVM, o volume de destino é criptografado automaticamente, a menos que o destino não contenha um nó compatível com criptografia de volume. Nesse caso, a replicação seja bem-sucedida, mas o volume de destino não seja criptografado. • Para configurações do MetroCluster, cada cluster puxa chaves de gerenciamento de chaves externas de seus servidores de chaves configurados. As chaves OKM são replicadas para o site do parceiro pelo serviço de replicação de configuração.
Conformidade	A partir do ONTAP 9.2, o SnapLock tem suporte nos modos conformidade e empresa, apenas para novos volumes. Não é possível ativar a encriptação num volume SnapLock existente.

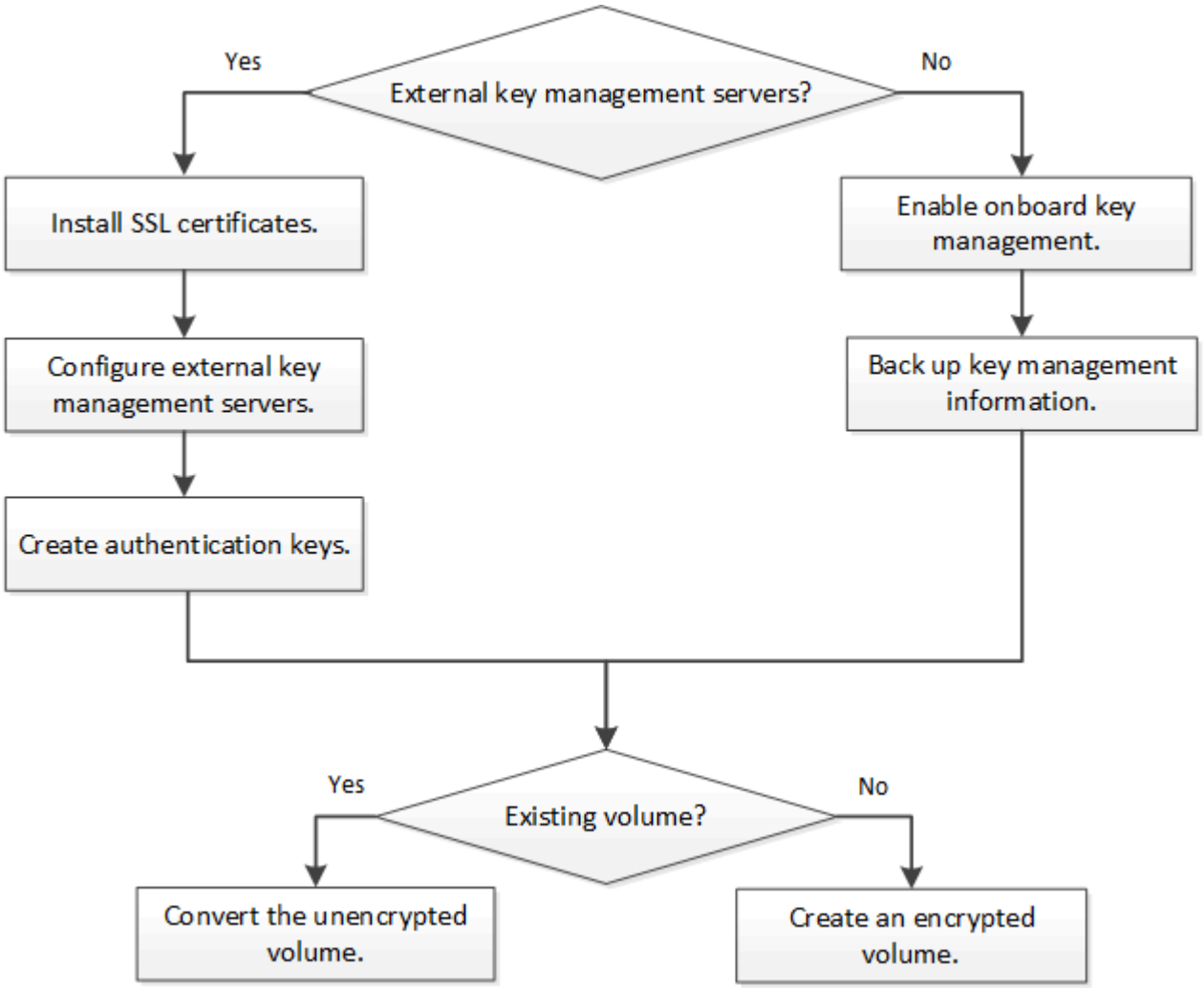
FlexGroups	A partir do ONTAP 9.2, os grupos flexíveis são suportados. Os agregados de destino devem ser do mesmo tipo que os agregados de origem, tanto em nível de volume como em nível de agregado. A partir do ONTAP 9.5, é suportada a rechavear no local de volumes FlexGroup.
Transição de 7 modos	A partir da ferramenta de transição de 7 modos 3,3, você pode usar a CLI da ferramenta de transição de 7 modos para realizar a transição baseada em cópia para volumes de destino habilitados para NVE no sistema em cluster.

Informações relacionadas

"Perguntas frequentes - encriptação de volume NetApp e encriptação agregada NetApp"

Fluxo de trabalho do NetApp volume Encryption

Você deve configurar os serviços de gerenciamento de chaves antes de ativar a criptografia de volume. Pode ativar a encriptação num novo volume ou num volume existente.



"Tem de instalar a licença VE" E configure os serviços de gerenciamento de chaves antes de criptografar dados com NVE. Antes de instalar a licença, você deve "Determine se sua versão do ONTAP é compatível

com NVE".

Configurar o NVE

Determine se a versão do cluster é compatível com NVE

Você deve determinar se a versão do cluster é compatível com NVE antes de instalar a licença. Você pode usar o `version` comando para determinar a versão do cluster.

Sobre esta tarefa

A versão do cluster é a versão mais baixa do ONTAP em execução em qualquer nó no cluster.

Passo

1. Determine se a versão do cluster é compatível com NVE:

   `version -v`

   NVE não é suportado se o comando output exibir o texto "'1Ono-DARE" (para "'criptografia sem dados em repouso"') ou se você estiver usando uma plataforma que não está listada no "Detalhes do suporte".

   O comando a seguir determina se o NVE é suportado `cluster1` no .

   ```
   cluster1::> version -v
   NetApp Release 9.1.0: Tue May 10 19:30:23 UTC 2016 <1Ono-DARE>
   ```

   A saída de `1Ono-DARE` indica que o NVE não é suportado na versão do cluster.

Instale a licença

Uma licença VE permite que você use o recurso em todos os nós do cluster. Essa licença é necessária para que você possa criptografar dados com NVE. Está incluído com "ONTAP One".

Antes do ONTAP One, a licença VE foi incluída com o pacote de encriptação. O pacote de criptografia não é mais oferecido, mas ainda é válido. Embora não seja necessário atualmente, os clientes existentes podem optar por "Atualize para o ONTAP One".

Antes de começar

- Você deve ser um administrador de cluster para executar esta tarefa.
- Tem de ter recebido a chave de licença VE do seu representante de vendas ou ter o ONTAP One instalado.

Passos

1. "Verifique se a licença VE está instalada".

   O nome do pacote de licença VE é `VE`.

2. Se a licença não estiver instalada, "Use o Gerenciador do sistema ou a CLI do ONTAP para instalá-lo".

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) é compatível com o Gerenciador de chaves integrado no ONTAP 9.1 e posterior. A partir do ONTAP 9.3, o NVE é compatível com gerenciamento de chaves externas (KMIP) e Gerenciador de chaves integrado. A partir do ONTAP 9.10,1, você pode usar Serviço do Azure Key Vault ou do Google Cloud Key Manager para proteger suas chaves NVE. 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.

Gerencie gerenciadores de chaves externos com o System Manager

A partir do ONTAP 9.7, você pode armazenar e gerenciar chaves de autenticação e criptografia com o Gerenciador de chaves integrado. A partir do ONTAP 9.13,1, você também pode usar gerenciadores de chaves externos para armazenar e gerenciar essas chaves.

O Gerenciador de chaves integrado armazena e gerencia chaves em um banco de dados seguro interno ao cluster. Seu escopo é o cluster. Um gerenciador de chaves externo armazena e gerencia chaves fora do cluster. Seu escopo pode ser o cluster ou a VM de storage. Um ou mais gerenciadores de chaves externos podem ser usados. Aplicam-se as seguintes condições:

- Se o Gerenciador de chaves integrado estiver habilitado, um gerenciador de chaves externo não poderá ser habilitado no nível do cluster, mas poderá ser habilitado no nível da VM de armazenamento.
- Se um gerenciador de chaves externo estiver habilitado no nível do cluster, o Gerenciador de chaves integrado não poderá ser habilitado.

Ao usar gerenciadores de chaves externos, você pode Registrar até quatro servidores de chaves primárias por VM de armazenamento e cluster. Cada servidor de chave primária pode ser agrupado com até três servidores de chaves secundárias.

Configurar um gerenciador de chaves externo

Para adicionar um gerenciador de chaves externo para uma VM de armazenamento, você deve adicionar um gateway opcional ao configurar a interface de rede para a VM de armazenamento. Se a VM de armazenamento foi criada sem a rota de rede, você terá que criar a rota explicitamente para o gerenciador de chaves externo. "Criar um LIF (interface de rede)"Consulte .

Passos

Você pode configurar um gerenciador de chaves externo a partir de diferentes locais no System Manager.

1. Para configurar um gerenciador de chaves externo, execute um dos seguintes passos iniciais.

Fluxo de trabalho	Navegação	Etapa inicial
Configure o Gerenciador de chaves	**Cluster** > **Settings**	Role até a seção **Segurança**. Em **encriptação**, selecione . Selecione **External Key Manager**.
Adicionar nível local	**Armazenamento** > **camadas**	Selecione * Adicionar nível local*. Marque a caixa de seleção "Configurar Gerenciador de chaves". Selecione **External Key Manager**.
Prepare o armazenamento	**Painel**	Na seção **capacidade**, selecione **preparar armazenamento**. Em seguida, selecione "Configure Key Manager". Selecione **External Key Manager**.
Configurar a criptografia (gerenciador de chaves somente no escopo da VM de storage)	**Storage** > **Storage VMs**	Selecione a VM de armazenamento. Selecione a guia **Configurações**. Na seção **criptografia** em **Segurança**, selecione .

2. Para adicionar um servidor de chave primária, selecione + Add e preencha os campos **Endereço IP ou Nome do host** e **porta**.
3. Os certificados instalados existentes são listados nos campos **certificados KMIP Server CA** e **KMIP Client Certificate**. Você pode executar qualquer uma das seguintes ações:
   - Selecione para selecionar os certificados instalados que pretende mapear para o gestor de chaves. (Podem ser selecionados vários certificados de CA de serviço, mas apenas um certificado de cliente pode ser selecionado.)
   - Selecione **Adicionar novo certificado** para adicionar um certificado que ainda não tenha sido instalado e mapeie-o para o gerenciador de chaves externo.
   - Selecione ao lado do nome do certificado para excluir os certificados instalados que você não deseja mapear para o gerenciador de chaves externo.
4. Para adicionar um servidor de chaves secundário, selecione **Add** na coluna **Secondary Key Servers** e forneça seus detalhes.
5. Selecione **Save** para concluir a configuração.

Editar um gerenciador de chaves externo existente

Se você já tiver configurado um gerenciador de chaves externo, poderá modificar suas configurações.

Passos

1. Para editar a configuração de um gerenciador de chaves externo, execute um dos seguintes passos iniciais.

Âmbito de aplicação	Navegação	Etapa inicial

Gerenciador de chaves externo do escopo do cluster	**Cluster** > **Settings**	Role até a seção **Segurança**. Em **Encryption**, selecione e, em seguida, selecione **Edit External Key Manager**.
Gerenciador de chaves externo de escopo da VM de storage	**Storage** > **Storage VMs**	Selecione a VM de armazenamento. Selecione a guia **Configurações**. Na seção **criptografia** em **Segurança**, selecione e selecione **Editar Gerenciador de chaves externas**.

2. Os servidores de chave existentes estão listados na tabela **Key Servers**. Você pode executar as seguintes operações:
   - Adicione um novo servidor de chaves selecionando + Add .
   - Exclua um servidor de chaves selecionando no final da célula da tabela que contém o nome do servidor de chaves. Os servidores de chave secundária associados a esse servidor de chave primária também são removidos da configuração.

Excluir um gerenciador de chaves externo

Um gerenciador de chaves externo pode ser excluído se os volumes não forem criptografados.

Passos

1. Para excluir um gerenciador de chaves externo, execute uma das etapas a seguir.

Âmbito de aplicação	Navegação	Etapa inicial
Gerenciador de chaves externo do escopo do cluster	**Cluster** > **Settings**	Role até a seção **Segurança**. Em **Encryption**, selecione e, em seguida, selecione **Delete External Key Manager**.
Gerenciador de chaves externo de escopo da VM de storage	**Storage** > **Storage VMs**	Selecione a VM de armazenamento. Selecione a guia **Configurações**. Na seção **criptografia** em **Segurança**, selecione e selecione **Excluir Gerenciador de chaves externas**.

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 versões posteriores (NVE)

Você pode usar um ou mais servidores KMIP para proteger as chaves que o cluster usa para acessar dados criptografados. A partir do ONTAP 9.6, você tem a opção de configurar um gerenciador de chaves externo separado para proteger as chaves que um SVM de dados usa para acessar dados criptografados.

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 .

Sobre esta tarefa

É possível conectar até quatro servidores KMIP a um cluster ou SVM. Recomenda-se um mínimo de dois servidores para redundância e recuperação de desastres.

O escopo do gerenciamento de chaves externas determina se os servidores de gerenciamento de chaves protegem todos os SVMs no cluster ou somente SVMs selecionadas:

- Você pode usar um *cluster scope* para configurar o gerenciamento de chaves externas para todos os SVMs no cluster. O administrador do cluster tem acesso a todas as chaves armazenadas nos servidores.
- A partir do ONTAP 9.6, você pode usar um *escopo SVM* para configurar o gerenciamento de chaves externas para um SVM de dados no cluster. Isso é melhor para ambientes com alocação a vários clientes nos quais cada locatário usa um SVM diferente (ou conjunto de SVMs) para fornecer dados. Somente o administrador do SVM de um determinado locatário tem acesso às chaves desse locatário.

- Para ambientes multitenant, instale uma licença para *MT_EK_MGMT* usando o seguinte comando:

  ```
  system license add -license-code <MT_EK_MGMT license code>
  ```

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

Você pode usar ambos os escopos no mesmo cluster. Se os servidores de gerenciamento de chaves tiverem sido configurados para um SVM, o ONTAP usará apenas esses servidores para proteger chaves. Caso contrário, o ONTAP protege as chaves com os servidores de gerenciamento de chaves configurados para o cluster.

Você pode configurar o gerenciamento de chaves integradas no escopo do cluster e o gerenciamento de chaves externas no escopo da SVM. Você pode usar o `security key-manager key migrate` comando para migrar chaves do gerenciamento de chaves integradas no escopo do cluster para gerenciadores de chaves externos no escopo da SVM.

Antes de começar

- Os certificados de cliente e servidor KMIP SSL devem ter sido instalados.
- Você deve ser um administrador de cluster ou SVM para executar essa tarefa.
- Para habilitar o gerenciamento de chaves externas para um ambiente MetroCluster, o MetroCluster deve estar totalmente configurado antes de habilitar o gerenciamento de chaves externas.
- 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. Se você executar o comando no prompt de login do cluster, *`admin_SVM`* o padrão será o administrador SVM do cluster atual. Você deve ser o administrador do cluster para configurar o escopo do cluster. Você pode executar o `security key-manager external modify` comando para alterar a configuração de gerenciamento de chaves externas.
   > ◦ 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 -vserver cluster1 -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. Configurar um gerenciador de chaves e uma SVM:

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

   - Se você executar o comando no prompt de login SVM, `SVM` o padrão será SVM atual. Você precisa ser um administrador de cluster ou SVM para configurar o escopo do SVM. Você pode executar o `security key-manager external modify` comando para alterar a configuração de gerenciamento de chaves externas.
   - Em um ambiente MetroCluster, se você estiver configurando o gerenciamento de chaves externas para um SVM de dados, não será necessário repetir o `security key-manager external enable` comando no cluster de parceiros.

   O comando a seguir habilita o gerenciamento de chaves externas para `svm1` que um servidor de chave única esteja escutando na porta padrão 5696:

```
svm1l::> security key-manager external enable -vserver svm1 -key-servers
keyserver.svm1.com -client-cert SVM1ClientCert -server-ca-certs
SVM1ServerCaCert
```

3. Repita a última etapa para quaisquer SVMs adicionais.

   Você também pode usar o `security key-manager external add-servers` comando para configurar SVMs adicionais. O `security key-manager external add-servers` comando substitui o `security key-manager add` comando. Para obter a sintaxe completa do comando, consulte a página man.

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

   `security key-manager external show-status -node node_name`

   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
      svm1
               keyserver.svm1.com:5696                          available
      cluster1
               10.0.0.10:5696                                   available
               fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234     available
               ks1.local:15696                                  available
node2
      svm1
               keyserver.svm1.com:5696                          available
      cluster1
               10.0.0.10:5696                                   available
               fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234     available
               ks1.local:15696                                  available

8 entries were displayed.
```

5. 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.

Habilite o gerenciamento de chaves externas no ONTAP 9.5 e versões anteriores

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.

Gerencie chaves com um provedor de nuvem

A partir do ONTAP 9.10,1, você pode usar "Azure Key Vault (AKV)" e "Serviço de gerenciamento de chaves do Google Cloud Platform (Cloud KMS)"proteger suas chaves de criptografia ONTAP em um aplicativo hospedado na nuvem. A partir do ONTAP 9.12,0, também é possível proteger as chaves NVE com "KMS DA AWS"o .

O AWS KMS, AKV e o Cloud KMS podem ser usados para proteger "Chaves de criptografia de volume NetApp (NVE)" somente SVMs de dados.

Sobre esta tarefa

O gerenciamento de chaves com um fornecedor de nuvem pode ser habilitado com a CLI ou a API REST do ONTAP.

Ao usar um provedor de nuvem para proteger suas chaves, esteja ciente de que, por padrão, um data SVM LIF é usado para se comunicar com o endpoint de gerenciamento de chaves na nuvem. Uma rede de gerenciamento de nós é usada para se comunicar com os serviços de autenticação do provedor de nuvem (login.microsoftonline.com para Azure; oauth2.googleapis.com para Cloud KMS). Se a rede do cluster não estiver configurada corretamente, o cluster não utilizará adequadamente o serviço de gerenciamento de chaves.

Ao utilizar um serviço de gerenciamento de chaves do provedor de nuvem, você deve estar ciente das seguintes limitações:

- O gerenciamento de chaves do fornecedor de nuvem não está disponível para criptografia de storage NetApp (NSE) e criptografia agregada NetApp (NAE). "KMIPs externos" pode ser usado em vez disso.
- O gerenciamento de chaves do fornecedor de nuvem não está disponível para configurações do MetroCluster.
- O gerenciamento de chaves do fornecedor de nuvem só pode ser configurado em um data SVM.

Antes de começar

- Você deve ter configurado o KMS no provedor de nuvem apropriado.
- Os nós do cluster do ONTAP devem ser compatíveis com NVE.
- "Você deve ter instalado as licenças de criptografia de volume (VE) e gerenciamento de chaves de criptografia de vários locatários (MTEKM)". Estas licenças estão incluídas no "ONTAP One".
- Você precisa ser um administrador de cluster ou SVM.
- O SVM não deve incluir volumes criptografados nem empregar um gerenciador de chaves. Se o SVM de dados incluir volumes criptografados, você precisará migrá-los antes de configurar o KMS.

Ativar o gerenciamento de chaves externas

A ativação do gerenciamento de chaves externas depende do gerenciador de chaves específico que você usa. Escolha a guia do gerenciador de chaves e do ambiente apropriados.

AWS

Antes de começar

- Você deve criar uma subvenção para a chave AWS KMS que será usada pela função de gerenciamento de criptografia do IAM. A função IAM deve incluir uma política que permita as seguintes operações:
  - `DescribeKey`
  - `Encrypt`
  - `Decrypt` Para obter mais informações, consulte a documentação da AWS para "subvenções".

Habilite o AWS KMV em um SVM do ONTAP

1. Antes de começar, obtenha o ID da chave de acesso e a chave secreta do seu AWS KMS.
2. Defina o nível de privilégio como avançado:
   `set -priv advanced`
3. Habilite o AWS KMS:
   `security key-manager external aws enable -vserver` *`svm_name`* `-region` *`AWS_region`* `-key-id` *`key_ID`* `-encryption-context` *`encryption_context`*
4. Quando solicitado, insira a chave secreta.
5. Confirme se o AWS KMS foi configurado corretamente:
   `security key-manager external aws show -vserver` *`svm_name`*

Azure

Habilite o cofre de chaves do Azure em um SVM do ONTAP

1. Antes de começar, você precisa obter as credenciais de autenticação apropriadas da sua conta Azure, seja um segredo de cliente ou certificado. Você também precisa garantir que todos os nós no cluster estejam íntegros. Você pode verificar isso com o comando `cluster show`.
2. Defina o nível privilegiado como avançado
   `set -priv advanced`
3. Ativar AKV no SVM
   `security key-manager external azure enable -client-id` *`client_id`* `-tenant-id` *`tenant_id`* `-name -key-id` *`key_id`* `-authentication-method {certificate|client-secret}` quando solicitado, insira o certificado de cliente ou o segredo do cliente na sua conta Azure.
4. Verifique se o AKV está ativado corretamente:
   `security key-manager external azure show vserver` *`svm_name`* Se a acessibilidade do serviço não estiver OK, estabeleça a conetividade com o serviço de gerenciamento de chaves AKV através dos dados SVM LIF.

Google Cloud

Habilite o KMS da nuvem em um SVM do ONTAP

1. Antes de começar, obtenha a chave privada para o arquivo de chave de conta KMS do Google Cloud em um formato JSON. Isso pode ser encontrado na sua conta do GCP. Você também precisa garantir que todos os nós no cluster estejam íntegros. Você pode verificar isso com o comando `cluster show`.
2. Defina o nível privilegiado como avançado:
   `set -priv advanced`

3. Ative o Cloud KMS no SVM
`security key-manager external gcp enable -vserver` *`svm_name`* `-project-id` *`project_id`*`-key-ring-name` *`key_ring_name`* `-key-ring-location` *`key_ring_location`* `-key-name` *`key_name`* quando solicitado, insira o conteúdo do arquivo JSON com a chave privada da conta de serviço
4. Verifique se o Cloud KMS está configurado com os parâmetros corretos:
`security key-manager external gcp show vserver` *`svm_name`* O status do `kms_wrapped_key_status` será "`UNKNOWN`" se nenhum volume criptografado tiver sido criado. Se a acessibilidade do serviço não estiver OK, estabeleça a conectividade com o serviço de gerenciamento de chaves do GCP por meio do data SVM LIF.

Se um ou mais volumes criptografados já estiverem configurados para um SVM de dados e as chaves NVE correspondentes forem gerenciadas pelo gerenciador de chaves integrado SVM de administrador, essas chaves deverão ser migradas para o serviço de gerenciamento de chaves externo. Para fazer isso com a CLI, execute o comando:
`security key-manager key migrate -from-Vserver` *`admin_SVM`* `-to-Vserver` *`data_SVM`*
Novos volumes criptografados não podem ser criados para o SVM de dados do locatário até que todas as chaves NVE do SVM de dados sejam migradas com sucesso.

Informações relacionadas

- "Criptografia de volumes com soluções de criptografia NetApp para Cloud Volumes ONTAP"

Habilite o gerenciamento de chaves integradas no ONTAP 9.6 e posterior (NVE)

Você pode usar o Gerenciador de chaves integrado para proteger as chaves que o cluster usa para acessar dados criptografados. É necessário ativar o Gerenciador de chaves integrado em cada cluster que acessa um volume criptografado ou um disco com autocriptografia.

Sobre esta tarefa

Você deve executar o `security key-manager onboard sync` comando sempre que adicionar um nó ao cluster.

Se você tiver uma configuração do MetroCluster, deverá executar primeiro o `security key-manager onboard enable` comando no cluster local e, em seguida, executar o `security key-manager onboard sync` comando no cluster remoto, usando a mesma senha em cada um. Ao executar o `security key-manager onboard enable` comando a partir do cluster local e depois sincronizar no cluster remoto, não é necessário executar o `enable` comando novamente a partir do cluster remoto.

Por padrão, você não é obrigado a inserir a senha do gerenciador de chaves quando um nó é reinicializado. Pode utilizar a `cc-mode-enabled=yes` opção para exigir que os utilizadores introduzam a frase-passe após uma reinicialização.

Para NVE, se você definir `cc-mode-enabled=yes`o , os volumes criados com os `volume create` comandos e `volume move start` serão criptografados automaticamente. Para `volume create`, não é necessário especificar `-encrypt true`. Para `volume move start`, não é necessário especificar `-encrypt-destination true`.

Ao configurar a criptografia de dados em repouso do ONTAP, para atender aos requisitos de soluções comerciais para classificação (CSfC), você deve usar o NSE com NVE e garantir que o Gerenciador de chaves integrado esteja habilitado no modo critérios comuns. Consulte a "Resumo da solução CSfC"para

obter mais informações sobre o CSfC.

Quando o Gerenciador de chaves integrado está habilitado no modo Common Criteria (`cc-mode-enabled=yes`), o comportamento do sistema é alterado das seguintes maneiras:

- O sistema monitoriza as tentativas consecutivas de frase-passe do cluster falhadas ao funcionar no modo Common Criteria (critérios comuns).

  Se não conseguir introduzir a frase-passe correta do cluster no arranque, os volumes encriptados não são montados. Para corrigir isso, você deve reinicializar o nó e inserir a senha correta do cluster. Uma vez iniciado, o sistema permite até 5 tentativas consecutivas para inserir corretamente a senha do cluster em um período de 24 horas para qualquer comando que exija a senha do cluster como um parâmetro. Se o limite for atingido (por exemplo, você não conseguiu inserir corretamente a senha do cluster 5 vezes em uma linha), então você deve esperar o período de tempo limite de 24 horas para decorrer, ou você deve reiniciar o nó, a fim de redefinir o limite.

- As atualizações de imagem do sistema usam o certificado de assinatura de código NetApp RSA-3072 juntamente com os digests assinados por código SHA-384 para verificar a integridade da imagem em vez do certificado de assinatura de código NetApp RSA-2048 usual e os digests assinados por código SHA-256.

  O comando upgrade verifica se o conteúdo da imagem não foi alterado ou corrompido verificando várias assinaturas digitais. O processo de atualização da imagem prossegue para o próximo passo se a validação for bem-sucedida; caso contrário, a atualização da imagem falhará. Consulte a `cluster image` página de manual para obter informações sobre atualizações do sistema.

O Gerenciador de chaves integrado armazena as chaves na memória volátil. O conteúdo da memória volátil é apagado quando o sistema é reinicializado ou interrompido. Em condições normais de funcionamento, o conteúdo da memória volátil será apagado dentro de 30sMB quando um sistema for interrompido.

Antes de começar

- Você deve ser um administrador de cluster para executar esta tarefa.
- Você deve configurar o ambiente MetroCluster antes de configurar o Gerenciador de chaves integrado.

Passos

1. Inicie a configuração do gerenciador de chaves:

   ```
   security key-manager onboard enable -cc-mode-enabled yes|no
   ```

   Defina `cc-mode-enabled=yes` para exigir que os usuários inseram a senha do gerenciador de chaves após uma reinicialização. Para NVE, se você definir `cc-mode-enabled=yes`o , os volumes criados com os `volume create` comandos e `volume move start` serão criptografados automaticamente. A – `cc-mode-enabled` opção não é suportada nas configurações do MetroCluster. O `security key-manager onboard enable` comando substitui o `security key-manager setup` comando.

   O exemplo a seguir inicia o comando de configuração do gerenciador de chaves no cluster1 sem exigir que a senha seja inserida após cada reinicialização:

```
cluster1::> security key-manager onboard enable

Enter the cluster-wide passphrase for onboard key management in Vserver
"cluster1"::    <32..256 ASCII characters long text>
Reenter the cluster-wide passphrase:    <32..256 ASCII characters long
text>
```

2. No prompt de frase-passe, insira uma frase-passe entre 32 e 256 carateres ou, para "cc-mode", uma frase-passe entre 64 e 256 carateres.

> Se a senha "'cc-mode'" especificada for inferior a 64 carateres, haverá um atraso de cinco segundos antes que a operação de configuração do gerenciador de chaves exiba o prompt de senha novamente.

3. No prompt de confirmação da senha, redigite a senha.
4. Verifique se as chaves de autenticação foram criadas:

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

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

```
cluster1::> security key-manager key query -key-type NSE-AK
               Node: node1
            Vserver: cluster1
        Key Manager: onboard
   Key Manager Type: OKM
 Key Manager Policy: -

 Key Tag                                  Key Type Encryption   Restored

-----------------------------------  -------- ------------ --------

node1                                    NSE-AK   AES-256      true

    Key ID:
000000000000000002000000000000100056178fc6ace6d91472df8a9286daacc00000000
00000000

node1                                    NSE-AK   AES-256      true

    Key ID:
000000000000000002000000000000100df1689a148fdfbf9c2b198ef974d0baa00000000
00000000

2 entries were displayed.
```

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

   `volume encryption conversion start`

   O Gerenciador de chaves integrado deve estar totalmente configurado antes de converter os volumes. Em um ambiente MetroCluster, o Gerenciador de chaves integrado deve ser configurado em ambos os sites.

Depois de terminar

Copie a senha para um local seguro fora do sistema de armazenamento para uso futuro.

Sempre que você configurar a senha do Gerenciador de chaves integrado, você também deve fazer backup das informações manualmente para um local seguro fora do sistema de armazenamento para uso em caso de desastre. "Faça backup manual das informações de gerenciamento de chaves integradas"Consulte .

Habilite o gerenciamento de chaves integradas no ONTAP 9.5 e versões anteriores (NVE)

Você pode usar o Gerenciador de chaves integrado para proteger as chaves que o cluster usa para acessar dados criptografados. É necessário habilitar o Gerenciador de chaves integrado em cada cluster que acessa um volume criptografado ou um disco com autocriptografia.

Sobre esta tarefa

Você deve executar o `security key-manager setup` comando sempre que adicionar um nó ao cluster.

Se você tiver uma configuração do MetroCluster, revise estas diretrizes:

- No ONTAP 9.5, você deve executar `security key-manager setup` no cluster local e `security key-manager setup -sync-metrocluster-config yes` no cluster remoto, usando a mesma senha em cada um.
- Antes do ONTAP 9.5, você deve executar `security key-manager setup` no cluster local, esperar aproximadamente 20 segundos e, em seguida, executar `security key-manager setup` no cluster remoto, usando a mesma senha em cada um.

Por padrão, você não é obrigado a inserir a senha do gerenciador de chaves quando um nó é reinicializado. A partir do ONTAP 9.4, pode utilizar a `-enable-cc-mode yes` opção para exigir que os utilizadores introduzam a frase-passe após uma reinicialização.

Para NVE, se você definir `-enable-cc-mode yes`o , os volumes criados com os `volume create` comandos e `volume move start` serão criptografados automaticamente. Para `volume create`, não é necessário especificar `-encrypt true`. Para `volume move start`, não é necessário especificar `-encrypt-destination true`.

Depois de uma tentativa de frase-passe com falha, tem de reiniciar o nó novamente.

Antes de começar

- Se você estiver usando o NSE ou o NVE com um servidor de gerenciamento de chaves externo (KMIP), exclua o banco de dados do gerenciador de chaves externo.

  "Transição para o gerenciamento de chaves integrado do gerenciamento de chaves externas"

- Você deve ser um administrador de cluster para executar esta tarefa.
- Você deve configurar o ambiente MetroCluster antes de configurar o Gerenciador de chaves integrado.

Passos

1. Inicie a configuração do gerenciador de chaves:

   ```
   security key-manager setup -enable-cc-mode yes|no
   ```

   A partir do ONTAP 9.4, pode utilizar a `-enable-cc-mode yes` opção para exigir que os utilizadores introduzam a frase-passe do gestor de chaves após uma reinicialização. Para NVE, se você definir `-enable-cc-mode yes`o , os volumes criados com os `volume create` comandos e `volume move start` serão criptografados automaticamente.

   O exemplo a seguir inicia a configuração do gerenciador de chaves no cluster1 sem exigir que a senha seja inserida após cada reinicialização:

```
cluster1::> security key-manager setup
Welcome to the key manager setup wizard, which will lead you through
the steps to add boot information.

...

Would you like to use onboard key-management? {yes, no} [yes]:
Enter the cluster-wide passphrase:    <32..256 ASCII characters long
text>
Reenter the cluster-wide passphrase:    <32..256 ASCII characters long
text>
```

2. Digite `yes` no prompt para configurar o gerenciamento de chaves integradas.
3. No prompt de frase-passe, insira uma frase-passe entre 32 e 256 carateres ou, para "cc-mode", uma frase-passe entre 64 e 256 carateres.

> Se a senha "'cc-mode'" especificada for inferior a 64 carateres, haverá um atraso de cinco segundos antes que a operação de configuração do gerenciador de chaves exiba o prompt de senha novamente.

4. No prompt de confirmação da senha, redigite a senha.
5. Verifique se as chaves estão configuradas para todos os nós:

   `security key-manager key show`

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

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

Node: node1
Key Store: onboard
Key ID                                                           Used By
-----------------------------------------------------------------------
--------
000000000000000020000000000010059851742AF2703FC91369B7DB47C4722 NSE-AK
000000000000000020000000000001008C07CC0AF1EF49E0105300EFC83004BF NSE-AK

Node: node2
Key Store: onboard
Key ID                                                           Used By
-----------------------------------------------------------------------
--------
000000000000000020000000000010059851742AF2703FC91369B7DB47C4722 NSE-AK
000000000000000020000000000001008C07CC0AF1EF49E0105300EFC83004BF NSE-AK
```

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

   `volume encryption conversion start`

   O Gerenciador de chaves integrado deve estar totalmente configurado antes de converter os volumes. Em um ambiente MetroCluster, o Gerenciador de chaves integrado deve ser configurado em ambos os sites.

Depois de terminar

Copie a senha para um local seguro fora do sistema de armazenamento para uso futuro.

Sempre que você configurar a senha do Gerenciador de chaves integrado, você também deve fazer backup das informações manualmente para um local seguro fora do sistema de armazenamento para uso em caso de desastre. "Faça backup manual das informações de gerenciamento de chaves integradas"Consulte .

Habilite o gerenciamento de chaves integradas em nós recém-adicionados

Você pode usar o Gerenciador de chaves integrado para proteger as chaves que o cluster usa para acessar dados criptografados. É necessário habilitar o Gerenciador de chaves integrado em cada cluster que acessa um volume criptografado ou um disco com autocriptografia.

> Para o ONTAP 9.5 e versões anteriores, você deve executar o `security key-manager setup` comando sempre que adicionar um nó ao cluster.
>
> Para o ONTAP 9.6 e posterior, você deve executar o `security key-manager sync` comando sempre que adicionar um nó ao cluster.
>
> Se você adicionar um nó a um cluster que tenha o gerenciamento de chaves integradas configurado, você executará esse comando para atualizar as chaves ausentes.

Se você tiver uma configuração do MetroCluster, revise estas diretrizes:

- A partir do ONTAP 9.6, é necessário executar `security key-manager onboard enable` primeiro no cluster local e, em seguida, executar `security key-manager onboard sync` no cluster remoto, usando a mesma frase-passe em cada um.
- No ONTAP 9.5, você deve executar `security key-manager setup` no cluster local e `security key-manager setup -sync-metrocluster-config yes` no cluster remoto, usando a mesma senha em cada um.
- Antes do ONTAP 9.5, você deve executar `security key-manager setup` no cluster local, esperar aproximadamente 20 segundos e, em seguida, executar `security key-manager setup` no cluster remoto, usando a mesma senha em cada um.

Por padrão, você não é obrigado a inserir a senha do gerenciador de chaves quando um nó é reinicializado. A partir do ONTAP 9.4, pode utilizar a `-enable-cc-mode yes` opção para exigir que os utilizadores introduzam a frase-passe após uma reinicialização.

Para NVE, se você definir `-enable-cc-mode yes`o , os volumes criados com os `volume create` comandos e `volume move start` serão criptografados automaticamente. Para `volume create`, não é necessário especificar `-encrypt true`. Para `volume move start`, não é necessário especificar `-encrypt-destination true`.

Depois de uma tentativa de frase-passe com falha, tem de reiniciar o nó novamente.

Migrar chaves de criptografia de dados do ONTAP entre gerenciadores de chaves

Você pode gerenciar suas chaves de criptografia de dados usando o Gerenciador de chaves integrado do ONTAP ou um gerenciador de chaves externo (ou ambos). Os gerenciadores de chaves externos só podem ser ativados no nível de VM de armazenamento. No nível do cluster do ONTAP, você pode ativar o gerenciador de chaves integrado ou um gerenciador de chaves externo.

Se ativar o seu gestor de chaves na…	Você pode usar…
Somente no nível do cluster	O gerenciador de chaves integrado ou um gerenciador de chaves externo
Somente nível SVM	Apenas um gerenciador de chaves externo
Tanto o cluster quanto o nível da SVM	Uma das seguintes combinações de gerenciador de chaves: • Opção 1 Nível de cluster: Gerenciador de chaves integrado Nível da SVM: Gerente de chaves externo • Opção 2 Nível de cluster: Gerenciador de chaves externo Nível da SVM: Gerente de chaves externo

Migre chaves entre os gerenciadores-chave no nível do cluster do ONTAP

A partir do ONTAP 9.16,1, você pode usar a interface de linha de comando (CLI) do ONTAP para migrar chaves entre gerenciadores de chaves no nível do cluster.

Do gerenciador de chaves integrado ao gerenciador de chaves externo

Passos

1. Defina o nível de privilégio como avançado:

```
set -privilege advanced
```

2. Criar uma configuração de gerenciador de chaves externo inativo:

```
security key-manager external create-config
```

3. Mude para o gerenciador de chaves externo:

```
security key-manager keystore enable -vserver <svm_name> -type KMIP
```

4. Exclua a configuração do gerenciador de chaves integrado:

```
security key-manager keystore delete-config -vserver <svm_name>
-type OKM
```

5. Defina o nível de privilégio como admin:

```
set -privilege admin
```

Do gerenciador de chaves externo ao gerenciador de chaves integrado

Passos

1. Defina o nível de privilégio como avançado:

```
set -privilege advanced
```

2. Criar uma configuração inativa do gerenciador de chaves integrado:

```
security key-manager onboard create-config
```

3. Ative a configuração do gerenciador de chaves integrado:

```
security key-manager keystore enable -vserver <svm_name> -type OKM
```

4. Exclua a configuração do gerenciador de chaves externo

```
security key-manager keystore delete-config -vserver <svm_name>
-type KMIP
```

5. Defina o nível de privilégio como admin:

```
set -privilege admin
```

Migre chaves entre gerenciadores de chaves em cluster ONTAP e níveis de VM de armazenamento

Você pode usar a interface de linha de comando (CLI) do ONTAP para migrar chaves entre o gerenciador de chaves no nível do cluster e um gerenciador de chaves no nível da VM de storage.

Passos

1. Defina o nível de privilégio como avançado:

```
set -privilege advanced
```

2. Migrar as chaves:

```
security key-manager key migrate -from-vserver <svm_name> -to-vserver
<svm_name>
```

3. Defina o nível de privilégio como admin:

```
set -privilege admin
```

Criptografia de dados de volume com NVE

Criptografe dados de volume com a visão geral do NVE

A partir do ONTAP 9.7, a criptografia de agregado e volume é ativada por padrão quando você tem a licença VE e o gerenciamento de chaves internas ou externas. Para o ONTAP 9.6 e versões anteriores, é possível ativar a criptografia em um novo volume ou em um volume existente. Tem de ter instalado a licença VE e ativado a gestão de chaves para poder ativar a encriptação de volume. O NVE está em conformidade com FIPS-140-2 nível 1.

Ative a encriptação em nível de agregado com licença VE

A partir do ONTAP 9.7, agregados e volumes recém-criados são criptografados por padrão quando você tem o "Licença VE" e gerenciamento de chaves externas ou

integradas. A partir do ONTAP 9.6, você pode usar a criptografia em nível de agregado para atribuir chaves ao agregado que contém para que os volumes sejam criptografados.

Sobre esta tarefa

Você deve usar criptografia em nível de agregado se planeja executar deduplicação in-line ou em segundo plano. De outra forma, a deduplicação em nível de agregado não é compatível com NVE.

Um agregado habilitado para criptografia de nível agregado é chamado de *agregado NAE* (para criptografia agregada NetApp). Todos os volumes em um agregado NAE precisam ser criptografados com criptografia NAE ou NVE. Com a criptografia de nível agregado, os volumes criados no agregado são criptografados com criptografia NAE por padrão. Em vez disso, você pode substituir o padrão para usar a criptografia NVE.

Os volumes de texto sem formatação não são suportados em agregados NAE.

Antes de começar

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

Passos

1. Ativar ou desativar a encriptação de nível agregado:

Para…	Use este comando…
Crie um agregado NAE com o ONTAP 9.7 ou posterior	`storage aggregate create -aggregate` *`aggregate_name`* `-node` *`node_name`*
Crie um agregado NAE com o ONTAP 9.6	`storage aggregate create -aggregate` *`aggregate_name`* `-node` *`node_name`* `-encrypt-with -aggr-key true`
Converter um agregado não-naE em um agregado NAE	`storage aggregate modify -aggregate` *`aggregate_name`* `-node` *`node_name`* `-encrypt-with -aggr-key true`
Converter um agregado NAE em um agregado não-naE	`storage aggregate modify -aggregate` *`aggregate_name`* `-node` *`node_name`* `-encrypt-with -aggr-key false`

Para obter a sintaxe completa do comando, consulte as páginas man.

O comando a seguir habilita a criptografia de nível agregado `aggr1` no :

- ONTAP 9.7 ou posterior:

```
cluster1::> storage aggregate create -aggregate aggr1
```

- ONTAP 9.6 ou anterior:

```
cluster1::> storage aggregate create -aggregate aggr1 -encrypt-with
-aggr-key true
```

2. Verifique se o agregado está habilitado para criptografia:

   `storage aggregate show -fields encrypt-with-aggr-key`

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

   O comando a seguir verifica se `aggr1` está habilitado para criptografia:

```
cluster1::> storage aggregate show -fields encrypt-with-aggr-key
aggregate            encrypt-aggr-key
-------------------- ----------------
aggr0_vsim4          false
aggr1                true
2 entries were displayed.
```

Depois de terminar

Execute o `volume create` comando para criar os volumes criptografados.

Se você estiver usando um servidor KMIP para armazenar as chaves de criptografia de um nó, o ONTAP automaticamente "envia" uma chave de criptografia para o servidor quando você criptografa um volume.

Ative a criptografia em um novo volume

Você pode usar o `volume create` comando para habilitar a criptografia em um novo volume.

Sobre esta tarefa

É possível criptografar volumes usando o NetApp volume Encryption (NVE) e, a partir do ONTAP 9.6, NetApp Aggregate Encryption (NAE). Para saber mais sobre NAE e NVE, consulte o descrição geral da encriptação de volumes.

Saiba mais sobre os comandos descritos neste procedimento no "Referência do comando ONTAP".

O procedimento para habilitar a criptografia em um novo volume no ONTAP varia de acordo com a versão do ONTAP que você está usando e sua configuração específica:

- A partir do ONTAP 9.4, se você ativar `cc-mode` ao configurar o Gerenciador de chaves integrado, os volumes criados com o `volume create` comando serão automaticamente criptografados, independentemente de você especificar ou não `-encrypt true` .
- No ONTAP 9.6 e versões anteriores, você deve usar `-encrypt true` comandos com `volume create` para ativar a criptografia (desde que não tenha ativado `cc-mode`).
- Se você quiser criar um volume NAE no ONTAP 9.6, você deve habilitar o NAE no nível agregado. Ative a encriptação em nível de agregado com a licença VEConsulte para obter mais detalhes sobre esta tarefa.

- A partir do ONTAP 9.7, os volumes recém-criados são criptografados por padrão quando você tem o "Licença VE" e gerenciamento de chaves integradas ou externas. Por padrão, novos volumes criados em um agregado NAE serão do tipo NAE em vez de NVE.
  - No ONTAP 9.7 e versões posteriores, se você adicionar `-encrypt true` ao `volume create` comando para criar um volume em um agregado NAE, o volume terá criptografia NVE em vez de NAE. Todos os volumes em um agregado NAE precisam ser criptografados com NVE ou NAE.

Os volumes de texto sem formatação não são suportados em agregados NAE.

Passos

1. Crie um novo volume e especifique se a criptografia está ativada no volume. Se o novo volume estiver em um agregado NAE, por padrão o volume será um volume NAE:

Para criar…	Use este comando…
Um volume NAE	`volume create -vserver` *`SVM_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`*
Um volume NVE	`volume create -vserver` *`SVM_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`* `-encrypt true` E No ONTAP 9.6 e anterior, em que o NAE não é suportado, `-encrypt true` especifica que o volume deve ser criptografado com NVE. No ONTAP 9.7 e posterior, onde os volumes são criados em agregados NAE, `-encrypt true` substitui o tipo de criptografia padrão do NAE para criar um volume NVE.
Um volume de texto simples	`volume create -vserver` *`SVM_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`* `-encrypt false`

   Saiba mais sobre `volume create` o "Referência do comando ONTAP"na .

2. Verifique se os volumes estão ativados para criptografia:

   ```
   volume show -is-encrypted true
   ```

   Para obter a sintaxe de comando completa, consulte "Referência do comando ONTAP".

Resultado

Se você estiver usando um servidor KMIP para armazenar as chaves de criptografia de um nó, o ONTAP "enviará" automaticamente uma chave de criptografia ao servidor quando você criptografar um volume.

=
:allow-uri-read:

Ative a criptografia em um volume existente

Você pode usar o `volume move start` comando ou o `volume encryption`

`conversion start` para habilitar a criptografia em um volume existente.

Sobre esta tarefa

- A partir do ONTAP 9.3, você pode usar o `volume encryption conversion start` comando para habilitar a criptografia de um volume existente "no lugar", sem ter que mover o volume para um local diferente. Alternativamente, você pode usar o `volume move start` comando.
- Para o ONTAP 9.2 e versões anteriores, você pode usar apenas o `volume move start` comando para habilitar a criptografia movendo um volume existente.

Ative a criptografia em um volume existente com o comando de início da conversão de criptografia de volume

A partir do ONTAP 9.3, você pode usar o `volume encryption conversion start` comando para habilitar a criptografia de um volume existente "no lugar", sem ter que mover o volume para um local diferente.

Depois de iniciar uma operação de conversão, ela deve ser concluída. Se você encontrar um problema de desempenho durante a operação, você pode executar o `volume encryption conversion pause` comando para pausar a operação e o `volume encryption conversion resume` comando para retomar a operação.

> Não pode utilizar `volume encryption conversion start` para converter um volume SnapLock.

Passos

1. Ativar encriptação num volume existente:

   `volume encryption conversion start -vserver SVM_name -volume volume_name`

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

   O comando a seguir habilita a criptografia no volume `vol1`existente :

   ```
   cluster1::> volume encryption conversion start -vserver vs1 -volume vol1
   ```

   O sistema cria uma chave de criptografia para o volume. Os dados no volume são criptografados.

2. Verifique o status da operação de conversão:

   `volume encryption conversion show`

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

   O comando a seguir exibe o status da operação de conversão:

   ```
   cluster1::> volume encryption conversion show

   Vserver   Volume   Start Time           Status
   -------   ------   ------------------   --------------------------
   vs1       vol1     9/18/2017 17:51:41   Phase 2 of 2 is in progress.
   ```

3. Quando a operação de conversão estiver concluída, verifique se o volume está ativado para criptografia:

   `volume show -is-encrypted true`

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

   O comando a seguir exibe os volumes criptografados em `cluster1`:

```
cluster1::> volume show -is-encrypted true

Vserver  Volume  Aggregate  State  Type  Size  Available  Used
-------  ------  ---------  -----  ----  -----  ---------  ----
vs1      vol1    aggr2     online    RW  200GB    160.0GB  20%
```

Resultado

Se você estiver usando um servidor KMIP para armazenar as chaves de criptografia de um nó, o ONTAP automaticamente "envia" uma chave de criptografia para o servidor quando você criptografa um volume.

Ative a criptografia em um volume existente com o comando volume Move start

Você pode usar o `volume move start` comando para habilitar a criptografia movendo um volume existente. Você deve usar `volume move start` no ONTAP 9.2 e anterior. Você pode usar o mesmo agregado ou um agregado diferente.

Sobre esta tarefa

- A partir do ONTAP 9.8, pode utilizar `volume move start` para ativar a encriptação num volume SnapLock ou FlexGroup.
- A partir do ONTAP 9.4, se você ativar o "cc-mode" quando você configurar o Gerenciador de chaves integrado, os volumes criados com o `volume move start` comando serão automaticamente criptografados. Não é necessário especificar `-encrypt-destination true`.
- A partir do ONTAP 9.6, você pode usar a criptografia em nível de agregado para atribuir chaves ao agregado contendo para os volumes a serem movidos. Um volume criptografado com uma chave exclusiva é chamado de *volume NVE* (ou seja, usa criptografia de volume NetApp). Um volume criptografado com uma chave de nível agregado é chamado de *volume NAE* (para criptografia agregada NetApp). Os volumes de texto sem formatação não são suportados em agregados NAE.
- A partir do ONTAP 9.14,1, é possível criptografar um volume raiz do SVM com NVE. Para obter mais informações, Configurar o NetApp volume Encryption em um volume raiz da SVMconsulte .

Antes de começar

Você deve ser um administrador de cluster para executar essa tarefa ou um administrador SVM a quem o administrador de cluster delegou autoridade.

"Delegando autoridade para executar o comando de movimentação de volume"

Passos

1. Mova um volume existente e especifique se a criptografia está ativada no volume:

Para converter…	Use este comando…

Um volume de texto sem formatação para um volume NVE	`volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-destination true`
Um volume NVE ou de texto sem formatação para um volume NAE (assumindo que a criptografia no nível de agregado esteja ativada no destino)	`volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-with-aggr-key true`
Um volume NAE para um volume NVE	`volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-with-aggr-key false`
Um volume NAE para um volume de texto sem formatação	`volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-destination false -encrypt-with-aggr-key false`
Um volume NVE para um volume de texto sem formatação	`volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-destination false`

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

O comando a seguir converte um volume de texto sem formatação nomeado `vol1` em um volume NVE:

```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination
-aggregate aggr2 -encrypt-destination true
```

Supondo que a criptografia em nível de agregado esteja ativada no destino, o comando a seguir converte um volume NVE ou de texto sem formatação nomeado `vol1` em um volume NAE:

```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination
-aggregate aggr2 -encrypt-with-aggr-key true
```

O comando a seguir converte um volume NAE nomeado `vol2` em um volume NVE:

```
cluster1::> volume move start -vserver vs1 -volume vol2 -destination
-aggregate aggr2 -encrypt-with-aggr-key false
```

O comando a seguir converte um volume NAE nomeado `vol2` para um volume de texto sem formatação:

```
cluster1::> volume move start -vserver vs1 -volume vol2 -destination
-aggregate aggr2 -encrypt-destination false -encrypt-with-aggr-key false
```

O comando a seguir converte um volume NVE nomeado `vol2` em um volume de texto sem formatação:

```
cluster1::> volume move start -vserver vs1 -volume vol2 -destination
-aggregate aggr2 -encrypt-destination false
```

2. Exibir o tipo de criptografia de volumes de cluster:

   `volume show -fields encryption-type none|volume|aggregate`

   O `encryption-type` campo está disponível no ONTAP 9.6 e posterior.

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

   O comando a seguir exibe o tipo de criptografia de volumes no `cluster2`:

```
cluster2::> volume show -fields encryption-type

vserver  volume  encryption-type
-------  ------  ---------------
vs1      vol1    none
vs2      vol2    volume
vs3      vol3    aggregate
```

3. Verifique se os volumes estão ativados para criptografia:

   `volume show -is-encrypted true`

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

   O comando a seguir exibe os volumes criptografados em `cluster2`:

```
cluster2::> volume show -is-encrypted true

Vserver  Volume  Aggregate  State  Type  Size  Available  Used
-------  ------  ---------  -----  ----  -----  ---------  ----
vs1      vol1    aggr2     online    RW  200GB    160.0GB  20%
```

Resultado

Se você estiver usando um servidor KMIP para armazenar as chaves de criptografia de um nó, o ONTAP enviará automaticamente uma chave de criptografia ao servidor quando você criptografar um volume.

Configurar o NetApp volume Encryption em um volume raiz da SVM

A partir do ONTAP 9.14,1, é possível ativar o NetApp volume Encryption (NVE) em um volume raiz de VM de storage (SVM). Com o NVE, o volume raiz é criptografado com uma chave exclusiva, o que possibilita maior segurança no SVM.

Sobre esta tarefa

O NVE em um volume raiz do SVM só pode ser ativado após a criação do SVM.

Antes de começar

- O volume raiz do SVM não deve estar em um agregado criptografado com o NetApp Aggregate Encryption (NAE).
- Você deve ter habilitado a criptografia com o Gerenciador de chaves integrado ou um gerenciador de chaves externo.
- Você deve estar executando o ONTAP 9.14,1 ou posterior.
- Para migrar um SVM que contenha um volume raiz criptografado com NVE, você precisa converter o volume raiz do SVM em um volume de texto sem formatação após a conclusão da migração e, em seguida, criptografar novamente o volume raiz do SVM.
  - Se o agregado de destino da migração SVM usar NAE, o volume raiz herdará NAE por padrão.
- Se o SVM estiver em uma relação de recuperação de desastres do SVM:
  - As configurações de criptografia em um SVM espelhado não são copiadas para o destino. Se você ativar o NVE na origem ou no destino, habilite o NVE separadamente no volume raiz do SVM espelhado.
  - Se todos os agregados no cluster de destino usarem NAE, o volume raiz da SVM usará NAE.

Passos

Você pode ativar o NVE em um volume raiz da SVM com a CLI ou o Gerenciador de sistema do ONTAP.

CLI

Você pode ativar o NVE no volume raiz da SVM no local ou movendo o volume entre agregados.

Criptografe o volume raiz no lugar

1. Converta o volume raiz para um volume criptografado:

   `volume encryption conversion start -vserver` *`svm_name`* `-volume` *`volume`*

2. Confirme se a criptografia foi bem-sucedida. O `volume show -encryption-type volume` exibe uma lista de todos os volumes usando NVE.

Criptografe o volume raiz do SVM movendo-o.

1. Iniciar uma movimentação de volume:

   `volume move start -vserver` *`svm_name`* `-volume` *`volume`* `-destination-aggregate` *`aggregate`* `-encrypt-with-aggr-key false -encrypt-destination true`

   Para obter mais informações sobre `volume move`o , Mover um volumeconsulte .

2. Confirme se a `volume move` operação foi bem-sucedida com o `volume move show` comando. O `volume show -encryption-type volume` exibe uma lista de todos os volumes usando NVE.

System Manager

1. Navegue até **armazenamento** > **volumes**.
2. Ao lado do nome do volume raiz SVM que você deseja criptografar, selecione image:icon_kabob.gif<strong class=""Ícone de opções do menu"">Editar.
3. No título **armazenamento e Otimização**, selecione **Ativar criptografia**.
4. Selecione **Guardar**.

Habilite a criptografia de volume raiz do nó

A partir do ONTAP 9.8, você pode usar a criptografia de volume do NetApp para proteger o volume raiz do nó.

Sobre esta tarefa

Este procedimento aplica-se ao volume raiz do nó. Isso não se aplica aos volumes raiz do SVM. Os volumes de raiz da SVM podem ser protegidos com a criptografia no nível de agregado e, A partir do ONTAP 9.14,1, NVE.

Assim que a criptografia de volume raiz começar, ela deve ser concluída. Não é possível interromper a operação. Quando a criptografia estiver concluída, você não poderá atribuir uma nova chave ao volume raiz e não poderá executar uma operação de limpeza segura.

Antes de começar

- Seu sistema precisa estar usando uma configuração de HA.
- O volume raiz do nó já deve ser criado.
- Seu sistema precisa ter um gerenciador de chaves integrado ou um servidor externo de gerenciamento de chaves usando o Key Management Interoperability Protocol (KMIP).

Passos

1. Encriptar o volume raiz:

   ```
   volume encryption conversion start -vserver SVM_name -volume root_vol_name
   ```

2. Verifique o status da operação de conversão:

   ```
   volume encryption conversion show
   ```

3. Quando a operação de conversão estiver concluída, verifique se o volume está criptografado:

   ```
   volume show -fields
   ```

   A seguir mostra exemplos de saída para um volume criptografado.

   ```
   ::> volume show -vserver xyz  -volume vol0 -fields is-encrypted
   vserver    volume is-encrypted
   ---------- ------ ------------
   xyz        vol0   true
   ```

Configurar a criptografia baseada em hardware do NetApp

Configure a visão geral da criptografia baseada em hardware do NetApp

A criptografia baseada em hardware da NetApp oferece suporte à criptografia de disco completo (FDE) dos dados conforme eles são gravados. Os dados não podem ser lidos sem uma chave de criptografia armazenada no firmware. A chave de criptografia, por sua vez, é acessível apenas para um nó autenticado.

Compreensão da criptografia baseada em hardware do NetApp

Um nó se autentica em uma unidade de autocriptografia usando uma chave de autenticação recuperada de um servidor de gerenciamento de chaves externo ou Gerenciador de chaves integrado:

- O 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). É uma prática recomendada configurar servidores de gerenciamento de chaves externos em um sistema de armazenamento diferente dos seus dados.
- O Gerenciador de chaves integrado é uma ferramenta integrada que serve chaves de autenticação para nós do mesmo sistema de storage que seus dados.

Você pode usar a criptografia de volume do NetApp com criptografia baseada em hardware para "criptografar dados" em unidades com autocriptografia.

Quando as unidades de autocriptografia estão ativadas, o despejo de memória também é criptografado.

Se um par de HA estiver usando a criptografia de unidades SAS ou NVMe (SED, NSE, FIPS), siga as instruções no Retornar uma unidade FIPS ou SED para o modo desprotegido tópico para todas as unidades do par de HA antes de inicializar o sistema (opções de inicialização 4 ou 9). Se não fizer isso, poderá resultar em perda de dados futura se as unidades forem reaproveitadas.

Tipos de unidade com autocriptografia compatíveis

Dois tipos de unidades com autocriptografia são compatíveis:

- As unidades SAS ou NVMe com certificação FIPS são compatíveis com todos os sistemas FAS e AFF. Essas unidades, chamadas unidades *FIPS,* estão em conformidade com os requisitos da publicação padrão Federal de processamento de informações 140-2, nível 2. Os recursos certificados habilitam proteções além da criptografia, como impedir ataques de negação de serviço na unidade. As unidades FIPS não podem ser combinadas com outros tipos de unidades no mesmo nó ou par de HA.
- A partir do ONTAP 9.6, as unidades NVMe com autocriptografia que não foram submetidas ao teste FIPS são compatíveis com sistemas AFF A800, A320 e posteriores. Essas unidades, chamadas *SEDs*, oferecem os mesmos recursos de criptografia que as unidades FIPS, mas podem ser combinadas com unidades sem criptografia no mesmo nó ou par de HA.
- Todas as unidades validadas FIPS usam um módulo criptográfico de firmware que passou pela validação FIPS. O módulo criptográfico da unidade FIPS não usa nenhuma chave gerada fora da unidade (a senha de autenticação que é inserida na unidade é usada pelo módulo criptográfico de firmware da unidade para obter uma chave de criptografia de chave).

Unidades com autocriptografia são unidades que não são unidades FIPS ou SEDs.

Se você estiver usando o NSE em um sistema com um módulo Flash Cache, também deverá ativar o NVE ou NAE. O NSE não criptografa dados que residem no módulo Flash Cache.

Quando usar o gerenciamento de chaves externas

Embora seja mais barato e normalmente mais conveniente usar o gerenciador de chaves integrado, você deve usar o gerenciamento de chaves externas se alguma das seguintes opções for verdadeira:

- A política da sua organização requer uma solução de gerenciamento de chaves que use um módulo criptográfico FIPS 140-2 nível 2 (ou superior).
- Você precisa de uma solução de vários clusters, com gerenciamento centralizado de chaves de criptografia.
- Sua empresa requer a segurança adicional de armazenar chaves de autenticação em um sistema ou em um local diferente dos dados.

Detalhes do suporte

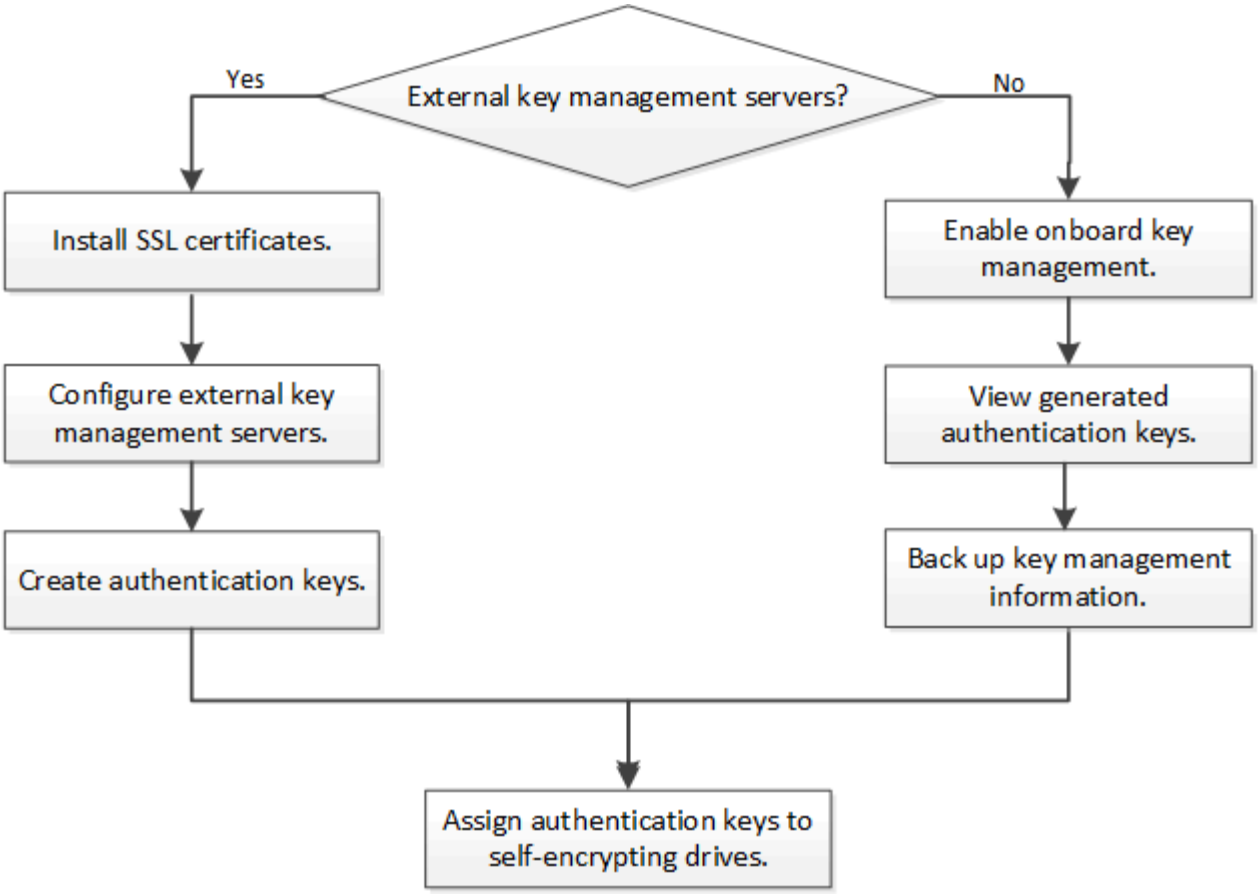
A tabela a seguir mostra detalhes importantes do suporte à criptografia de hardware. Consulte a Matriz de interoperabilidade para obter as informações mais recentes sobre servidores KMIP, sistemas de storage e compartimentos de disco compatíveis.

Recurso ou recurso	Detalhes do suporte

Conjuntos de discos não homogéneos	• As unidades FIPS não podem ser combinadas com outros tipos de unidades no mesmo nó ou par de HA. Pares de HA em conformidade podem coexistir com pares de HA não conformes no mesmo cluster. • As SEDs podem ser combinadas com unidades sem criptografia no mesmo nó ou par de HA.
Tipo de unidade	• As unidades FIPS podem ser unidades SAS ou NVMe. • As SEDs devem ser unidades NVMe.
Interfaces de rede de 10 GB	A partir do ONTAP 9.3, as configurações de gerenciamento de chaves KMIP suportam interfaces de rede de 10 GB para comunicações com servidores de gerenciamento de chaves externas.
Portas para comunicação com o servidor de gerenciamento de chaves	A partir do ONTAP 9.3, você pode usar qualquer porta de controlador de armazenamento para comunicação com o servidor de gerenciamento de chaves. Caso contrário, você deve usar a porta e0M para comunicação com servidores de gerenciamento de chaves. Dependendo do modelo do controlador de storage, algumas interfaces de rede podem não estar disponíveis durante o processo de inicialização para comunicação com servidores de gerenciamento de chaves.
MetroCluster (MCC)	• As unidades NVMe são compatíveis com MCC. • As unidades SAS não suportam MCC.

Fluxo de trabalho de criptografia baseado em hardware

Você deve configurar os serviços de gerenciamento de chaves antes que o cluster possa se autenticar na unidade de autocriptografia. Você pode usar um servidor de gerenciamento de chaves externo ou um gerenciador de chaves integrado.



Informações relacionadas

- "NetApp Hardware Universe"
- "Criptografia de volumes do NetApp e criptografia agregada do NetApp"

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:

   ```
   clusterl::> 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:
   000000000000000002000000000001006268333f870860128fbe17d393e5083b00000000
   00000000
   ```

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
[...]
```

Configurar o gerenciamento de chaves integradas

Habilite o gerenciamento de chaves integradas no ONTAP 9.6 e posterior

Você pode usar o Gerenciador de chaves integrado para autenticar nós de cluster em uma unidade FIPS ou SED. O Gerenciador de chaves integrado é uma ferramenta integrada que serve chaves de autenticação para nós do mesmo sistema de storage que seus dados. O Gerenciador de chaves integrado é compatível com FIPS-140-2 nível 1.

Você pode usar o Gerenciador de chaves integrado para proteger as chaves que o cluster usa para acessar dados criptografados. É necessário habilitar o Gerenciador de chaves integrado em cada cluster que acessa um volume criptografado ou um disco com autocriptografia.

Sobre esta tarefa

Você deve executar o `security key-manager onboard enable` comando sempre que adicionar um nó ao cluster. Nas configurações do MetroCluster, você deve executar `security key-manager onboard`

`enable` primeiro no cluster local e, em seguida, executar `security key-manager onboard sync` no cluster remoto, usando a mesma senha em cada um.

Por padrão, você não é obrigado a inserir a senha do gerenciador de chaves quando um nó é reinicializado. Exceto no MetroCluster, você pode usar a `cc-mode-enabled=yes` opção para exigir que os usuários digitem a senha após uma reinicialização.

Quando o Gerenciador de chaves integrado está habilitado no modo Common Criteria (`cc-mode-enabled=yes`), o comportamento do sistema é alterado das seguintes maneiras:

- O sistema monitoriza as tentativas consecutivas de frase-passe do cluster falhadas ao funcionar no modo Common Criteria (critérios comuns).

  Se a encriptação de armazenamento NetApp (NSE) estiver ativada e não conseguir introduzir a frase-passe correta do cluster no arranque, o sistema não pode autenticar-se nas suas unidades e reinicia automaticamente. Para corrigir isso, você deve inserir a senha correta do cluster no prompt de inicialização. Uma vez iniciado, o sistema permite até 5 tentativas consecutivas para inserir corretamente a senha do cluster em um período de 24 horas para qualquer comando que exija a senha do cluster como um parâmetro. Se o limite for atingido (por exemplo, você não conseguiu inserir corretamente a senha do cluster 5 vezes em uma linha), então você deve esperar o período de tempo limite de 24 horas para decorrer, ou você deve reiniciar o nó, a fim de redefinir o limite.

- As atualizações de imagem do sistema usam o certificado de assinatura de código NetApp RSA-3072 juntamente com os digests assinados por código SHA-384 para verificar a integridade da imagem em vez do certificado de assinatura de código NetApp RSA-2048 usual e os digests assinados por código SHA-256.

  O comando upgrade verifica se o conteúdo da imagem não foi alterado ou corrompido verificando várias assinaturas digitais. O processo de atualização da imagem prossegue para o próximo passo se a validação for bem-sucedida; caso contrário, a atualização da imagem falhará. Consulte a página de manual ""imagem de cluster"" para obter informações sobre atualizações do sistema.

O Gerenciador de chaves integrado armazena as chaves na memória volátil. O conteúdo da memória volátil é apagado quando o sistema é reinicializado ou interrompido. Em condições normais de funcionamento, o conteúdo da memória volátil será apagado dentro de 30sMB quando um sistema for interrompido.

Antes de começar

- Se você estiver usando o NSE com um servidor de gerenciamento de chaves externas (KMIP), exclua o banco de dados do gerenciador de chaves externo.

  "Transição para o gerenciamento de chaves integrado do gerenciamento de chaves externas"

- Você deve ser um administrador de cluster para executar esta tarefa.
- Você deve configurar o ambiente MetroCluster antes que o Gerenciador de chaves integrado seja configurado.

Passos

1. Inicie o comando de configuração do gerenciador de chaves:

```
security key-manager onboard enable -cc-mode-enabled yes|no
```

> Defina `cc-mode-enabled=yes` para exigir que os usuários inseram a senha do gerenciador de chaves após uma reinicialização. A `- cc-mode-enabled` opção não é suportada nas configurações do MetroCluster. O `security key-manager onboard enable` comando substitui o `security key-manager setup` comando.

O exemplo a seguir inicia o comando de configuração do gerenciador de chaves no cluster1 sem exigir que a senha seja inserida após cada reinicialização:

```
cluster1::> security key-manager onboard enable

Enter the cluster-wide passphrase for onboard key management in Vserver
"cluster1"::    <32..256 ASCII characters long text>
Reenter the cluster-wide passphrase:    <32..256 ASCII characters long
text>
```

2. No prompt de frase-passe, insira uma frase-passe entre 32 e 256 carateres ou, para "cc-mode", uma frase-passe entre 64 e 256 carateres.

> Se a senha "'cc-mode'" especificada for inferior a 64 carateres, haverá um atraso de cinco segundos antes que a operação de configuração do gerenciador de chaves exiba o prompt de senha novamente.

3. No prompt de confirmação da senha, redigite a senha.
4. 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 exemplo a seguir verifica se as chaves de autenticação foram criadas para `cluster1`:

```
cluster1::> security key-manager key query
       Vserver: cluster1
   Key Manager: onboard
          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: onboard
          Node: node2

Key Tag                                  Key Type  Restored
---------------------------------------  --------  --------
node1                                    NSE-AK    yes
    Key ID:
000000000000000002000000000001000c11b3863f78c2273343d7ec5a67762e00000000
00000000
node2                                    NSE-AK    yes
    Key ID:
000000000000000002000000000001006f4e2513353a674305872a4c9f3bf79700000000
00000000
```

Depois de terminar

Copie a senha para um local seguro fora do sistema de armazenamento para uso futuro.

Todas as informações de gerenciamento de chaves são automaticamente armazenadas no banco de dados replicado (RDB) para o cluster. Você também deve fazer backup das informações manualmente para uso em caso de desastre.

Habilite o gerenciamento de chaves integradas no ONTAP 9.5 e versões anteriores

Você pode usar o Gerenciador de chaves integrado para autenticar nós de cluster em uma unidade FIPS ou SED. O Gerenciador de chaves integrado é uma ferramenta integrada que serve chaves de autenticação para nós do mesmo sistema de storage que seus dados. O Gerenciador de chaves integrado é compatível com FIPS-140-2 nível 1.

Você pode usar o Gerenciador de chaves integrado para proteger as chaves que o cluster usa para acessar

dados criptografados. É necessário habilitar o Gerenciador de chaves integrado em cada cluster que acessa um volume criptografado ou um disco com autocriptografia.

Sobre esta tarefa

Você deve executar o `security key-manager setup` comando sempre que adicionar um nó ao cluster.

Se você tiver uma configuração do MetroCluster, revise estas diretrizes:

- No ONTAP 9.5, você deve executar `security key-manager setup` no cluster local e `security key-manager setup -sync-metrocluster-config yes` no cluster remoto, usando a mesma senha em cada um.
- Antes do ONTAP 9.5, você deve executar `security key-manager setup` no cluster local, esperar aproximadamente 20 segundos e, em seguida, executar `security key-manager setup` no cluster remoto, usando a mesma senha em cada um.

Por padrão, você não é obrigado a inserir a senha do gerenciador de chaves quando um nó é reinicializado. A partir do ONTAP 9.4, pode utilizar a `-enable-cc-mode yes` opção para exigir que os utilizadores introduzam a frase-passe após uma reinicialização.

Para NVE, se você definir `-enable-cc-mode yes`o , os volumes criados com os `volume create` comandos e `volume move start` serão criptografados automaticamente. Para `volume create`, não é necessário especificar `-encrypt true`. Para `volume move start`, não é necessário especificar `-encrypt-destination true`.

Depois de uma tentativa de frase-passe com falha, tem de reiniciar o nó novamente.

Antes de começar

- Se você estiver usando o NSE com um servidor de gerenciamento de chaves externas (KMIP), exclua o banco de dados do gerenciador de chaves externo.

  "Transição para o gerenciamento de chaves integrado do gerenciamento de chaves externas"

- Você deve ser um administrador de cluster para executar esta tarefa.
- Você deve configurar o ambiente MetroCluster antes que o Gerenciador de chaves integrado seja configurado.

Passos

1. Inicie a configuração do gerenciador de chaves:

   ```
   security key-manager setup -enable-cc-mode yes|no
   ```

   A partir do ONTAP 9.4, pode utilizar a `-enable-cc-mode yes` opção para exigir que os utilizadores introduzam a frase-passe do gestor de chaves após uma reinicialização. Para NVE, se você definir `-enable-cc-mode yes`o , os volumes criados com os `volume create` comandos e `volume move start` serão criptografados automaticamente.

   O exemplo a seguir inicia a configuração do gerenciador de chaves no cluster1 sem exigir que a senha seja inserida após cada reinicialização:

```
cluster1::> security key-manager setup
Welcome to the key manager setup wizard, which will lead you through
the steps to add boot information.

...

Would you like to use onboard key-management? {yes, no} [yes]:
Enter the cluster-wide passphrase:    <32..256 ASCII characters long
text>
Reenter the cluster-wide passphrase:    <32..256 ASCII characters long
text>
```

2. Digite `yes` no prompt para configurar o gerenciamento de chaves integradas.
3. No prompt de frase-passe, insira uma frase-passe entre 32 e 256 carateres ou, para "cc-mode", uma frase-passe entre 64 e 256 carateres.

> Se a senha "'cc-mode'" especificada for inferior a 64 carateres, haverá um atraso de cinco segundos antes que a operação de configuração do gerenciador de chaves exiba o prompt de senha novamente.

4. No prompt de confirmação da senha, redigite a senha.
5. Verifique se as chaves estão configuradas para todos os nós:

   `security key-manager key show`

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

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

Node: node1
Key Store: onboard
Key ID                                                           Used By
-----------------------------------------------------------------------
--------
000000000000000020000000000010059851742AF2703FC91369B7DB47C4722 NSE-AK
000000000000000020000000000001008C07CC0AF1EF49E0105300EFC83004BF NSE-AK

Node: node2
Key Store: onboard
Key ID                                                           Used By
-----------------------------------------------------------------------
--------
000000000000000020000000000010059851742AF2703FC91369B7DB47C4722 NSE-AK
000000000000000020000000000001008C07CC0AF1EF49E0105300EFC83004BF NSE-AK
```

Depois de terminar

Todas as informações de gerenciamento de chaves são automaticamente armazenadas no banco de dados replicado (RDB) para o cluster.

Sempre que você configurar a senha do Gerenciador de chaves integrado, você também deve fazer backup das informações manualmente para um local seguro fora do sistema de armazenamento para uso em caso de desastre. "Faça backup manual das informações de gerenciamento de chaves integradas"Consulte .

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

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 acessar dados 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.

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 key query -key-type NSE-AK` comando para exibir IDs de chave.

   ```
   cluster1::> storage encryption disk modify -disk 0.10.* -data-key-id
   000000000000000002000000000010019215b9738bc7b43d4698c80246db1f4

   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
000000000000000002000000000010019215b9738bc7b43d4698c80246db1f4
0.0.1   data
000000000000000002000000000010059851742AF2703FC91369B7DB47C4722
[...]
```

Atribuir uma chave de autenticação FIPS 140-2-2 a uma unidade FIPS

Você pode usar o `storage encryption disk modify` comando com a `-fips-key-id` opção para atribuir uma chave de autenticação FIPS 140-2 a uma unidade FIPS. Os nós de cluster usam essa chave para operações de unidade que não sejam o acesso a dados, como impedir ataques de negação de serviço na unidade.

Sobre esta tarefa

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

Este procedimento não causa interrupções.

Antes de começar

O firmware da unidade deve ser compatível com a conformidade FIPS 140-2-2. O "Ferramenta de Matriz de interoperabilidade do NetApp" contém informações sobre as versões de firmware da unidade suportadas.

Passos

1. Primeiro, você deve garantir que atribuiu uma chave de autenticação de dados. Isso pode ser feito com o uso de um gerenciador de chaves externo ou um gerenciador de chaves integrado. Verifique se a chave está atribuída com o comando `storage encryption disk show`.
2. Atribuir uma chave de autenticação FIPS 140-2 a SEDs:

   `storage encryption disk modify -disk` *`disk_id`* `-fips-key-id` *`fips_authentication_key_id`*

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

```
cluster1::> storage encryption disk modify -disk 2.10.* -fips-key-id
6A1E21D8000000000100000000000005A1FB4EE8F62FD6D8AE6754C9019F35A

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

3. Verifique se a chave de autenticação foi atribuída:

   `storage encryption disk show -fips`

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

```
cluster1::> storage encryption disk show -fips
Disk    Mode FIPS-Compliance Key ID
------  ----
-------------------------------------------------------------------
2.10.0  full
6A1E21D8000000000100000000000005A1FB4EE8F62FD6D8AE6754C9019F35A
2.10.1  full
6A1E21D8000000000100000000000005A1FB4EE8F62FD6D8AE6754C9019F35A
[...]
```

Habilite o modo compatível com FIPS em todo o cluster para conexões de servidor KMIP

Você pode usar o `security config modify` comando com a `-is-fips-enabled` opção de ativar o modo compatível com FIPS em todo o cluster para dados em trânsito. Isso força o cluster a usar o OpenSSL no modo FIPS ao se conetar a servidores KMIP.

Sobre esta tarefa

Quando você ativa o modo compatível com FIPS em todo o cluster, o cluster usará automaticamente somente pacotes de codificação validados por FIPS e TLS1,2. O modo compatível com FIPS em todo o cluster está desativado por padrão.

Você deve reinicializar os nós de cluster manualmente após modificar a configuração de segurança em todo o cluster.

Antes de começar

- O controlador de storage deve ser configurado no modo compatível com FIPS.
- Todos os servidores KMIP precisam oferecer suporte a TLSv1,2. O sistema requer o TLSv1,2 para concluir a conexão com o servidor KMIP quando o modo compatível com FIPS em todo o cluster estiver ativado.

Passos

1. Defina o nível de privilégio como avançado:

   `set -privilege advanced`

2. Verifique se o TLSv1,2 é suportado:

   `security config show -supported-protocols`

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

```
cluster1::> security config show
          Cluster                                                 Cluster
Security
Interface FIPS Mode  Supported Protocols     Supported Ciphers Config
Ready
--------- ---------- ----------------------- -----------------
----------------
SSL       false      TLSv1.2, TLSv1.1, TLSv1 ALL:!LOW:         yes
                                             !aNULL:!EXP:
                                             !eNULL
```

3. Ativar o modo compatível com FIPS em todo o cluster:

   `security config modify -is-fips-enabled true -interface SSL`

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

4. Reinicializar os nós de cluster manualmente.
5. Verifique se o modo compatível com FIPS em todo o cluster está ativado:

   `security config show`

```
cluster1::> security config show
          Cluster                                                 Cluster
Security
Interface FIPS Mode  Supported Protocols     Supported Ciphers Config
Ready
--------- ---------- ----------------------- -----------------
----------------
SSL       true       TLSv1.2, TLSv1.1        ALL:!LOW:         yes
                                             !aNULL:!EXP:
                                             !eNULL:!RC4
```

Gerenciar a criptografia NetApp

Descriptografe dados de volume

Você pode usar o `volume move start` comando para mover e descriptografar dados de volume.

Antes de começar

Você deve ser um administrador de cluster para executar esta tarefa. Como alternativa, você pode ser um administrador SVM a quem o administrador do cluster delegou autoridade. Para obter mais informações, "Delegar autoridade para executar o comando de movimentação de volume"consulte .

Passos

1. Mova um volume criptografado existente e descriptografe os dados no volume:

   `volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-destination false`

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

   O comando a seguir move um volume existente nomeado `vol1` para o agregado de destino `aggr3` e descriptografa os dados no volume:

   ```
   cluster1::> volume move start -vserver vs1 -volume vol1 -destination
   -aggregate aggr3 -encrypt-destination false
   ```

   O sistema exclui a chave de criptografia do volume. Os dados no volume não são criptografados.

2. Verifique se o volume está desativado para criptografia:

   `volume show -encryption`

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

   O comando a seguir exibe se os volumes em `cluster1` são criptografados:

   ```
   cluster1::> volume show -encryption

   Vserver  Volume   Aggregate   State    Encryption State
   -------  ------   ---------   -----    ----------------
   vs1      vol1     aggr1       online   none
   ```

Mover um volume criptografado

Você pode usar o `volume move start` comando para mover um volume criptografado. O volume movido pode residir no mesmo agregado ou em um agregado diferente.

Sobre esta tarefa

A movimentação falhará se o nó de destino ou o volume de destino não suportar criptografia de volume.

A `-encrypt-destination` opção para `volume move start` o padrão é verdadeiro para volumes criptografados. O requisito para especificar que não deseja que o volume de destino seja criptografado garante que você não descriptografe inadvertidamente os dados no volume.

Antes de começar

Você deve ser um administrador de cluster para executar esta tarefa. Como alternativa, você pode ser um administrador SVM a quem o administrador do cluster delegou autoridade. Para obter mais informações, "delegar autoridade para executar o comando de movimentação de volume"consulte .

Passos

1. Mova um volume criptografado existente e deixe os dados no volume criptografados:

   `volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name`

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

   O comando a seguir move um volume existente nomeado `vol1` para o agregado de destino `aggr3` e deixa os dados no volume criptografados:

   ```
   cluster1::> volume move start -vserver vs1 -volume vol1 -destination
   -aggregate aggr3
   ```

2. Verifique se o volume está ativado para criptografia:

   `volume show -is-encrypted true`

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

   O comando a seguir exibe os volumes criptografados em `cluster1`:

   ```
   cluster1::> volume show -is-encrypted true

   Vserver  Volume  Aggregate  State  Type  Size  Available  Used
   -------  ------  ---------  -----  ----  -----  ---------  ----
   vs1      vol1    aggr3     online    RW  200GB    160.0GB  20%
   ```

Delegar autoridade para executar o comando de movimentação de volume

Você pode usar o `volume move` comando para criptografar um volume existente, mover um volume criptografado ou descriptografar um volume. Os administradores de cluster podem executar `volume move` o comando sozinho ou delegar a autoridade para executar o comando aos administradores do SVM.

Sobre esta tarefa

Por padrão, a função é atribuída aos administradores de SVM `vsadmin`, que não inclui a autoridade para mover volumes. É necessário atribuir a `vsadmin-volume` função aos administradores do SVM para permitir que eles executem o `volume move` comando.

Passo

1. Delegar autoridade para executar o `volume move` comando:

   `security login modify -vserver SVM_name -user-or-group-name user_or_group_name -application application -authmethod authentication_method -role vsadmin-volume`

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

O comando a seguir concede ao administrador SVM autoridade para executar o `volume move` comando.

```
cluster1::>security login modify -vserver engData -user-or-group-name
SVM-admin -application ssh -authmethod domain -role vsadmin-volume
```

Altere a chave de criptografia de um volume com o comando de início de rechavear de criptografia de volume

É uma prática recomendada de segurança alterar a chave de criptografia para um volume periodicamente. A partir do ONTAP 9.3, você pode usar o `volume encryption rekey start` comando para alterar a chave de criptografia.

Sobre esta tarefa

Depois de iniciar uma operação de rechavear, ela deve ser concluída. Não há retorno à chave antiga. Se você encontrar um problema de desempenho durante a operação, você pode executar o `volume encryption rekey pause` comando para pausar a operação e o `volume encryption rekey resume` comando para retomar a operação.

Até que a operação de rechavear termine, o volume terá duas teclas. Novas gravações e suas leituras correspondentes usarão a nova chave. Caso contrário, as leituras usarão a chave antiga.

Você não pode usar `volume encryption rekey start` para rechavear um volume SnapLock.

Passos

1. Alterar uma chave de encriptação:

   `volume encryption rekey start -vserver SVM_name -volume volume_name`

   O comando a seguir altera a chave de criptografia `vol1` no SVM`vs1`:

   ```
   cluster1::> volume encryption rekey start -vserver vs1 -volume vol1
   ```

2. Verifique o estado da operação de rechavear:

   `volume encryption rekey show`

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

   O seguinte comando apresenta o estado da operação de rechavear:

```
cluster1::> volume encryption rekey show

Vserver   Volume   Start Time           Status
-------   ------   ------------------   --------------------------
vs1       vol1     9/18/2017 17:51:41   Phase 2 of 2 is in progress.
```

3. Quando a operação de rechavear estiver concluída, verifique se o volume está ativado para encriptação:

   `volume show -is-encrypted true`

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

   O comando a seguir exibe os volumes criptografados em `cluster1`:

```
cluster1::> volume show -is-encrypted true

Vserver  Volume  Aggregate  State  Type  Size  Available  Used
-------  ------  ---------  -----  ----  -----  ---------  ----
vs1      vol1    aggr2     online    RW  200GB    160.0GB  20%
```

Altere a chave de criptografia de um volume com o comando volume Move start

É uma prática recomendada de segurança alterar a chave de criptografia para um volume periodicamente. Você pode usar o `volume move start` comando para alterar a chave de criptografia. Você deve usar `volume move start` no ONTAP 9.2 e anterior. O volume movido pode residir no mesmo agregado ou em um agregado diferente.

Sobre esta tarefa

Você não pode usar `volume move start` para rechavear um volume SnapLock ou FlexGroup.

Antes de começar

Você deve ser um administrador de cluster para executar esta tarefa. Como alternativa, você pode ser um administrador SVM a quem o administrador do cluster delegou autoridade. Para obter mais informações, "delegar autoridade para executar o comando de movimentação de volume"consulte .

Passos

1. Mova um volume existente e altere a chave de criptografia:

   `volume move start -vserver` *`SVM_name`* `-volume` *`volume_name`* `-destination-aggregate` *`aggregate_name`* `-generate-destination-key true`

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

   O comando a seguir move um volume existente nomeado **`vol1`** para o agregado de destino **`aggr2`** e altera a chave de criptografia:

```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination
-aggregate aggr2 -generate-destination-key true
```

Uma nova chave de criptografia é criada para o volume. Os dados no volume permanecem criptografados.

2. Verifique se o volume está ativado para criptografia:

   `volume show -is-encrypted true`

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

   O comando a seguir exibe os volumes criptografados em `cluster1`:

```
cluster1::> volume show -is-encrypted true

Vserver  Volume  Aggregate  State  Type  Size  Available  Used
-------  ------  ---------  -----  ----  -----  ---------  ----
vs1      vol1    aggr2     online    RW  200GB    160.0GB  20%
```

Rode as chaves de autenticação para a encriptação de armazenamento NetApp

Você pode girar as chaves de autenticação ao usar a criptografia de armazenamento NetApp (NSE).

Sobre esta tarefa

A rotação de chaves de autenticação em um ambiente NSE é suportada se você estiver usando o KMIP (External Key Manager).

> A rotação de chaves de autenticação em um ambiente NSE não é compatível com OKM (Onboard Key Manager).

Passos

1. Use o `security key-manager create-key` comando para gerar novas chaves de autenticação.

   É necessário gerar novas chaves de autenticação antes de poder alterar as chaves de autenticação.

2. Use o `storage encryption disk modify -disk * -data-key-id` comando para alterar as chaves de autenticação.

Eliminar um volume encriptado

Você pode usar o `volume delete` comando para excluir um volume criptografado.

Antes de começar

- Você deve ser um administrador de cluster para executar esta tarefa. Como alternativa, você pode ser um administrador SVM a quem o administrador do cluster delegou autoridade. Para obter mais informações, "delegar autoridade para executar o comando de movimentação de volume"consulte .

- O volume deve estar offline.

Passo

1. Eliminar um volume encriptado:

   `volume delete -vserver` *`SVM_name`* `-volume` *`volume_name`*

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

   O comando a seguir exclui um volume criptografado chamado `vol1`:

   ```
   cluster1::> volume delete -vserver vs1 -volume vol1
   ```

   Digite `yes` quando for solicitado que você confirme a exclusão.

   O sistema exclui a chave de criptografia do volume após 24 horas.

   Use `volume delete` com a `-force true` opção para excluir um volume e destruir a chave de criptografia correspondente imediatamente. Este comando requer Privileges avançado. Para obter mais informações, consulte a página de manual.

Depois de terminar

Você pode usar o `volume recovery-queue` comando para recuperar um volume excluído durante o período de retenção após a emissão do `volume delete` comando:

`volume recovery-queue` *`SVM_name`* `-volume` *`volume_name`*

"Como usar o recurso recuperação de volume"

Limpe os dados com segurança em um volume criptografado

Limpe os dados com segurança em uma visão geral de volume criptografado

A partir do ONTAP 9.4, você usa a limpeza segura para limpeza de dados em volumes habilitados para NVE sem interrupções. A análise de dados em um volume criptografado garante que ele não possa ser recuperado da Mídia física, por exemplo, em casos de "spillage", onde os rastreamentos de dados podem ter sido deixados para trás quando os blocos foram substituídos, ou para excluir com segurança os dados de um locatário em vazio.

A limpeza segura funciona apenas para arquivos excluídos anteriormente em volumes habilitados para NVE. Não é possível limpar um volume não criptografado. Você precisa usar servidores KMIP para fornecer chaves, não o gerenciador de chaves integrado.

Considerações sobre a utilização de uma purga segura

- Os volumes criados em um agregado habilitado para NetApp Aggregate Encryption (NAE) não oferecem suporte à limpeza segura.
- A limpeza segura funciona apenas para arquivos excluídos anteriormente em volumes habilitados para

NVE.

- Não é possível limpar um volume não criptografado.
- Você precisa usar servidores KMIP para fornecer chaves, não o gerenciador de chaves integrado.

A limpeza segura funciona de forma diferente, dependendo da sua versão do ONTAP.

ONTAP 9 F.8 e mais tarde

- A purga segura é suportada pelo MetroCluster e pelo FlexGroup.
- Se o volume a ser purgado for a origem de uma relação SnapMirror, não é necessário interromper a relação SnapMirror para executar uma limpeza segura.
- O método de recriptografia é diferente para volumes que usam a proteção de dados do SnapMirror em vez de volumes que não usam a proteção de dados do SnapMirror (DP) ou aqueles que usam a proteção de dados estendida do SnapMirror.
  - Por padrão, os volumes que usam o modo de proteção de dados SnapMirror (DP) recriptografam os dados usando o método de recriptografia de movimentação de volume.
  - Por padrão, os volumes que não usam a proteção de dados SnapMirror ou volumes que usam o modo SnapMirror Extended Data Protection (XDP) usam o método de recriptografia no local.
  - Esses padrões podem ser alterados usando o `secure purge re-encryption-method [volume-move|in-place-rekey]` comando.
- Por padrão, todas as cópias Snapshot nos volumes FlexVol são automaticamente excluídas durante a operação de limpeza segura. Por padrão, os snapshots em volumes e volumes do FlexGroup que usam a proteção de dados do SnapMirror não são excluídos automaticamente durante a operação de limpeza segura. Esses padrões podem ser alterados usando o `secure purge delete-all-snapshots [true|false]` comando.

ONTAP 9.7 e anteriores:

- A purga segura não suporta o seguinte:
  - FlexClone
  - SnapVault
  - FabricPool
- Se o volume que está sendo purgado for a origem de uma relação do SnapMirror, você deve quebrar a relação do SnapMirror antes de poder limpar o volume.

  Se houver cópias snapshot ocupadas no volume, você precisará liberar as cópias Snapshot para poder limpar o volume. Por exemplo, talvez seja necessário dividir um volume FlexClone de seu pai.

- Chamar com êxito o recurso de limpeza segura aciona uma movimentação de volume que recriptografa os dados restantes e não limpos com uma nova chave.

  O volume movido permanece no agregado atual. A chave antiga é destruída automaticamente, garantindo que os dados purgados não possam ser recuperados da Mídia de armazenamento.

Limpe os dados com segurança em um volume criptografado sem uma relação com o SnapMirror

A partir do ONTAP 9.4, você pode usar a limpeza segura para dados "crostas" sem interrupções em volumes habilitados para NVE.

Sobre esta tarefa

A limpeza segura pode levar de vários minutos a muitas horas para ser concluída, dependendo da quantidade de dados nos arquivos excluídos. Pode utilizar o `volume encryption secure-purge show` comando para visualizar o estado da operação. Você pode usar o `volume encryption secure-purge abort` comando para encerrar a operação.

> Para fazer uma limpeza segura em um host SAN, você deve excluir todo o LUN que contém os arquivos que deseja limpar, ou você deve ser capaz de perfurar buracos no LUN para os blocos que pertencem aos arquivos que deseja limpar. Se você não puder excluir o LUN ou o sistema operacional do host não suportar furos no LUN, não será possível executar uma limpeza segura.

Antes de começar

- Você deve ser um administrador de cluster para executar esta tarefa.
- São necessários Privileges avançados para esta tarefa.

Passos

1. Exclua os arquivos ou o LUN que você deseja limpar com segurança.
   - Em um cliente nas, exclua os arquivos que você deseja limpar com segurança.
   - Em um host SAN, exclua o LUN que você deseja limpar com segurança ou perfurar buracos no LUN para os blocos que pertencem aos arquivos que deseja limpar.
2. No sistema de armazenamento, altere para nível de privilégio avançado:

   ```
   set -privilege advanced
   ```

3. Se os arquivos que você deseja limpar com segurança estiverem em snapshots, exclua os snapshots:

   ```
   snapshot delete -vserver SVM_name -volume volume_name -snapshot
   ```

4. Limpe com segurança os arquivos excluídos:

   ```
   volume encryption secure-purge start -vserver SVM_name -volume volume_name
   ```

   O comando a seguir limpa com segurança os arquivos excluídos `vol1` no SVM`vs1`:

   ```
   cluster1::> volume encryption secure-purge start -vserver vs1 -volume
   vol1
   ```

5. Verifique o estado da operação de purga segura:

   ```
   volume encryption secure-purge show
   ```

Limpe com segurança os dados em um volume criptografado com uma relação assíncrona do SnapMirror

A partir do ONTAP 9.8, você pode usar uma limpeza segura para dados "cruzadores" sem interrupções em volumes habilitados para NVE com uma relação assíncrona do SnapMirror.

Antes de começar

- Você deve ser um administrador de cluster para executar esta tarefa.
- São necessários Privileges avançados para esta tarefa.

Sobre esta tarefa

A limpeza segura pode levar de vários minutos a muitas horas para ser concluída, dependendo da quantidade de dados nos arquivos excluídos. Pode utilizar o `volume encryption secure-purge show` comando para visualizar o estado da operação. Você pode usar o `volume encryption secure-purge abort` comando para encerrar a operação.

> Para fazer uma limpeza segura em um host SAN, você deve excluir todo o LUN que contém os arquivos que deseja limpar, ou você deve ser capaz de perfurar buracos no LUN para os blocos que pertencem aos arquivos que deseja limpar. Se você não puder excluir o LUN ou o sistema operacional do host não suportar furos no LUN, não será possível executar uma limpeza segura.

Passos

1. No sistema de armazenamento, mude para o nível de privilégio avançado:

   ```
   set -privilege advanced
   ```

2. Exclua os arquivos ou o LUN que você deseja limpar com segurança.
   - Em um cliente nas, exclua os arquivos que você deseja limpar com segurança.
   - Em um host SAN, exclua o LUN que você deseja limpar com segurança ou perfurar buracos no LUN para os blocos que pertencem aos arquivos que deseja limpar.
3. Prepare o volume de destino na relação assíncrona para ser purgado com segurança:

   ```
   volume encryption secure-purge start -vserver SVM_name -volume volume_name
   -prepare true
   ```

   Repita esta etapa em cada volume em sua relação assíncrona do SnapMirror.

4. Se os arquivos que você deseja limpar com segurança estiverem em cópias Snapshot, exclua as cópias Snapshot:

   ```
   snapshot delete -vserver SVM_name -volume volume_name -snapshot
   ```

5. Se os arquivos que você deseja limpar com segurança estiverem nas cópias Snapshot base, faça o seguinte:

   a. Crie uma cópia Snapshot no volume de destino na relação assíncrona do SnapMirror:

      ```
      volume snapshot create -snapshot snapshot_name -vserver SVM_name -volume
      volume_name
      ```

   b. Atualize o SnapMirror para mover a cópia Snapshot base para frente:

      ```
      snapmirror update -source-snapshot snapshot_name -destination-path
      destination_path
      ```

   Repita esta etapa para cada volume na relação assíncrona do SnapMirror.

a. Repita as etapas (a) e (b) iguais ao número de cópias Snapshot base mais uma.

   Por exemplo, se você tiver duas cópias Snapshot básicas, repita as etapas (a) e (b) três vezes.

b. Verifique se a cópia Snapshot base está presente
   `snapshot show -vserver SVM_name -volume volume_name`

c. Eliminar a cópia Snapshot base
   `snapshot delete -vserver svm_name -volume volume_name -snapshot snapshot`

6. Limpe com segurança os arquivos excluídos:

   `volume encryption secure-purge start -vserver svm_name -volume volume_name`

   Repita esta etapa em cada volume na relação assíncrona do SnapMirror.

   O seguinte comando limpa com segurança os arquivos excluídos no "'vol1" na SVM "'VS1":

```
cluster1::> volume encryption secure-purge start -vserver vs1 -volume
vol1
```

7. Verifique o estado da operação de purga segura:

   `volume encryption secure-purge show`

Limpeza de dados em um volume criptografado com uma relação síncrona SnapMirror

A partir do ONTAP 9.8, você pode usar uma limpeza segura para "limpar" dados em volumes habilitados para NVE sem interrupções, com uma relação síncrona SnapMirror.

Sobre esta tarefa

Uma limpeza segura pode levar de vários minutos a muitas horas para ser concluída, dependendo da quantidade de dados nos arquivos excluídos. Pode utilizar o `volume encryption secure-purge show` comando para visualizar o estado da operação. Você pode usar o `volume encryption secure-purge abort` comando para encerrar a operação.

> Para fazer uma limpeza segura em um host SAN, você deve excluir todo o LUN que contém os arquivos que deseja limpar, ou você deve ser capaz de perfurar buracos no LUN para os blocos que pertencem aos arquivos que deseja limpar. Se você não puder excluir o LUN ou o sistema operacional do host não suportar furos no LUN, não será possível executar uma limpeza segura.

Antes de começar

- Você deve ser um administrador de cluster para executar esta tarefa.
- São necessários Privileges avançados para esta tarefa.

Passos

1. No sistema de armazenamento, altere para nível de privilégio avançado:

   `set -privilege advanced`

2. Exclua os arquivos ou o LUN que você deseja limpar com segurança.
   - Em um cliente nas, exclua os arquivos que você deseja limpar com segurança.
   - Em um host SAN, exclua o LUN que você deseja limpar com segurança ou perfurar buracos no LUN para os blocos que pertencem aos arquivos que deseja limpar.
3. Prepare o volume de destino na relação assíncrona para ser purgado com segurança:

   ```
   volume encryption secure-purge start -vserver <SVM_name> -volume <volume_name>
   -prepare true
   ```

   Repita esta etapa para o outro volume em sua relação síncrona do SnapMirror.

4. Se os arquivos que você deseja limpar com segurança estiverem em cópias Snapshot, exclua as cópias Snapshot:

   ```
   snapshot delete -vserver <SVM_name> -volume <volume_name> -snapshot <snapshot>
   ```

5. Se o arquivo de limpeza segura estiver na base ou nas cópias Snapshot comuns, atualize o SnapMirror para mover a cópia Snapshot comum para frente:

   ```
   snapmirror update -source-snapshot <snapshot_name> -destination-path
   <destination_path>
   ```

   Há duas cópias Snapshot comuns, portanto, esse comando deve ser emitido duas vezes.

6. Se o arquivo de limpeza segura estiver na cópia Snapshot consistente com o aplicativo, exclua a cópia Snapshot em ambos os volumes na relação síncrona do SnapMirror:

   ```
   snapshot delete -vserver <SVM_name> -volume <volume_name> -snapshot <snapshot>
   ```

   Execute esta etapa em ambos os volumes.

7. Limpe com segurança os arquivos excluídos:

   ```
   volume encryption secure-purge start -vserver <SVM_name> -volume <volume_name>
   ```

   Repita esta etapa em cada volume na relação síncrona do SnapMirror.

   O comando a seguir limpa com segurança os arquivos excluídos no "'vol1" no SVM "'VS1".

   ```
   cluster1::> volume encryption secure-purge start -vserver vs1 -volume
   vol1
   ```

8. Verifique o estado da operação de purga segura:

   ```
   volume encryption secure-purge show
   ```

Altere a senha de gerenciamento de chave integrada

É uma prática recomendada de segurança alterar periodicamente a senha de gerenciamento de chaves integradas. Copie a nova senha de gerenciamento de chaves

integrada para um local seguro fora do sistema de storage para uso futuro.

Antes de começar

- Você deve ser um administrador de cluster ou SVM para executar essa tarefa.
- São necessários Privileges avançados para esta tarefa.

Passos

1. Alterar para nível de privilégio avançado:

   ```
   set -privilege advanced
   ```

2. Altere a senha de gerenciamento de chaves integradas:

Para esta versão ONTAP…	Use este comando…
ONTAP 9 F.6 e mais tarde	`security key-manager onboard update-passphrase`
ONTAP 9 F.5 e anteriores	`security key-manager update-passphrase`

   Para obter a sintaxe completa do comando, consulte as páginas man.

   O seguinte comando ONTAP 9.6 permite alterar a senha de gerenciamento de chaves integradas para `cluster1`:

   ```
   clusterl::> security key-manager onboard update-passphrase
   Warning: This command will reconfigure the cluster passphrase for
   onboard key management for Vserver "cluster1".
   Do you want to continue? {y|n}: y
   Enter current passphrase:
   Enter new passphrase:
   ```

3. Digite `y` no prompt para alterar a senha de gerenciamento de chave integrada.
4. Introduza a frase-passe atual no prompt da frase-passe atual.
5. No novo prompt de senha, insira uma senha entre 32 e 256 carateres ou, para "cc-mode", uma senha entre 64 e 256 carateres.

   Se a senha "'cc-mode'" especificada for inferior a 64 carateres, haverá um atraso de cinco segundos antes que a operação de configuração do gerenciador de chaves exiba o prompt de senha novamente.

6. No prompt de confirmação da senha, redigite a senha.

Depois de terminar

Em um ambiente MetroCluster, você deve atualizar a senha no cluster de parceiros:

- No ONTAP 9.5 e versões anteriores, é necessário executar `security key-manager update-`

`passphrase` com a mesma senha no cluster de parceiros.

- No ONTAP 9.6 e posterior, você será solicitado a executar `security key-manager onboard sync` com a mesma senha no cluster de parceiros.

Copie a senha de gerenciamento de chaves integrada para um local seguro fora do sistema de storage para uso futuro.

Você deve fazer backup manual das informações de gerenciamento de chaves sempre que alterar a senha de gerenciamento de chaves integradas.

"Fazer backup manual de informações de gerenciamento de chaves integradas"

Faça backup manual das informações de gerenciamento de chaves integradas

Você deve copiar as informações de gerenciamento de chaves integradas para um local seguro fora do sistema de armazenamento sempre que configurar a senha do Gerenciador de chaves integrado.

O que você vai precisar

- Você deve ser um administrador de cluster para executar esta tarefa.
- São necessários Privileges avançados para esta tarefa.

Sobre esta tarefa

Todas as informações de gerenciamento de chaves são automaticamente armazenadas no banco de dados replicado (RDB) para o cluster. Você também deve fazer backup manual das informações de gerenciamento de chaves para uso em caso de desastre.

Passos

1. Alterar para nível de privilégio avançado:

   ```
   set -privilege advanced
   ```

2. Apresentar as informações de cópia de segurança da gestão de chaves para o cluster:

Para esta versão ONTAP…	Use este comando…
ONTAP 9 F.6 e mais tarde	`security key-manager onboard show-backup`
ONTAP 9 F.5 e anteriores	`security key-manager backup show`

Para obter a sintaxe completa do comando, consulte as páginas man.

O seguinte comando 9,6 exibe as informações de backup de gerenciamento de chaves `cluster1` para :

E

```
cluster1::> security key-manager onboard show-backup

      -------------------------BEGIN BACKUP-------------------------
      TmV0QXBwIEtleSBCbG9iAAEAAAAEAAAAcAEAAAAAADuD+byAAAAACEAAAAAAAAA
      QAAAAAAAAABvOlH0AAAAAMh7qDLRyH1DBz12piVdy9ATSFMT0C0TlYFss4PDjTaV
      dzRYkLd1PhQLxAWJwOIyqSr8qY1SEBgm1IWgE5DLRqkiAAAAAAAAACgAAAAAAAAA
      3WTh7gAAAAAAAAAAAAAAAAIAAAAAAAgAZJEIWvdeHr5RCAvHGclo+wAAAAAAAAAA
      IgAAAAAAAAoAAAAAAAAAEOTcR0AAAAAAAAAAAAAAACAAAAAAAJAGr3tJA/LRzU
      QRHwv+1aWvAAAAAAAAAACQAAAAAAAAgAAAAAAAACdhTcvAAAAAJ1PXeBfml4N
      BsSyV1B4jc4A7cvWEFY6lLG6hc6tbKLAHZuvfQ4rIbYAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABOZXRBcHAgS2V5IEJsb2IA
      AQAAAAMAAAAYAQAAAAAADA5/ccAAAAAIgAAAAAAAAAoAAAAAAAAAEOTcR0AAAAA
      AAAAAAAAAAACAAAAAAAJAGr3tJA/LRzUQRHwv+1aWvAAAAAAAAAAACIAAAAAAAAA
      KAAAAAAAAACI8z/bAAAAAAAAAAAAAAAAAgAAAAAAAQAbxMcI4qiaMS4Uts5tTUnU
      AAAAAAAAAAAkAAAAAAAAAIAAAAAAAAAAqwxTcwAAAACkiwBAI3YeeV3jMFg5Smyj
      LSgoK/qc8FAmMMcrRXY6uriulnL0WPB/AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAAAAAAAAAAAAE5ldEFwcCBLZXkgQmxvYgABAAAAAwAAABgBAAAAAAAA
      1cNLLwAAAAiAAAAAAAAACgAAAAAAAAQ5NxHQAAAAAAAAAAAAAAAIAAAAAAAkA
      ave0kD8tHNRBEfC/7Vpa8AAAAAAAAAAIgAAAAAAAAoAAAAAAAAAJ4/cQsAAAAA
      AAAAAAAAAAACAAAAAAABAF6JCZch+IF+ZeOutovhv8oAAAAAAAAAACQAAAAAAAA
      gAAAAAAAAAN3Zq7AAAAALO7qD20+H8TuGgSauEHoqAyWcLv4uA0m2rrH4nPQM0n
      rDRYRa9SCv8AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      -------------------------END BACKUP-------------------------
```

1. Copie as informações de backup para um local seguro fora do sistema de armazenamento para uso em caso de desastre.

Restaurar chaves de criptografia integradas de gerenciamento de chaves

O procedimento a seguir para restaurar as chaves de criptografia integradas de gerenciamento de chaves varia de acordo com a versão do ONTAP.

Antes de começar

- Se você estiver usando o NSE com um servidor de gerenciamento de chaves externas (KMIP), exclua o banco de dados do gerenciador de chaves externo. Para obter mais informações, consulte "transição para o gerenciamento de chaves integrado do gerenciamento de chaves externas"

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

Se você estiver usando o NSE em um sistema com um módulo Flash Cache, também deverá ativar o NVE ou NAE. O NSE não criptografa dados que residem no módulo Flash Cache.

ONTAP 9 F.6 e mais tarde

Se você estiver executando o ONTAP 9.8 ou posterior e o volume raiz estiver criptografado, siga o procedimento para [ontap-9-8].

1. Verifique se a chave precisa ser restaurada
   `security key-manager key query -node node`
2. Restaurar a chave
   `security key-manager onboard sync`

   Para obter a sintaxe completa do comando, consulte as páginas man.

   O seguinte comando ONTAP 9.6 sincroniza as chaves na hierarquia de chaves integradas:

```
cluster1::> security key-manager onboard sync

Enter the cluster-wide passphrase for onboard key management in Vserver
"cluster1"::    <32..256 ASCII characters long text>
```

3. No prompt de frase-passe, insira a senha de gerenciamento de chave integrada para o cluster.

ONTAP 9.8 ou posterior com volume de raiz criptografado

Se você estiver executando o ONTAP 9.8 e posterior e seu volume raiz estiver criptografado, defina uma senha de recuperação de gerenciamento de chaves integrado com o menu de inicialização. Este processo também é necessário se você fizer uma substituição de Mídia de inicialização.

1. Inicialize o nó no menu de inicialização e selecione a opção `(10) Set onboard key management recovery secrets`.
2. Enter `y` para utilizar esta opção.
3. No prompt, insira a senha de gerenciamento de chaves integradas para o cluster.
4. No prompt, insira os dados da chave de backup.

   O nó retorna ao menu de inicialização.

5. No menu de inicialização, selecione a opção `(1) Normal Boot`.

ONTAP 9 F.5 e anteriores

1. Verifique se a chave precisa ser restaurada
   `security key-manager key show`
2. Se você estiver executando o ONTAP 9.8 e posterior e o volume raiz estiver criptografado, execute estas etapas:

Se você estiver executando o ONTAP 9.6 ou 9,7, ou se estiver executando o ONTAP 9.8 ou posterior e o volume raiz não estiver criptografado, pule esta etapa.

3. Restaurar a chave
   `security key-manager setup -node node`

   Para obter a sintaxe completa do comando, consulte as páginas man.

4. No prompt de frase-passe, insira a senha de gerenciamento de chave integrada para o cluster.

Restaurar chaves de criptografia de gerenciamento de chaves externas

Você pode restaurar manualmente as chaves de criptografia de gerenciamento de chaves externas e enviá-las para um nó diferente. Você pode querer fazer isso se estiver reiniciando um nó que estava inativo temporariamente quando criou as chaves para o cluster.

Sobre esta tarefa

No ONTAP 9.6 e posterior, você pode usar o `security key-manager key query -node node_name` comando para verificar se sua chave precisa ser restaurada.

No ONTAP 9.5 e anteriores, você pode usar o `security key-manager key show` comando para verificar se sua chave precisa ser restaurada.

> Se você estiver usando o NSE em um sistema com um módulo Flash Cache, também deverá ativar o NVE ou NAE. O NSE não criptografa dados que residem no módulo Flash Cache.

Antes de começar

Você deve ser um administrador de cluster ou SVM para executar essa tarefa.

Passos

1. Se você estiver executando o ONTAP 9.8 ou posterior e o volume raiz estiver criptografado, faça o seguinte:

   Se você estiver executando o ONTAP 9.7 ou anterior, ou se estiver executando o ONTAP 9.8 ou posterior e o volume raiz não estiver criptografado, pule esta etapa.

   a. Defina os bototargs
      ```
      setenv kmip.init.ipaddr <ip-address>
      setenv kmip.init.netmask <netmask>
      setenv kmip.init.gateway <gateway>
      setenv kmip.init.interface e0M
      boot_ontap
      ```

   b. Inicialize o nó no menu de inicialização e selecione a opção `(11) Configure node for external key management.`

   c. Siga as instruções para inserir o certificado de gerenciamento.

      Depois que todas as informações do certificado de gerenciamento forem inseridas, o sistema retornará ao menu de inicialização.

d. No menu de inicialização, selecione a opção `(1) Normal Boot.`

2. Restaure a chave:

Para esta versão ONTAP…	Use este comando…
ONTAP 9 F.6 e mais tarde	`security key-manager external restore -vserver SVM -node node -key-server host_name
IP_address:port -key-id key_id -key -tag key_tag`	ONTAP 9 F.5 e anteriores

> `node` o padrão é todos os nós. Para obter a sintaxe completa do comando, consulte as páginas man. Este comando não é suportado quando o gerenciamento de chaves integradas está habilitado.

O seguinte comando ONTAP 9.6 restaura chaves de autenticação de gerenciamento de chaves externas para todos os nós no `cluster1`:

```
clusterl::> security key-manager external restore
```

Substitua os certificados SSL

Todos os certificados SSL têm uma data de validade. Você deve atualizar seus certificados antes que eles expirem para evitar a perda de acesso às chaves de autenticação.

Antes de começar

- Você precisa ter obtido o certificado público de substituição e a chave privada do cluster (certificado de cliente KMIP).
- Você deve ter obtido o certificado público de substituição para o servidor KMIP (certificado KMIP Server-CA).
- Você deve ser um administrador de cluster ou SVM para executar essa tarefa.
- Se você estiver substituindo os certificados SSL KMIP em um ambiente MetroCluster, instale o mesmo certificado SSL KMIP de substituição em ambos os clusters.

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

Passos

1. Instale o novo certificado KMIP Server-CA:

   ```
   security certificate install -type server-ca -vserver <>
   ```

2. Instale o novo certificado de cliente KMIP:

   ```
   security certificate install -type client -vserver <>
   ```

3. Atualize a configuração do gerenciador de chaves para usar os certificados recém-instalados:

   ```
   security key-manager external modify -vserver <> -client-cert <> -server-ca
   -certs <>
   ```

   Se você estiver executando o ONTAP 9.6 ou posterior em um ambiente MetroCluster e quiser modificar a configuração do gerenciador de chaves no SVM admin, execute o comando nos dois clusters na configuração.

> Atualizar a configuração do gerenciador de chaves para usar os certificados recém-instalados retornará um erro se as chaves públicas/privadas do novo certificado de cliente forem diferentes das chaves instaladas anteriormente. Consulte o artigo da base de dados de Conhecimento "As novas chaves públicas ou privadas do certificado de cliente são diferentes do certificado de cliente existente"para obter instruções sobre como substituir este erro.

Substitua uma unidade FIPS ou SED

Você pode substituir uma unidade FIPS ou SED da mesma forma que substitui um disco comum. Certifique-se de atribuir novas chaves de autenticação de dados à unidade de substituição. Para uma unidade FIPS, você também pode querer atribuir uma nova chave de autenticação FIPS 140-2-2.

> Se um par de HA estiver usando "Criptografia de unidades SAS ou NVMe (SED, NSE, FIPS)", siga as instruções no "Retornar uma unidade FIPS ou SED para o modo desprotegido"tópico para todas as unidades do par de HA antes de inicializar o sistema (opções de inicialização 4 ou 9). Se não fizer isso, poderá resultar em perda de dados futura se as unidades forem reaproveitadas.

Antes de começar

- Você deve saber o ID da chave para a chave de autenticação usada pela unidade.
- Você deve ser um administrador de cluster para executar esta tarefa.

Passos

1. Certifique-se de que o disco foi marcado como com falha:

   ```
   storage disk show -broken
   ```

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

```
cluster1::> storage disk show -broken
Original Owner: cluster1-01
  Checksum Compatibility: block
                                                                    Usable
Physical
    Disk   Outage Reason HA Shelf Bay Chan   Pool  Type    RPM     Size
Size
    ------ ---- ------------ ---- --- ---- ------ -----  -----  -------
-------
    0.0.0  admin  failed  0b    1   0    A  Pool0  FCAL  10000  132.8GB
133.9GB
    0.0.7  admin  removed 0b    2   6    A  Pool1  FCAL  10000  132.8GB
134.2GB
[...]
```

2. Remova o disco com falha e substitua-o por uma nova unidade FIPS ou SED, seguindo as instruções no guia de hardware do modelo de compartimento de disco.
3. Atribua a propriedade do disco recém-substituído:

   `storage disk assign -disk disk_name -owner node`

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

   ```
   cluster1::> storage disk assign -disk 2.1.1 -owner cluster1-01
   ```

4. Confirme se o novo disco foi atribuído:

   `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
1.10.0  data
F1CB30AFF1CB30B00101000000000000CF0EFD81EA9F6324EA97B369351C56AC
1.10.1  data
F1CB30AFF1CB30B00101000000000000CF0EFD81EA9F6324EA97B369351C56AC
2.1.1   open 0x0
[...]
```

5. Atribua as chaves de autenticação de dados à unidade FIPS ou SED.

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

6. Se necessário, atribua uma chave de autenticação FIPS 140-2-2 à unidade FIPS.

   "Atribuição de uma chave de autenticação FIPS 140-2-2 a uma unidade FIPS"

Tornar os dados em uma unidade FIPS ou SED inacessíveis

Torne os dados em uma unidade FIPS ou visão geral do SED inacessíveis

Se você quiser tornar os dados em uma unidade FIPS ou SED permanentemente inacessíveis, mas manter o espaço não utilizado da unidade disponível para novos dados, você pode higienizar o disco. Se você quiser tornar os dados permanentemente inacessíveis e você não precisa reutilizar a unidade, você pode destruí-la.

- Sanitização de disco

  Quando você limpa uma unidade de autocriptografia, o sistema altera a chave de criptografia de disco para um novo valor aleatório, redefine o estado de bloqueio de inicialização para falso e define o ID da chave para um valor padrão, seja a ID segura do fabricante 0x0 (unidades SAS) ou uma chave nula (unidades NVMe). Isso torna os dados no disco inacessíveis e impossível de recuperar. Você pode reutilizar discos higienizados como discos sobressalentes não zerados.

- Destruição de disco

  Quando você destrói uma unidade FIPS ou SED, o sistema define a chave de criptografia de disco para um valor aleatório desconhecido e bloqueia o disco irreversivelmente. Isso torna o disco permanentemente inutilizável e os dados nele permanentemente inacessíveis.

Você pode higienizar ou destruir unidades de autocriptografia individuais ou todas as unidades de autocriptografia de um nó.

Higienize uma unidade FIPS ou SED

Se você quiser tornar os dados em uma unidade FIPS ou SED permanentemente inacessíveis e usar a unidade para novos dados, use o `storage encryption disk sanitize` comando para higienizar a unidade.

Sobre esta tarefa

Quando você limpa uma unidade de autocriptografia, o sistema altera a chave de criptografia de disco para um novo valor aleatório, redefine o estado de bloqueio de inicialização para falso e define o ID da chave para um valor padrão, seja a ID segura do fabricante 0x0 (unidades SAS) ou uma chave nula (unidades NVMe). Isso torna os dados no disco inacessíveis e impossível de recuperar. Você pode reutilizar discos higienizados como discos sobressalentes não zerados.

Antes de começar

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

Passos

1. Migre qualquer dado que precise ser preservado para um agregado em outro disco.
2. Exclua o agregado na unidade FIPS ou SED para ser higienizado:

   `storage aggregate delete -aggregate` *`aggregate_name`*

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

   ```
   cluster1::> storage aggregate delete -aggregate aggr1
   ```

3. Identifique a ID do disco para a unidade FIPS ou SED a ser higienizada:

   `storage encryption disk show -fields data-key-id,fips-key-id,owner`

   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
   1.10.2  data
   F1CB30AFF1CB30B00101000000000000CF0EFD81EA9F6324EA97B369351C56AC
   [...]
   ```

4. Se uma unidade FIPS estiver em execução no modo de conformidade com FIPS, defina o ID da chave de autenticação FIPS para o nó novamente para o MSID padrão 0x0:

```
storage encryption disk modify -disk disk_id -fips-key-id 0x0
```

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

```
cluster1::> storage encryption disk modify -disk 1.10.2 -fips-key-id 0x0

Info: Starting modify on 1 disk.
      View the status of the operation by using the
      storage encryption disk show-status command.
```

5. Higienize a unidade:

```
storage encryption disk sanitize -disk disk_id
```

Você pode usar este comando para higienizar discos hot spare ou quebrados somente. Para higienizar todos os discos independentemente do tipo, use a `-force-all-state` opção. Para obter a sintaxe completa do comando, consulte a página man.

> O ONTAP solicitará que você insira uma frase de confirmação antes de continuar. Insira a frase exatamente como mostrado na tela.

```
cluster1::> storage encryption disk sanitize -disk 1.10.2

Warning: This operation will cryptographically sanitize 1 spare or
broken self-encrypting disk on 1 node.
         To continue, enter sanitize disk: sanitize disk

Info: Starting sanitize on 1 disk.
      View the status of the operation using the
      storage encryption disk show-status command.
```

6. Desfalhe o disco higienizado:
`storage disk unfail -spare true -disk disk_id`
7. Verifique se o disco tem um proprietário:
`storage disk show -disk disk_id` Se o disco não tem um proprietário, atribua um.
`storage disk assign -owner node -disk disk_id`
8. Introduza o nodeshell para o nó que possui os discos que pretende higienizar:

```
system node run -node node_name
```

Executar o `disk sanitize release` comando.

9. Saia do nodeshell. Desfalhe o disco novamente:
`storage disk unfail -spare true -disk disk_id`
10. Verifique se o disco agora está sobressalente e pronto para ser reutilizado em um agregado:
`storage disk show -disk disk_id`

Destrua uma unidade FIPS ou SED

Se você quiser tornar os dados em uma unidade FIPS ou SED permanentemente inacessíveis e não precisar reutilizar a unidade, use o `storage encryption disk destroy` comando para destruir o disco.

Sobre esta tarefa

Quando você destrói uma unidade FIPS ou SED, o sistema define a chave de criptografia de disco para um valor aleatório desconhecido e bloqueia a unidade irreversivelmente. Isso torna o disco praticamente inutilizável e os dados nele permanentemente inacessíveis. No entanto, você pode redefinir o disco para suas configurações configuradas de fábrica usando a ID física segura (PSID) impressa na etiqueta do disco. Para obter mais informações, "Retornar uma unidade FIPS ou SED ao serviço quando as chaves de autenticação são perdidas"consulte .

> Você não deve destruir uma unidade FIPS ou SED, a menos que tenha o serviço Non-Returnable Disk Plus (NRD Plus). Destruir um disco anula sua garantia.

Antes de começar

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

Passos

1. Migre qualquer dado que precise ser preservado para um agregado em outro disco diferente.
2. Exclua o agregado na unidade FIPS ou SED a ser destruído:

   `storage aggregate delete -aggregate aggregate_name`

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

   ```
   cluster1::> storage aggregate delete -aggregate aggr1
   ```

3. Identifique a ID do disco para a unidade FIPS ou SED a ser destruída:

   `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
   1.10.2  data
   F1CB30AFF1CB30B00101000000000000CF0EFD81EA9F6324EA97B369351C56AC
   [...]
   ```

4. Destrua o disco:

   ```
   storage encryption disk destroy -disk disk_id
   ```

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

   > É-lhe pedido que introduza uma frase de confirmação antes de continuar. Insira a frase exatamente como mostrado na tela.

   ```
   cluster1::> storage encryption disk destroy -disk 1.10.2

   Warning: This operation will cryptographically destroy 1 spare or broken
            self-encrypting disks on 1 node.
            You cannot reuse destroyed disks unless you revert
            them to their original state using the PSID value.
            To continue, enter
             destroy disk
            :destroy disk

   Info: Starting destroy on 1 disk.
         View the status of the operation by using the
         "storage encryption disk show-status" command.
   ```

Dados de emergência cortados em uma unidade FIPS ou SED

Em caso de emergência de segurança, você pode impedir instantaneamente o acesso a uma unidade FIPS ou SED, mesmo que a energia não esteja disponível para o sistema de armazenamento ou para o servidor KMIP.

Antes de começar

- Se você estiver usando um servidor KMIP que não tem energia disponível, o servidor KMIP deve ser configurado com um item de autenticação facilmente destruído (por exemplo, um smart card ou unidade USB).
- Você deve ser um administrador de cluster para executar esta tarefa.

Passo

1. Execute a fragmentação de emergência de dados em uma unidade FIPS ou SED:

Se…	Então…

A energia está disponível para o sistema de armazenamento e você tem tempo para colocar o sistema de armazenamento offline graciosamente	a. Se o sistema de storage estiver configurado como um par de HA, desative o takeover. b. Tire todos os agregados off-line e exclua-os. c. Defina o nível de privilégio como avançado `set -privilege advanced` d. Se a unidade estiver no modo de conformidade FIPS, defina o ID da chave de autenticação FIPS para o nó de volta para o MSID padrão `storage encryption disk modify -disk * -fips-key-id 0x0` e. Parar o sistema de storage. f. Arranque no modo de manutenção. g. Sanitize ou destrua os discos: ◦ Se você quiser tornar os dados nos discos inacessíveis e ainda conseguir reutilizar os discos, limpe os discos `disk encrypt sanitize -all` ◦ Se você quiser tornar os dados nos discos inacessíveis e você não precisa salvar os discos, destrua os discos `disk encrypt destroy disk_id1 disk_id2 …`	A energia está disponível para o sistema de armazenamento e você deve destruir os dados imediatamente

a. **Se você quiser tornar os dados nos discos inacessíveis e ainda conseguir reutilizar os discos, higienize os discos:**
b. Se o sistema de storage estiver configurado como um par de HA, desative o takeover.
c. Defina o nível de privilégio como avançado:
`set -privilege advanced`
d. Se a unidade estiver no modo de conformidade FIPS, defina o ID da chave de autenticação FIPS para o nó de volta para o MSID padrão:
`storage encryption disk modify -disk * -fips-key-id 0x0`
e. Higienizar o disco:
`storage encryption disk sanitize -disk * -force-all-states true`
	a. **Se você quiser tornar os dados nos discos inacessíveis e não precisar salvar os discos, destrua os discos:**
	b. Se o sistema de storage estiver configurado como um par de HA, desative o takeover.
	c. Defina o nível de privilégio como avançado:
	`set -privilege advanced`
	d. Destrua os discos:
	`storage encryption disk destroy -disk * -force-all-states true`
		O sistema de armazenamento entra em pânico, deixando o sistema em um estado permanentemente desativado com todos os dados apagados. Para utilizar novamente o sistema, tem de o reconfigurar.

A energia está disponível para o servidor KMIP, mas não para o sistema de storage	a. Faça login no servidor KMIP. b. Destrua todas as chaves associadas às unidades FIPS ou SEDs que contenham os dados aos quais você deseja impedir o acesso. Isso impede o acesso a chaves de criptografia de disco pelo sistema de armazenamento.	A energia não está disponível para o servidor KMIP nem para o sistema de storage

Para obter a sintaxe completa do comando, consulte as páginas man.

Retorne uma unidade FIPS ou SED ao serviço usando o ONTAP quando as chaves de autenticação forem perdidas

O sistema trata uma unidade FIPS ou SED como quebrado se você perder as chaves de autenticação permanentemente e não conseguir recuperá-las do servidor KMIP. Embora você não possa acessar ou recuperar os dados no disco, você pode tomar medidas para

tornar o espaço não utilizado do SED disponível novamente para os dados.

Antes de começar

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

Sobre esta tarefa

Deve utilizar este processo apenas se tiver a certeza de que as chaves de autenticação para a unidade FIPS ou SED estão permanentemente perdidas e que não pode recuperá-las.

Se os discos forem particionados, eles devem primeiro ser desparticionados antes de iniciar esse processo.

> O comando para desparticionar um disco só está disponível no nível de diag e só deve ser executado sob supervisão de suporte NetApp. **É altamente recomendável que você entre em Contato com o suporte da NetApp antes de prosseguir.** Você também pode consultar o artigo da base de dados de Conhecimento "Como desparticionar uma unidade sobressalente no ONTAP".

Passos

1. Retornar uma unidade FIPS ou SED à manutenção:

Se os SEDS são…	Siga estes passos…

Não está no modo de conformidade FIPS nem no modo de conformidade FIPS, e a chave FIPS está disponível	a. Defina o nível de privilégio como avançado:
	`set -privilege advanced`
	b. Reponha a chave FIPS para a ID segura de fabricação padrão 0x0:
	`storage encryption disk modify -fips-key-id 0x0 -disk disk_id`
	c. Verifique se a operação foi bem-sucedida:
	`storage encryption disk show-status` Se a operação falhou, use o processo PSID neste tópico.
	d. Sanitize o disco quebrado:
	`storage encryption disk sanitize -disk disk_id` Verifique se a operação foi bem-sucedida com o comando `storage encryption disk show-status` antes de prosseguir para a próxima etapa.
	e. Desfalhe o disco higienizado:
	`storage disk unfail -spare true -disk disk_id`
	f. Verifique se o disco tem um proprietário:
	`storage disk show -disk disk_id` Se o disco não tem um proprietário, atribua um.
	`storage disk assign -owner node -disk disk_id`
	i. Introduza o nodeshell para o nó que possui os discos que pretende higienizar:
	`system node run -node node_name`
	Executar o `disk sanitize release` comando.
	g. Saia do nodeshell. Desfalhe o disco novamente:
	`storage disk unfail -spare true -disk disk_id`
	h. Verifique se o disco agora está sobressalente e pronto para ser reutilizado em um agregado:
	`storage disk show -disk disk_id`

No modo de conformidade com o FIPS, a chave FIPS não está disponível e os SEDs têm um PSID impresso na etiqueta	a. Obtenha o PSID do disco a partir da etiqueta do disco. b. Defina o nível de privilégio como avançado: `set -privilege advanced` c. Redefina o disco para suas configurações configuradas de fábrica: `storage encryption disk revert-to-original-state -disk` *`disk_id`* `-psid` *`disk_physical_secure_id`* Verifique se a operação foi bem-sucedida com o comando `storage encryption disk show-status` antes de prosseguir para a próxima etapa. d. Se você estiver executando o ONTAP 9.8P5 ou anterior, vá para a próxima etapa. Se você estiver executando o ONTAP 9.8P6 ou posterior, desmarque o disco higienizado. `storage disk unfail -disk` *`disk_id`* e. Verifique se o disco tem um proprietário: `storage disk show -disk` *`disk_id`* Se o disco não tem um proprietário, atribua um. `storage disk assign -owner node -disk` *`disk_id`* i. Introduza o nodeshell para o nó que possui os discos que pretende higienizar: `system node run -node` *`node_name`* Executar o `disk sanitize release` comando. f. Saia do nodeshell.. Desfalhe o disco novamente: `storage disk unfail -spare true -disk` *`disk_id`* g. Verifique se o disco agora está sobressalente e pronto para ser reutilizado em um agregado: `storage disk show -disk` *`disk_id`*

Saiba mais sobre os comandos descritos neste procedimento no "Referência do comando ONTAP".

Retorne uma unidade FIPS ou SED para o modo desprotegido

Uma unidade FIPS ou SED é protegida contra acesso não autorizado somente se o ID da chave de autenticação para o nó estiver definido para um valor diferente do padrão. Você pode retornar uma unidade FIPS ou SED para o modo desprotegido usando o `storage encryption disk modify` comando para definir o ID da chave como padrão.

Se um par de HA estiver usando a criptografia de unidades SAS ou NVMe (SED, NSE, FIPS), siga este processo para todas as unidades dentro do par de HA antes de inicializar o sistema (opções de inicialização 4 ou 9). Se não fizer isso, poderá resultar em perda de dados futura se as unidades forem reaproveitadas.

Antes de começar

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

Passos

1. Defina o nível de privilégio como avançado:

   `set -privilege advanced`

2. Se uma unidade FIPS estiver em execução no modo de conformidade com FIPS, defina o ID da chave de autenticação FIPS para o nó novamente para o MSID padrão 0x0:

   `storage encryption disk modify -disk disk_id -fips-key-id 0x0`

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

   ```
   cluster1::> storage encryption disk modify -disk 2.10.11 -fips-key-id
   0x0

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

   Confirme a operação com sucesso com o comando:

   `storage encryption disk show-status`

   Repita o comando show-status até que os números em "discos iniciados" e "discos concluídos" sejam os mesmos.

   ```
   cluster1:: storage encryption disk show-status

               FIPS    Latest   Start               Execution   Disks
   Disks Disks
   Node        Support Request  Timestamp           Time (sec)  Begun
   Done  Successful
   -------     ------- -------- ------------------  ---------- ------
   ------  ----------
   cluster1    true    modify   1/18/2022 15:29:38    3           14     5
   5
   1 entry was displayed.
   ```

3. Defina o ID da chave de autenticação de dados para o nó de volta para o MSID padrão 0x0:

   `storage encryption disk modify -disk disk_id -data-key-id 0x0`

   O valor de `-data-key-id` deve ser definido como 0x0 se você estiver retornando uma unidade SAS ou NVMe para o modo desprotegido.

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

```
cluster1::> storage encryption disk modify -disk 2.10.11 -data-key-id
0x0

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

Confirme a operação com sucesso com o comando:

`storage encryption disk show-status`

Repita o comando show-status até que os números sejam os mesmos. A operação é concluída quando os números em "discos iniciados" e "discos concluídos" são os mesmos.

Modo de manutenção

Começando com ONTAP 9.7, você pode rechavear uma unidade FIPS a partir do modo de manutenção. Você só deve usar o modo de manutenção se não puder usar as instruções da CLI do ONTAP na seção anterior.

Passos

1. Defina o ID da chave de autenticação FIPS para o nó de volta para o MSID padrão 0x0:

   `disk encrypt rekey_fips 0x0 *disklist*`

2. Defina o ID da chave de autenticação de dados para o nó de volta para o MSID padrão 0x0:

   `disk encrypt rekey 0x0 *disklist*`

3. Confirme se a chave de autenticação FIPS foi rekeyed com êxito:

   `disk encrypt show_fips`

4. Confirmar chave de autenticação de dados foi rekeyed com sucesso com:

   `disk encrypt show`

   Sua saída provavelmente exibirá o ID de chave padrão MSID 0x0 ou o valor de 64 carateres mantido pelo servidor de chaves. O `Locked?` campo refere-se ao bloqueio de dados.

```
Disk       FIPS Key ID                 Locked?
---------- --------------------------- -------
0a.01.0    0x0                          Yes
```

Remova uma conexão externa do gerenciador de chaves

Você pode desconetar um servidor KMIP de um nó quando não precisar mais do servidor. Por exemplo, você pode desconetar um servidor KMIP quando estiver migrando

para a criptografia de volume.

Sobre esta tarefa

Ao desconetar um servidor KMIP de um nó em um par de HA, o sistema desconeta automaticamente o servidor de todos os nós de cluster.

> Se você pretende continuar usando o gerenciamento de chaves externas depois de desconetar um servidor KMIP, verifique se outro servidor KMIP está disponível para servir as chaves de autenticação.

Antes de começar

Você deve ser um administrador de cluster ou SVM para executar essa tarefa.

Passo

1. Desconete um servidor KMIP do nó atual:

Para esta versão ONTAP…	Use este comando…
ONTAP 9 F.6 e mais tarde	`security key-manager external remove-servers -vserver SVM -key -servers host_name
IP_address:port,…`	ONTAP 9 F.5 e anteriores

   Em um ambiente do MetroCluster, você deve repetir esses comandos nos dois clusters para o SVM de administrador.

   Para obter a sintaxe completa do comando, consulte as páginas man.

   O seguinte comando ONTAP 9.6 desativa as conexões a dois servidores de gerenciamento de chaves externas para `cluster1`, o primeiro chamado `ks1`, ouvindo na porta padrão 5696, o segundo com o endereço IP 10,0.0,20, ouvindo na porta 24482:

```
cluster1::> security key-manager external remove-servers -vserver
cluster-1 -key-servers ks1,10.0.0.20:24482
```

Modifique as propriedades do servidor de gerenciamento de chaves externas

A partir do ONTAP 9.6, você pode usar o `security key-manager external modify-server` comando para alterar o tempo limite de e/S e o nome de usuário de um servidor de gerenciamento de chaves externo.

Antes de começar

- Você deve ser um administrador de cluster ou SVM para executar essa tarefa.
- São necessários Privileges avançados para esta tarefa.
- Em um ambiente do MetroCluster, repita essas etapas nos dois clusters para o SVM de administrador.

Passos

1. No sistema de armazenamento, altere para nível de privilégio avançado:

   ```
   set -privilege advanced
   ```

2. Modifique as propriedades do servidor do gerenciador de chaves externo para o cluster:

   ```
   security key-manager external modify-server -vserver admin_SVM -key-server
   host_name|IP_address:port,… -timeout 1…60 -username user_name
   ```

   > O valor de tempo limite é expresso em segundos. Se você modificar o nome de usuário, será solicitado que você insira uma nova senha. Se você executar o comando no prompt de login do cluster, *admin_SVM* o padrão será o administrador SVM do cluster atual. Você deve ser o administrador do cluster para modificar as propriedades do servidor do gerenciador de chaves externo.

   O comando a seguir altera o valor de tempo limite para 45 segundos para que o `cluster1` servidor de gerenciamento de chaves externo esteja escutando na porta padrão 5696:

   ```
   cluster1::> security key-manager external modify-server -vserver
   cluster1 -key-server ks1.local -timeout 45
   ```

3. Modificar as propriedades do servidor do gerenciador de chaves externo para uma SVM (somente NVE):

   ```
   security key-manager external modify-server -vserver SVM -key-server
   host_name|IP_address:port,… -timeout 1…60 -username user_name
   ```

   > O valor de tempo limite é expresso em segundos. Se você modificar o nome de usuário, será solicitado que você insira uma nova senha. Se você executar o comando no prompt de login SVM, *SVM* o padrão será SVM atual. Você deve ser o administrador do cluster ou SVM para modificar as propriedades do servidor do gerenciador de chaves externo.

   O comando a seguir altera o nome de usuário e a senha do `svm1` servidor de gerenciamento de chaves externo ouvindo na porta padrão 5696:

   ```
   svm1::> security key-manager external modify-server -vserver svm11 -key
   -server ks1.local -username svm1user
   Enter the password:
   Reenter the password:
   ```

4. Repita a última etapa para quaisquer SVMs adicionais.

Transição para o gerenciamento de chaves externas do gerenciamento de chaves integrado

Se você quiser alternar para o gerenciamento de chaves externas do gerenciamento de chaves integradas, exclua a configuração de gerenciamento de chaves integradas antes de habilitar o gerenciamento de chaves externas.

Antes de começar

- Para criptografia baseada em hardware, é necessário redefinir as chaves de dados de todas as unidades FIPS ou SEDs para o valor padrão.

  "Retornar uma unidade FIPS ou SED para o modo desprotegido"

- Para criptografia baseada em software, você deve descriptografar todos os volumes.

  "Uncriptografando dados de volume"

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

Passo

1. Exclua a configuração de gerenciamento de chaves integradas para um cluster:

Para esta versão ONTAP…	Use este comando…
ONTAP 9 F.6 e mais tarde	`security key-manager onboard disable -vserver SVM`
ONTAP 9 F.5 e anteriores	`security key-manager delete-key-database`

Para obter a sintaxe de comando completa, consulte "Referência do comando ONTAP" .

Transição para o gerenciamento de chaves integrado do gerenciamento de chaves externas

Se você quiser alternar para o gerenciamento de chaves integradas do gerenciamento de chaves externas, exclua a configuração de gerenciamento de chaves externas para ativar o gerenciamento de chaves integradas.

Antes de começar

- Para criptografia baseada em hardware, é necessário redefinir as chaves de dados de todas as unidades FIPS ou SEDs para o valor padrão.

  "Retornar uma unidade FIPS ou SED para o modo desprotegido"

- Você deve ter excluído todas as conexões externas do gerenciador de chaves.

  "Excluindo uma conexão externa do gerenciador de chaves"

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

Procedimento

As etapas para fazer a transição do gerenciamento de chaves dependem da versão do ONTAP que você está usando.

ONTAP 9 F.6 e mais tarde

1. Mude para o nível de privilégio avançado:

   ```
   set -privilege advanced
   ```

2. Use o comando:

   ```
   security key-manager external disable -vserver admin_SVM
   ```

   Em um ambiente MetroCluster, você deve repetir o comando nos dois clusters para o SVM de administrador.

ONTAP 9 F.5 e anteriores

Use o comando:
`security key-manager delete-kmip-config`

O que acontece quando os servidores de gerenciamento de chaves não são alcançáveis durante o processo de inicialização

O ONTAP toma certas precauções para evitar um comportamento indesejado caso um sistema de armazenamento configurado para NSE não alcance nenhum dos servidores de gerenciamento de chaves especificados durante o processo de inicialização.

Se o sistema de armazenamento estiver configurado para NSE, os SEDs são rekeyed e locked e os SEDs são ligados, o sistema de armazenamento deve recuperar as chaves de autenticação necessárias dos servidores de gerenciamento de chaves para se autenticar nos SEDs antes de poder acessar os dados.

O sistema de armazenamento tenta contactar os servidores de gestão de chaves especificados durante até três horas. Se o sistema de armazenamento não puder alcançar nenhum deles depois desse tempo, o processo de inicialização será interrompido e o sistema de armazenamento será interrompido.

Se o sistema de armazenamento entrar em Contato com qualquer servidor de gerenciamento de chaves especificado, ele tentará estabelecer uma conexão SSL por até 15 minutos. Se o sistema de armazenamento não puder estabelecer uma conexão SSL com qualquer servidor de gerenciamento de chaves especificado, o processo de inicialização será interrompido e o sistema de armazenamento será interrompido.

Enquanto o sistema de armazenamento tenta entrar em Contato e se conetar a servidores de gerenciamento de chaves, ele exibe informações detalhadas sobre as tentativas de Contato com falha na CLI. Você pode interromper as tentativas de Contato a qualquer momento pressionando Ctrl-C.

Como medida de segurança, os SEDs permitem apenas um número limitado de tentativas de acesso não autorizado, após o qual desativam o acesso aos dados existentes. Se o sistema de armazenamento não puder contactar qualquer servidor de gestão de chaves especificado para obter as chaves de autenticação adequadas, só poderá tentar autenticar com a chave predefinida, o que leva a uma tentativa de falha e a um pânico. Se o sistema de armazenamento estiver configurado para reiniciar automaticamente em caso de pânico, ele entra em um loop de inicialização que resulta em tentativas de autenticação com falha contínua nos SEDs.

Parar o sistema de armazenamento nesses cenários é por projeto para impedir que o sistema de armazenamento entre em um loop de inicialização e possível perda não intencional de dados como resultado

dos SEDs bloqueados permanentemente devido a exceder o limite de segurança de um certo número de tentativas consecutivas de autenticação falhadas. O limite e o tipo de proteção de bloqueio dependem das especificações de fabricação e do tipo de SED:

Tipo de SED	Número de tentativas consecutivas falhadas de autenticação, resultando em bloqueio	Tipo de proteção de bloqueio quando o limite de segurança é atingido
HDD	1024	Permanente. Os dados não podem ser recuperados, mesmo quando a chave de autenticação adequada se torna disponível novamente.
X440_PHM2800MCTO 800GB SSDs NSE com revisões de firmware NA00 ou NA01	5	Temporário. O bloqueio só está em vigor até que o disco seja ligado a um ciclo de energia.
X577_PHM2800MCTO 800GB SSDs NSE com revisões de firmware NA00 ou NA01	5	Temporário. O bloqueio só está em vigor até que o disco seja ligado a um ciclo de energia.
X440_PHM2800MCTO 800GB SSDs NSE com revisões de firmware mais altas	1024	Permanente. Os dados não podem ser recuperados, mesmo quando a chave de autenticação adequada se torna disponível novamente.
X577_PHM2800MCTO 800GB SSDs NSE com revisões de firmware mais altas	1024	Permanente. Os dados não podem ser recuperados, mesmo quando a chave de autenticação adequada se torna disponível novamente.
Todos os outros modelos de SSD	1024	Permanente. Os dados não podem ser recuperados, mesmo quando a chave de autenticação adequada se torna disponível novamente.

Para todos os tipos de SED, uma autenticação bem-sucedida redefine a contagem de tentativas para zero.

Se você encontrar este cenário em que o sistema de armazenamento é interrompido devido a falha em alcançar qualquer servidor de gerenciamento de chaves especificado, primeiro você deve identificar e corrigir a causa da falha de comunicação antes de tentar continuar inicializando o sistema de armazenamento.

Desative a criptografia por padrão

A partir do ONTAP 9.7, a criptografia de volume e agregado é ativada por padrão se você tiver uma licença de criptografia de volume (VE) e usar um gerenciador de chaves integrado ou externo. Se necessário, você pode desativar a criptografia por padrão para todo o cluster.

Antes de começar

Você deve ser um administrador de cluster para executar essa tarefa ou um administrador SVM a quem o administrador de cluster delegou autoridade.

Passo

1. Para desativar a criptografia por padrão para todo o cluster no ONTAP 9.7 ou posterior, execute o seguinte comando:

   ```
   options -option-name encryption.data_at_rest_encryption.disable_by_default
   -option-value on
   ```

Informações sobre direitos autorais

Informações sobre marcas comerciais